DO NOT REPRINT
© FORTINET

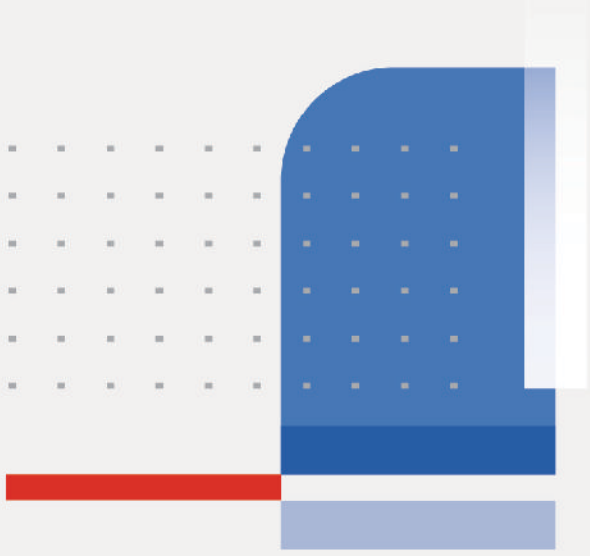
Passdumps.com

FORTINET CERTIFIED SOLUTION SPECIALIST Network Security

FORTINET CERTIFIED SOLUTION SPECIALIST Secure Access Service Edge

# SD-WAN Architect Study Guide

FortiOS 7.4



FORTINET Training Institute

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

**Fortinet Training Institute - Library**

https://training.fortinet.com

**Fortinet Product Documentation**

https://docs.fortinet.com

**Fortinet Knowledge Base**

https://kb.fortinet.com

**Fortinet Fuse User Community**

https://fusecommunity.fortinet.com/home

**Fortinet Forums**

https://forum.fortinet.com

**Fortinet Product Support**

https://support.fortinet.com

**FortiGuard Labs**

https://www.fortiguard.com

**Fortinet Training Program Information**

https://www.fortinet.com/nse-training

**Fortinet | Pearson VUE**

https://home.pearsonvue.com/fortinet

**Fortinet Training Institute Helpdesk (training questions, comments, feedback)**

https://helpdesk.training.fortinet.com/support/home

11/19/2024

Vouchers & Dumps are Available | WhatsApp +201224560923

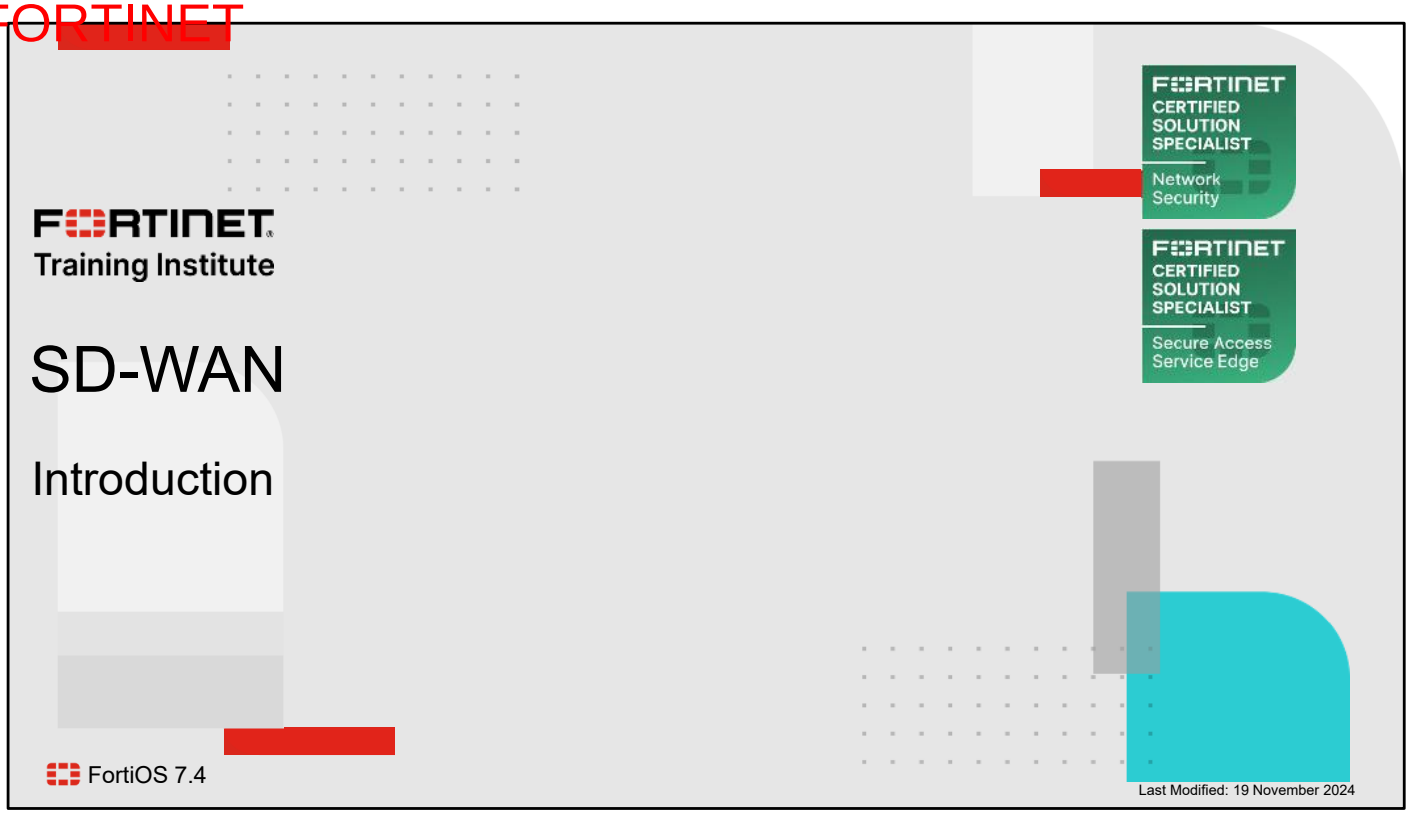
DO NOT REPRINT
© FORTINET
Brave-dumps.com

# TABLE OF CONTENTS

01 Introduction ..... 4
02 Centralized Management ..... 37
03 Zero-touch Provisioning and SD-WAN Monitoring ..... 81
04 Members, Zones, and Performance SLAs ..... 114
05 Routing and Sessions ..... 158
06 Rules ..... 197
07 SD-WAN Overlay Design and Best Practices ..... 257
08 Dual-Hub and Multiregion Topologies ..... 292
09 ADVPN ..... 331
Appendix - Troubleshooting and Redundancy Features ..... 386
Solution Slides ..... 417

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

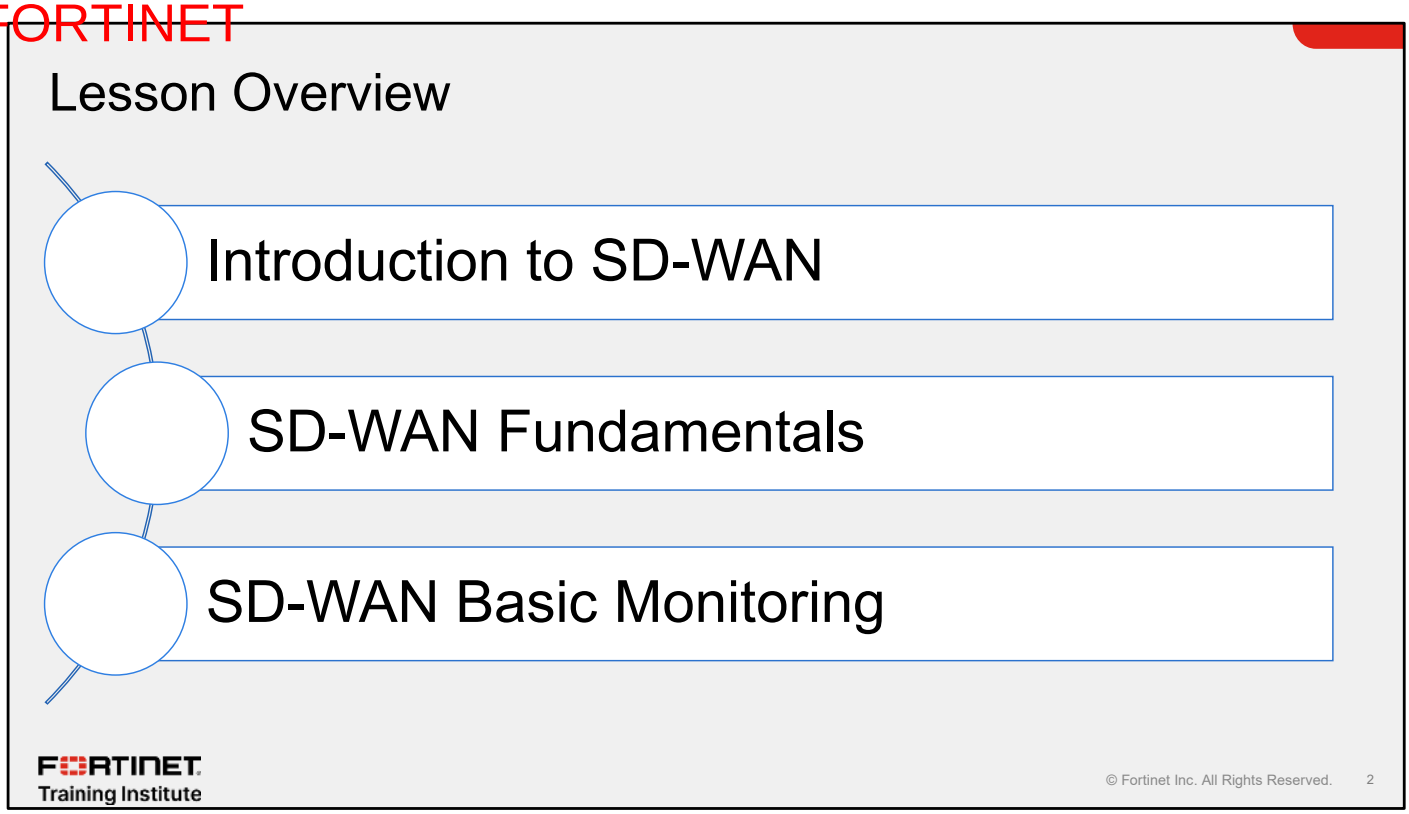



In this lesson, you will be introduced to the SD-WAN concept, use cases, and main components. You will also learn how to use the FortiGate GUI to configure and monitor a basic SD-WAN setup.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

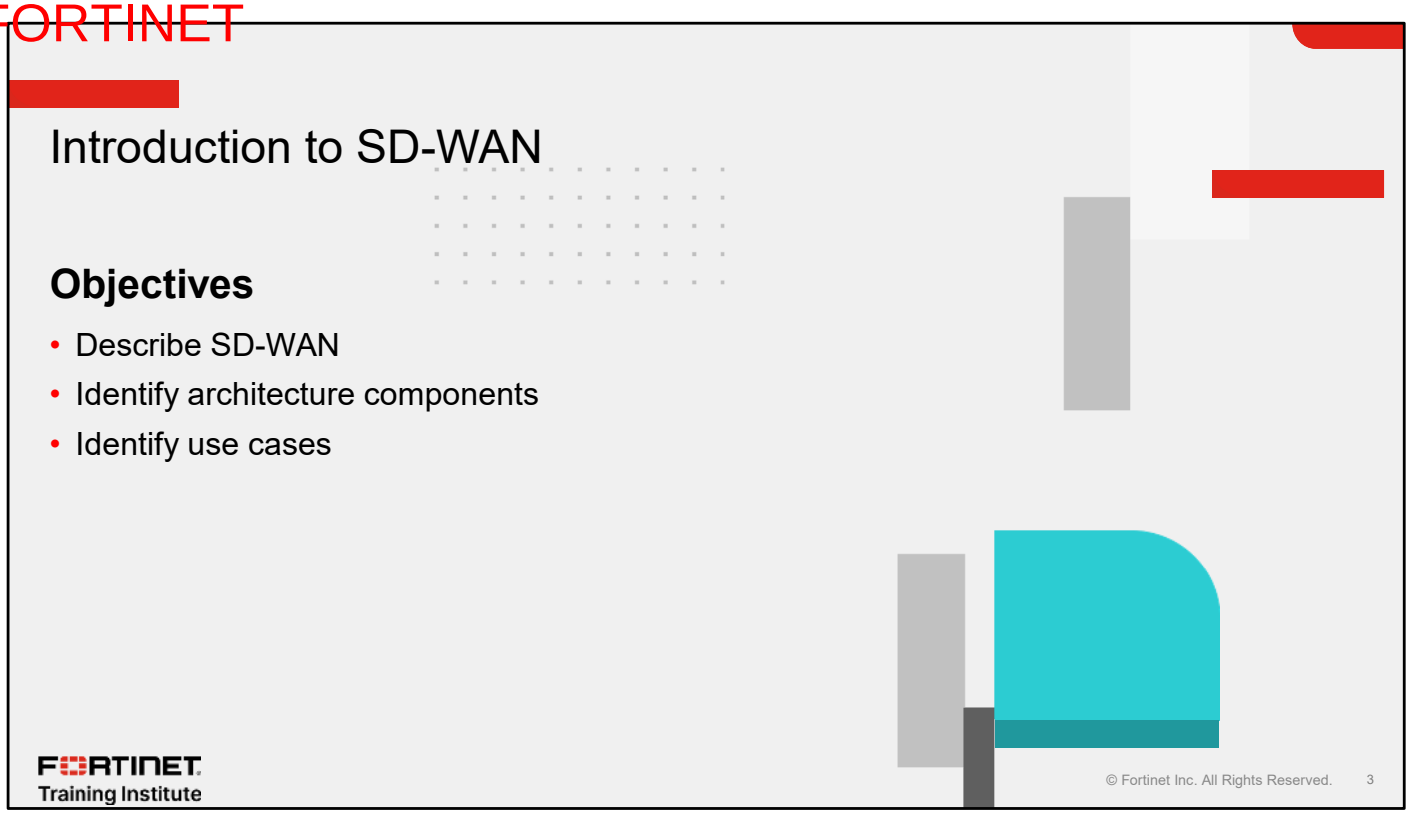



In this lesson, you will learn about the topics shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding an SD-WAN solution and its use cases, you should be able to identify the most common scenarios where SD-WAN can be deployed to distribute traffic across your WAN links effectively and securely.

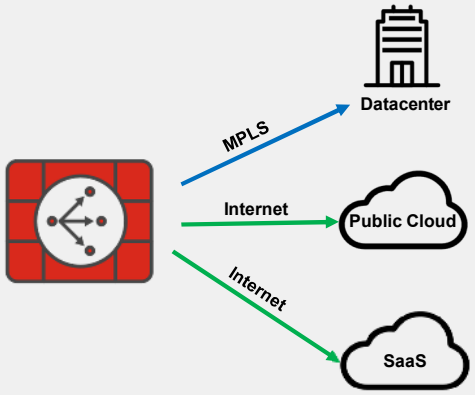


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## What Is SD-WAN?

- Software-defined approach to steer WAN traffic using:
  - Flexible user-defined rules
    - Protocol and service-based traffic matching
    - Application-awareness
    - Dynamic link selection
  - Session based
  - Controls egress traffic
- Secure SD-WAN
  - Fortinet SD-WAN implementation (built-in security)
- Benefits:
  - Effective WAN usage
  - Improved application performance
  - Cost reduction




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

According to Gartner, software-defined WAN (SD-WAN) provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services, such as WAN optimization and firewalls. Fortinet implementation of SD-WAN is called secure SD-WAN because it also provides security by leveraging the built-in security features available in FortiOS.

Secure SD-WAN relies on well-known FortiOS features such as IPsec, auto-discovery VPN (ADVPN), link monitoring, advanced routing, internet services database (ISDB), traffic shaping, UTM inspection, and load balancing. The administrator can then combine these features and set rules that define how FortiGate steers traffic across the WAN, based on multiple factors, such as the protocol, service, or application identified for the traffic; and the quality of the links. Note that SD-WAN controls egress traffic, not ingress traffic. This means that the return traffic may use a different link from the one SD-WAN chose for egress.

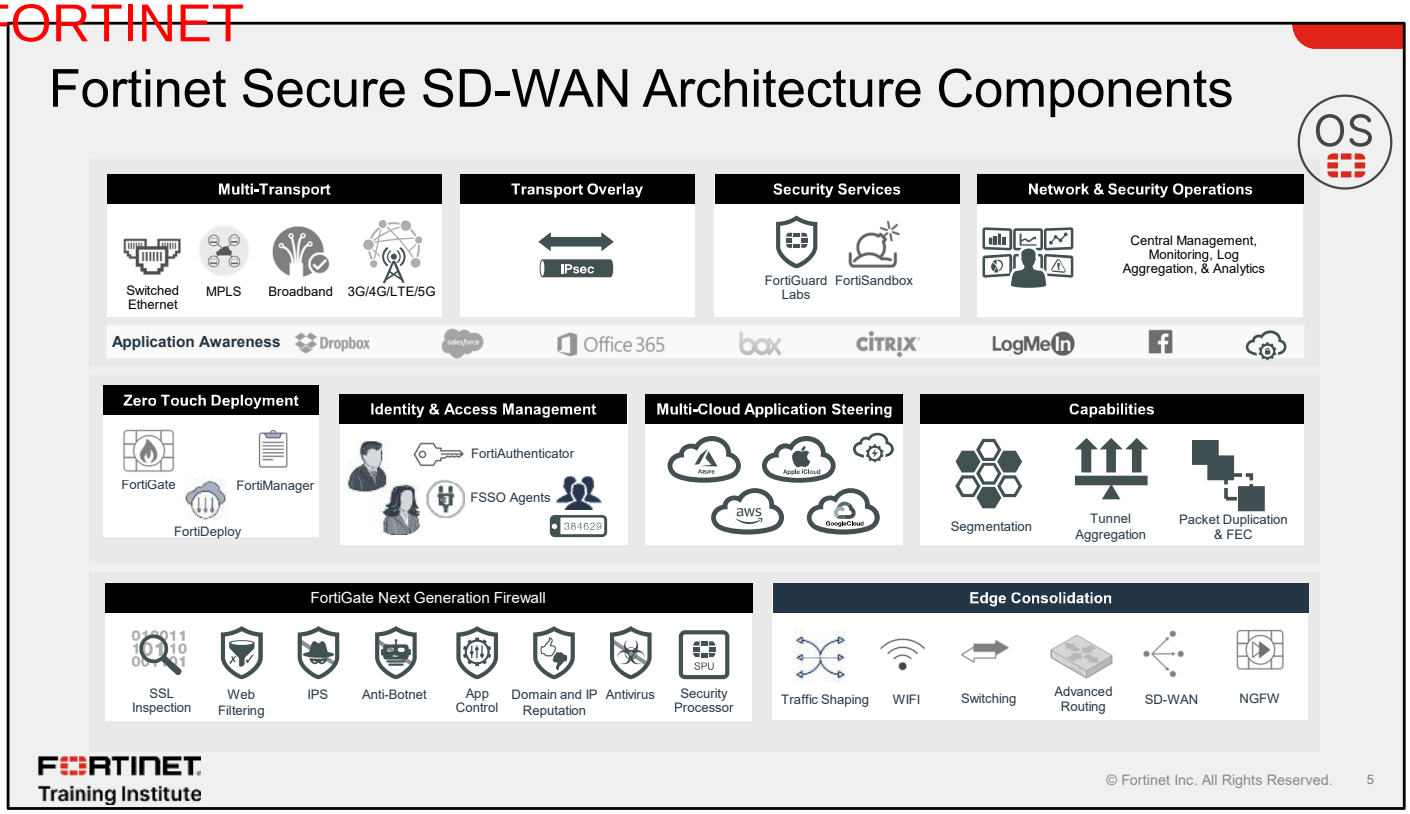
One benefit of SD-WAN is effective WAN usage. That is, you can use public (for example, broadband, LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of links to connect sites to private and public networks is known as hybrid WAN. Using a hybrid WAN reduces costs mainly because administrators usually steer traffic over low-cost fast internet links more than over high-cost slow private links. The result is that private links, such as MPLS links, are often used to steer critical traffic only, or as failover links for high availability.

Another benefit of SD-WAN is improved application performance because you can steer traffic through the best link that meets the application requirements. During congestion, you can leverage traffic shaping to prioritize sensitive and critical applications over less important ones. Also, the support of ADVPN shortcuts enables SD-WAN to use direct IPsec tunnels between sites to steer traffic, resulting in lower latency for traffic between the sites (spokes), and less load on the central locations (hubs).



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




This slide shows the architecture components of the Fortinet Secure SD-WAN solution.

The core component of the architecture is FortiGate. When you use FortiGate to deploy SD-WAN, you leverage the existing connectivity, management, and next-generation firewall (NGFW) features supported by FortiOS. This means that you can consolidate SD-WAN and security in a single device, thus the term Secure SD-WAN.

Because FortiGate is one of the core components in the Fortinet Security Fabric, then by extension, your SD-WAN deployment can also benefit from many of the features supported by other products in the fabric. For example, you could use FortiManager to perform zero touch provisioning for branches that require a SD-WAN setup. Similarly, you could use FortiSwitch to connect your WAN edge and LAN edge devices of your SD-WAN branch.

One key benefit of using FortiOS and FortiGate for your SD-WAN solution, is the ability to perform application steering in SD-WAN. FortiGate inspects traffic using its IPS engine and the application signatures provided by FortiGuard to identify thousands of applications. The result is that you can configure FortiGate to steer traffic based on the application detected, rather than ports, protocols, and IP addresses. The fact that FortiGate can identify the application regardless of the Layer 3 and Layer 4 information on the packet, enables you to significantly reduce administrative overhead and scale easier when deploying new applications and sites.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Vocabulary—Underlay and Overlay Links

- Categorize links and connections used in an SD-WAN context
- Underlay:
  - Physical links provided by ISP
    - Cable, DSL, fiber, MPLS, 3G/4G/5G/LTE, ATM
  - Restricted routing
  - No added security
- Overlay:
  - Virtual links built on top of underlay links
    - IPsec, GRE, IP-in-IP
  - Flexible routing
  - Enhanced security

| Supported SD-WAN members | |
|---|---|
| **Interface** | **Type** |
| Physical | Underlay |
| VLAN | |
| LAG | |
| 3G/4G/5G/LTE USB modems | |
| FortiExtender | |
| IPsec (including ADVPN) | Overlay |
| GRE | |
| IP-in-IP | |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

The terms *underlay* and *overlay* are used to describe the link type in an SD-WAN context.

Underlays refer to the physical links that you can rent or buy from an ISP, such as cable, DSL, fiber, MPLS, 3G/4G/5G/LTE, and ATM links. These links are part of the physical ISP infrastructure that is responsible for delivering packets across networks. The traffic that travels through underlays is restricted to the routing policies deployed by the ISP, and therefore, the packet source and destination IP addresses must be routable within the ISP network. This restriction leaves you with limited options to define your network addressing plan. In addition, traffic transmitted through underlays is usually not encrypted by the ISP network, which means that sensitive data can be accessed by unauthorized parties if the data is not encrypted by the sender.

Overlays are virtual links that you build on top of underlays. A common example of an overlay is an IPsec tunnel. Because original packets are often encapsulated in Encapsulating Security Payload (ESP) packets, the networks that communicate through the IPsec tunnel are no longer restricted to the routing policies of the ISP. In addition, the privacy and authentication features provided by IPsec protect your traffic from unauthorized access.

This slide shows the different underlay and overlay links supported by FortiGate as SD-WAN members.

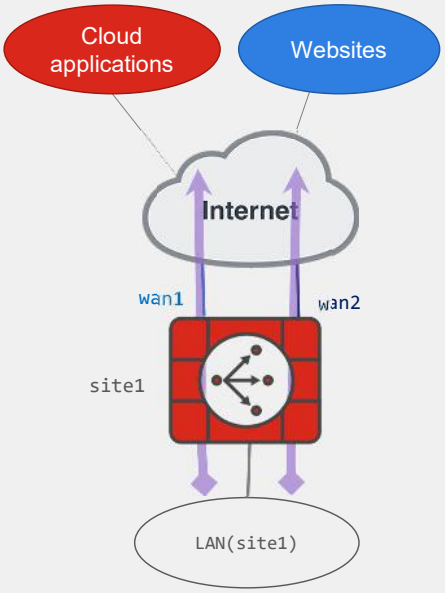


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Use Cases—Direct Internet Access

- Traffic steered across multiple physical internet links
- Typical operation:
  - Critical/sensitive traffic expedited and steered over best performing links
  - Costly links used for critical traffic or failover
  - Static default routing
- Upstream and downstream speeds can be:
  - Set manually by administrator
  - Set automatically by SD-WAN WAN monitoring service
- Supports single FortiGate deployment




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Direct internet access (DIA), also known as local breakout (LBO), is arguably the most common use case for SD-WAN. A site has multiple internet links (also known as underlay links), and the administrator wants FortiGate to steer internet traffic across the links. The links are connected to FortiGate using different types of physical interfaces: physical port, VLAN, link aggregation (LAG), USB modem, or through FortiExtender.

Usually, sensitive traffic is expedited and steered over the best performing links, while non-critical traffic is distributed across one or more links using a best effort approach. Costly internet links are commonly used as backup links, or to steer critical traffic only.

Because the internet traffic leaves the organization boundaries directly on the local site, administrators usually enforce strict security policies on the internet traffic. For routing, a typical configuration makes use of static default routes. However, in some cases, BGP is used between the ISP and FortiGate, especially if the site must advertise a public IP prefix.

Administrators can also manually define the upstream and downstream speeds of each link to prevent saturation during traffic distribution. Alternatively, they can configure FortiGate to use the SD-WAN bandwidth monitoring service to run speed tests against FortiGuard, and then automatically adjust the upstream and downstream speeds of the links based on the test results.

The diagram on this slide shows an example of DIA. A single FortiGate device has two internet links. One link is connected to wan1 and the other to wan2. FortiGate uses both links to steer traffic sourced from the LAN and destined to cloud applications and websites on the internet.

You can deploy FortiGate for DIA as a single device as shown on this slide or combined with other use cases in more complex topologies.



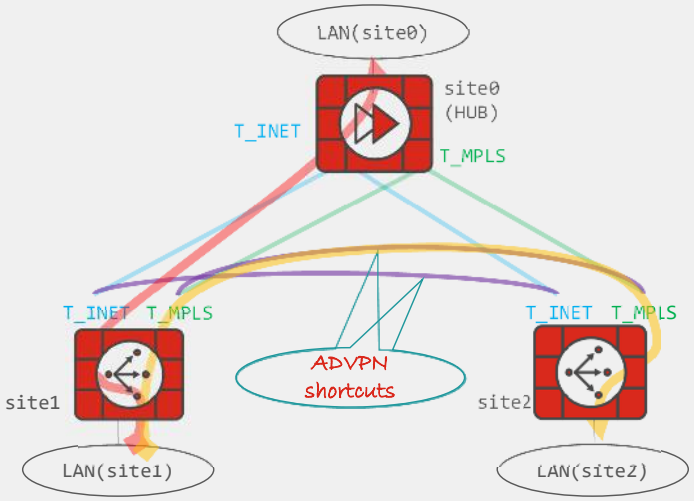
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Use Cases—Site-To-Site Traffic

- Use overlay links to steer site-to-site corporate traffic
  - Overlay: IPsec, GRE, IP-in-IP (established over underlays)
  - Underlay: physical links (internet and MPLS circuits, 3G/4G/LTE modems, and so on)
- Typical operation:
  - Dial-up IPsec used for overlay
  - If using ADVPN:
    - Offload site-to-site traffic to shortcuts
    - SD-WAN checks health of shortcuts
    - Apply full security inspection on spokes
  - Dynamic routing
    - More scalable




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

You can use SD-WAN to steer corporate site-to-site traffic. Usually, companies follow a hub-and-spoke topology, and use VPN tunnels—typically dial-up IPsec tunnels—to transport the traffic between the sites. The tunnels, also known as overlay links, are established over internet and MPLS links (underlay).

SD-WAN can monitor the link quality of the tunnels and select the best performing link for sensitive and critical traffic. If using ADVPN, SD-WAN can offload the traffic from a parent tunnel to a shortcut, thus reducing latency for spoke-to-spoke traffic. SD-WAN can also monitor the health of the shortcut tunnels to ensure they meet the configured service-level agreement (SLA).

For routing, a dynamic routing protocol such as BGP, is often used to exchange routing information through the tunnels, and scales easier when adding new sites. If you are using ADVPN, internal BGP (IBGP) is recommended to preserve next-hop information.

The diagram on this slide shows an example of a deployment that uses SD-WAN to steer site-to-hub and site-to-site traffic.

Each site has two overlays configured, one using the internet underlay and the other the MPLS underlay. SD-WAN steers spoke-to-spoke and spoke-to-hub traffic. Because ADVPN is configured on the network, shortcuts are automatically established between spokes when spoke-to-spoke traffic is sent across the network. SD-WAN can then automatically offload the spoke-to-spoke traffic from parent tunnels to shortcuts, thus improving performance. SD-WAN also monitors the health of shortcuts and dynamically makes steering decisions based on their health and availability.

Note that the hub site can use the SD-WAN function, but this is not mandatory. However, to use the ADVPN feature, the hub must be a FortiGate firewall.

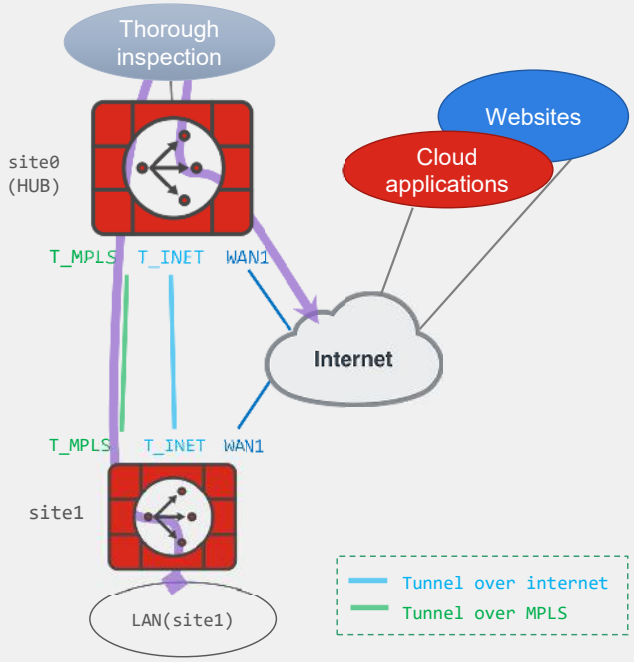


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Use Cases—SIA

- Internet traffic steered across overlay links to:
  - Centralize inspection on the hub
  - Improve performance if DIA performance is poor
  - Provide internet access if DIA is unavailable
- Typical operation:
  - Internet traffic is steered to MPLS
  - Hub performs thorough inspection




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

Secure internet access (SIA), also known as remote breakout, is another use case for SD-WAN. Internet traffic from the spokes is backhauled through the WAN using overlay links. When the traffic arrives at the hub, it breaks out to the internet.

The most common reason to use SIA is to centralize security inspection and internet access on the hub. For example, you can have a central high-end FortiGate device that inspects all the internet traffic that leaves the organization and that conforms with the company policy, instead of having each low-end spoke FortiGate device to inspect traffic, thus reducing costs and administrative overhead.

Another reason to use SIA is for DIA backup. For example, you could configure FortiGate to steer internet traffic through an MPLS link if the performance measured for internet applications on internet links is worse than on MPLS links, or simply if the internet links become unavailable.

The diagram on this slide shows an example of SIA.

Instead of using the local internet underlay to forward internet traffic, the FortiGate device on site 1 steers internet traffic to the hub through the overlay built over MPLS. Once the traffic reaches the hub, the traffic is subject to a thorough security inspection before it breaks out to the internet.

For such topologies, you must configure SD-WAN on both FortiGate firewalls, on the branch and on the hub site.

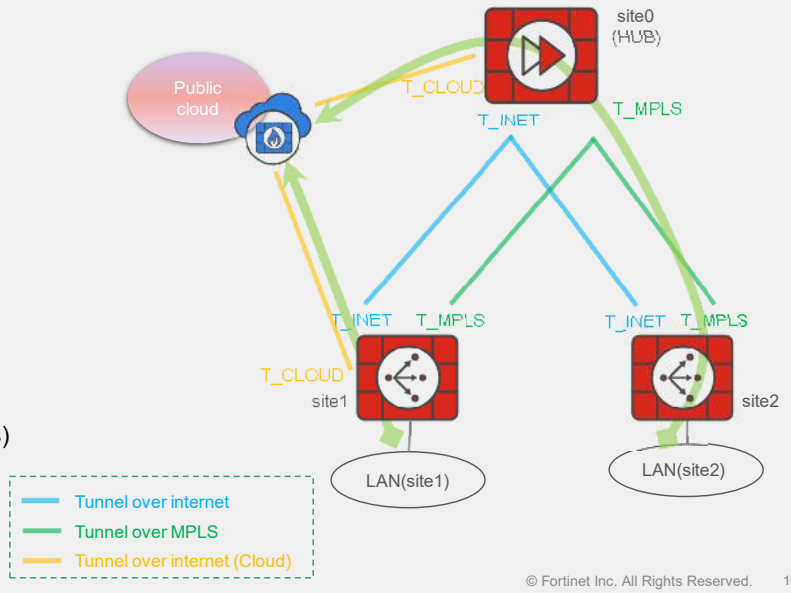


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Use Cases—Cloud On-Ramp

- Steer cloud application traffic to overlays against cloud POPs
  - High performance
  - Secure access
- Establish overlays to
  - Built-in cloud gateway
    - Unidirectional secure SD-WAN
  - Cloud FortiGate VMs
    - Bidirectional secure SD-WAN
- Typical operation:
  - Direct connection from spokes
    - Usually, the best performance
  - Backhaul traffic through WAN
    - Required by company policy
    - Best performance (premium WAN links)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

To improve the performance of cloud applications while keeping network traffic secure, you can configure overlays to the closest point of presence (PoP) offered by the cloud provider in the area, thus reducing latency. You can configure FortiGate to connect to the cloud provider's built-in VPN gateway. Alternatively, you can deploy a FortiGate VM in the cloud and establish the overlays to it. Choosing to deploy a FortiGate VM in the cloud enables you to use FortiOS security features on traffic entering or leaving the cloud, as well as to use SD-WAN to steer sessions originating from the cloud.

For optimal performance, a cloud on-ramp connection is usually established directly from the spoke because a direct connection often results in the lowest latency. However, in some cases, traffic could be backhauled through the WAN using overlay links because of company policy, or because cloud tunnels are available only on the hub. Another reason to backhaul cloud traffic through the WAN can be performance. For example, a company may use premium WAN links between the spokes and the hub, and between the hub and the cloud. The performance of the premium links is so high that backhauling traffic through the WAN would result in a better user experience than accessing the local POP directly from the spoke.

The diagram on this slide shows an example of a cloud on-ramp.

The FortiGate on site 1 has a direct tunnel to a FortiGate running as a cloud native firewall. This tunnel steers cloud application traffic to optimize performance and security. Also, unlike site 1, the FortiGate on site 2 uses an overlay to the hub to send cloud application traffic. The hub then routes the traffic through its local cloud tunnel.

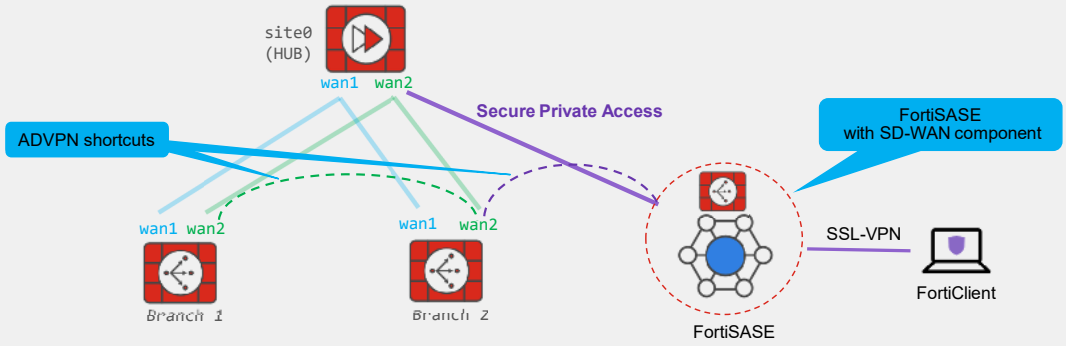


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Secure Private Access With SD-WAN and SASE

- Secure remote users with access to company resources
- Add FortiSASE as a spoke
- Benefit from all FortiSASE points of presence (POPs) for proximity to users
- Secure tunnels between SD-WAN hub and FortiSASE POPs
- Shortcut tunnels—ADVPN—possible between branches and FortiSASE




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

SASE stands for Secure Access Service Edge and refers to products that deliver converged network and security service capability. FortiSASE refers to the Fortinet SASE, which provides secure access to remote users for the following use cases:

- Secure internet access (SIA) when remote users access internet and web-based applications
- Secure private access (SPA) when remote users access private company-hosted applications
- Secure SaaS access (SSA) when remote users access SaaS applications

In the SPA use case, organizations integrate FortiSASE with FortiGate SD-WAN deployments to provide remote users with access to private resources. In this configuration, FortiSASE communicates with the FortiGate SD-WAN hub, and FortiSASE security POPs, located throughout the world, act as spokes.

The diagram on this slide shows an example of an SD-WAN deployment that integrates FortiSASE to provide remote users with secure access to company internal resources. Remote users establish a secure connection to FortiSASE, and then, through the hub, can access company resources. on the hub or on any branch sites. Optionally, to offload the hub and speed up traffic between branches or between branches and FortiSASE, the devices can establish shortcut VPN tunnels, also called ADVPN shortcuts.

FortiSASE has a built-in SD-WAN engine for intelligent routing selection among the established IPsec links. Note that the FortiGate SD-WAN hub requires an SPA license to establish a dedicated tunnel to FortiSASE.

To integrate FortiSASE to an SD-WAN topology, you must configure the **Secure Private Access** feature on the FortiSASE portal. Once configured, all FortiSASE POPs act as spokes to this hub, relying on IPsec VPN overlays and IBGP to secure and route traffic between POPs and the company networks behind the hub and branch FortiGate devices. FortiSASE acts as a bridge to connect a remote worker to the corporate applications hosted behind the company FortiGate devices.

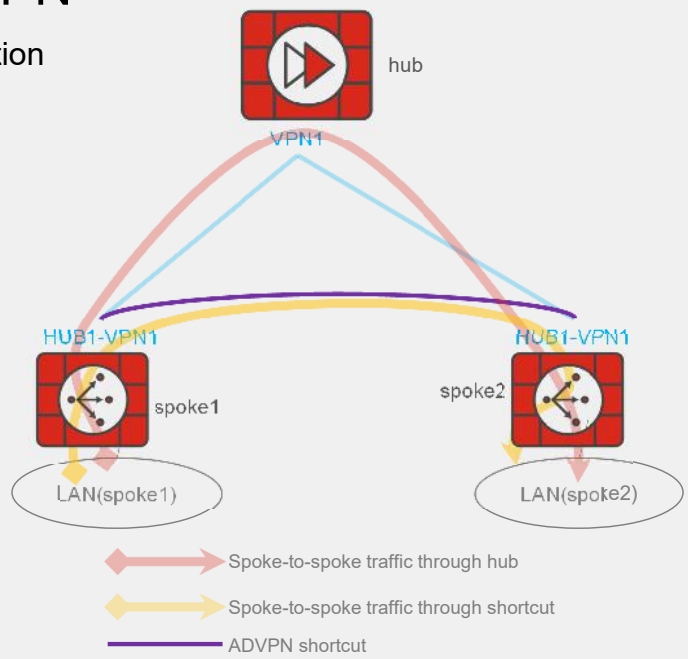


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Auto-Discovery VPN—ADVPN

- Enables direct spoke-to-spoke communication
  - Fortinet proprietary
  - Based on IKE and IPsec
  - Benefits of a full-mesh topology in a hub-and-spoke network
- Hub facilitates spokes shortcut negotiation
  - On-demand IPsec tunnels
  - Shortcuts carry spoke-to-spoke traffic
- Supported by SD-WAN
  - Automatically steers traffic through shortcuts
  - Shortcuts are monitored




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

Auto-discovery VPN (ADVPN) is a Fortinet-proprietary solution that provides the benefits of a full-mesh topology in a hub-and-spoke network.

Consider the simple hub-and-spoke topology shown on this slide. If a device behind spoke1 wants to communicate with a device behind spoke2, the device must do so through the hub. While a hub-and-spoke topology reduces cost and configuration overhead, the fact that a spoke must communicate with other spokes through the hub increases the delay of the communication, and therefore impacts the user experience, especially if the hub and spokes are in geographically distant locations.

An alternative is to use a full-mesh topology, which enables direct spoke-to-spoke communication at the expense of higher costs and increased administrative overhead. However, this is not always practical, or even feasible, especially in large networks.

ADVPN is based on IKE and IPsec, that addresses the need for direct spoke-to-spoke communication in hub-and-spoke topologies by enabling the spokes to automatically negotiate on-demand IPsec tunnels—called shortcuts—between them without you having to make topology changes or many configuration changes. After a shortcut is established and routing has converged, spoke-to-spoke traffic no longer needs to flow through the hub.

SD-WAN supports ADVPN shortcuts. For this, SD-WAN automatically steers the traffic through shortcuts and monitors their health and performance. You add the parent tunnel as an SD-WAN member, and after the shortcut is negotiated, SD-WAN automatically starts steering the traffic through the shortcut.

The topology on this slide also shows a shortcut established between spoke1 and spoke2. The result is that FortiGate routes the spoke-to-spoke traffic through the shortcuts instead of through the hub.

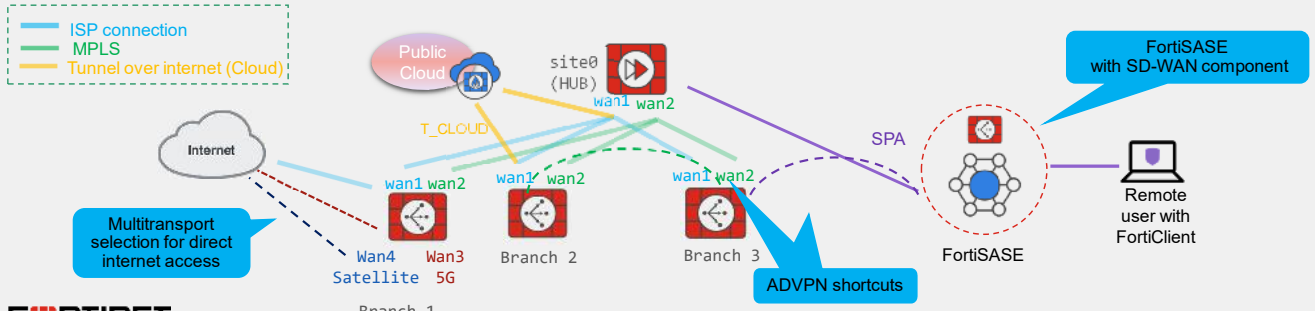


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Use Cases Summary

- Regardless of the topology, SD-WAN on FortiGate allows:
  - Dynamic application steering across multiple WAN links
  - Redundant WAN links selection between multiple transport types: MPLS, ISP, LTE/5G, satellite links
  - Transport-agnostic link selection
  - Optimized multicloud connectivity and cloud on-ramp
  - Application performance improvement, with the use of the application control feature for both application identification and application steering
  - Optimized and secured connectivity to remote users with a SASE connection



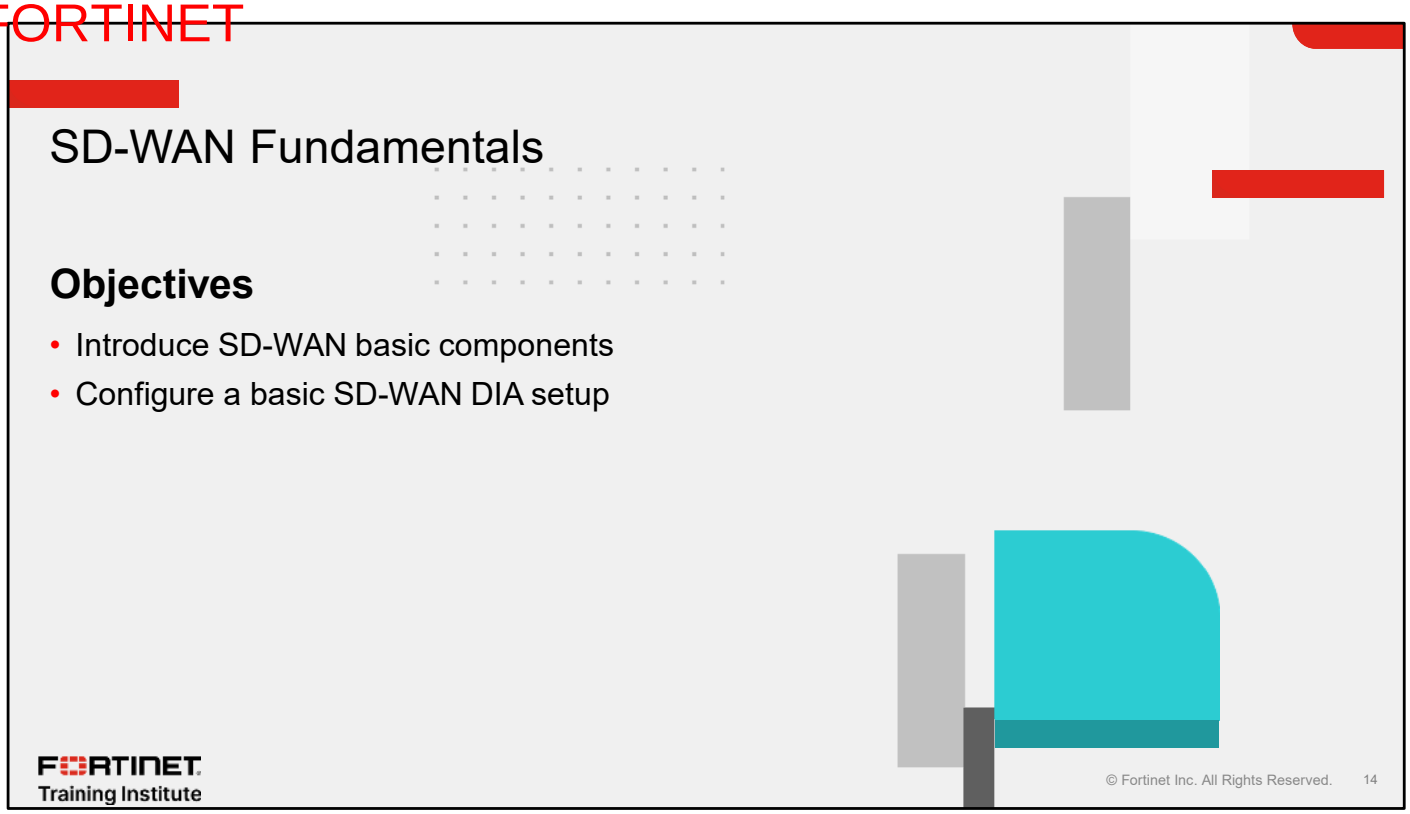

According to the company requirements, you can design topologies that combine multiple use cases described on the previous slides.

In the example shown on this slide:
- All sites require dynamic application steering across multiple WAN links.
- All sites require redundant WAN link selection, but only some sites benefit from multitransport types with 5G and satellite links that complement the ISP and MPLS links.
- All sites connect to the company hub to benefit from application steering to the corporate datacenter, but only some sites require direct internet access or direct cloud connectivity.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in SD-WAN fundamentals, you should be able to understand the basics of SD-WAN, including how to configure a basic DIA setup.

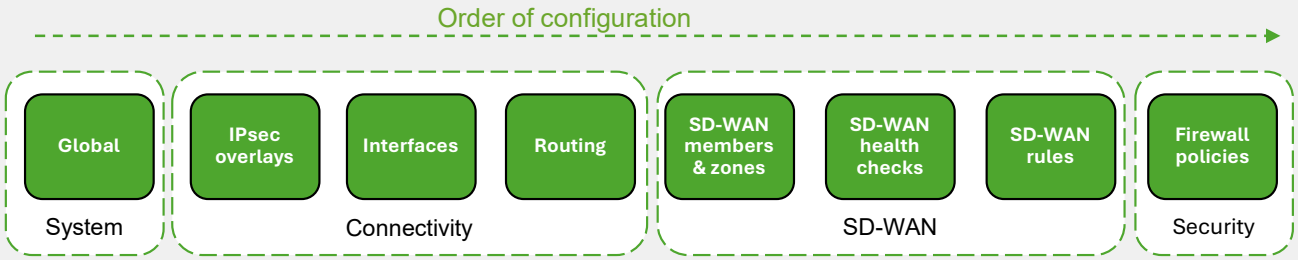


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Configuration on FortiGate

- Workflow




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

When you configure a FortiGate for SD-WAN, first you configure the global system settings, such as the device name and the admin users, then the interfaces and the routing—static or dynamic. These configuration tasks are the same for every FortiGate. Next, you perform the configuration tasks specific to SD-WAN, that includes the member and zone configuration, the performance SLA—also called health check—and the SD-WAN rule. Finaly, you define the security features and the firewall policies.

The diagram on this slide summarizes this configuration timeline. On the next few slides, you will learn how to configure the SD-WAN elements using the FortiGate GUI.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN on FortiGate—Main Concepts

- SD-WAN members and zones
  - Define FortiGate interfaces that participate in SD-WAN as members and group them in zones
- Performance SLA
  - Define performance SLA—also called health check—to monitor the link quality of SD-WAN interfaces
  - Used to determine the most qualified member to steer the traffic
- SD-WAN rules
  - Define rules to instruct FortiGate to steer the traffic to different links according to multiple criteria
  - Implement the administrator steering strategy
  - Main criteria
    - Type of traffic identified per subnet or per application
    - Link quality criteria, such as latency, jitter, or packet loss
- Foundations
  - FortiGate routing table: determine all possible routes to steer the traffic
  - FortiGate firewall policy: apply the security measures

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

From a high-level point of view, SD-WAN on FortiGate uses a set of rules, defined by the administrator, to steer the most important traffic in an organization through the best-qualified interfaces. To achieve these objectives, the administrator must define:

1. The SD-WAN members and zones—these are the interfaces that participate in SD-WAN
2. The performance SLA—this is how FortiGate monitor the quality of the SD-WAN link
3. The SD-WAN rules. This is how the administrator defines the traffic steering strategy

Usually, the administrator defines the sequenced SD-WAN rules with a focus on the applications that are the most critical for the organization. Each rule precisely defines the traffic matching criteria, by IP addresses, but also per application, and specifies the selection criteria for the outgoing interface. SD-WAN rules allow the administrator to use the link quality measured by the SD-WAN health check to steer a set of flows through the link with the lowest latency, another set of flows through the link with the lowest packet loss, and the remaining flows through the least-used link.

Note that SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic:

- The static and dynamic routing features provide the routing table that SD-WAN uses as a basis to determine the link to steer the traffic through.
- The firewall policies to define if the traffic is allowed to pass through or not, and the security measures to apply to allowed flows.

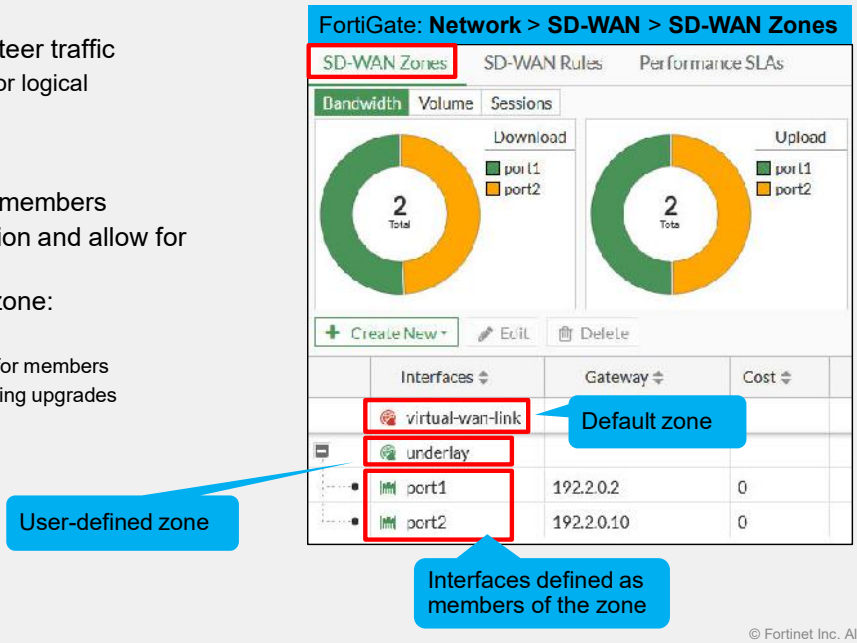


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Members and Zones

- Members
  - Interfaces used to steer traffic
    - Can be physical or logical
  - Organized in zones
- Zones
  - Logical grouping of members
  - Optimize configuration and allow for segmentation
  - Predefined default zone:
    - **virtual-wan-link**
      - Default zone for members
      - Also used during upgrades




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

The first step to configure SD-WAN is to define the members and assign them to zones on the **SD-WAN Zones** page.

Members (also known as links) are existing physical or logical FortiOS interfaces that you select to be part of SD-WAN. The interfaces are then used to steer traffic based on the SD-WAN rules configured.

When you configure a member in SD-WAN, you must assign it to a zone, and optionally set a gateway. Zones are logical groupings of interfaces. The interfaces in a zone have similar configuration requirements. Similar to FortiGate interface zones, SD-WAN zones exist to optimize the configuration by referencing zones instead of individual members. This approach helps avoid duplicate settings and enables effective network segmentation. When set, FortiGate uses the **Gateway** setting as the next hop to forward traffic through the zone members.

One zone is created by default: **virtual-wan-link**. The zone, **virtual-wan-link,** is the default zone where FortiGate places members when you create them. FortiGate also use the default zone when you upgrade a FortiGate device running a version with no support for zones to a version that supports zones. During the upgrade, FortiGate places all existing members in the **virtual-wan-link** zone.

The example on this slide shows the default SD-WAN zone—**virtual-wan-link**—and one user-defined zone: **underlay**. The **underlay** zone contains **port1** and **port2** as members, which are used for a basic DIA setup. Note that, although the zone is named **underlay** because it contains such members, you can assign any name you like.

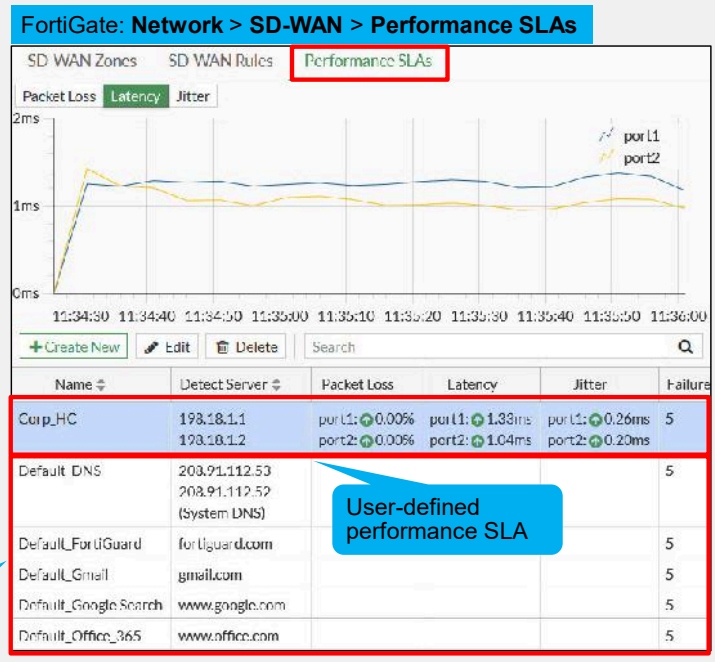


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Performance SLAs

- Performs member health check:
  - State
    - Alive or dead
  - Performance:
    - Packet loss, latency, and jitter
- Usage:
  - Detect unavailable links
  - Monitor performance criteria
- Health can be measured:
  - Actively
    - Based on periodic probes sent to configured servers
  - Passively
    - Based on member traffic




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

After you define your SD-WAN members and assign them to zones, you should monitor the health of your SD-WAN members on the **Performance SLAs** page.

FortiGate performance SLAs monitor the state of each member—alive or dead—and measures the member packet loss, latency, and jitter. SD-WAN then uses the member health information to make traffic steering decisions based on the configured SD-WAN rules. For example, you can instruct FortiGate to steer internet traffic to a member, provided the member is alive and its latency doesn't exceed a given threshold. Performance SLAs also detect situations where the interface is physically up, but FortiGate is unable to reach the desired destination and flags the corresponding link as dead.

When you configure a performance SLA, FortiGate lists several entries created by default that you can choose from. The default entries measure the health of members against well-known internet services, such as FortiGuard or Google Search. Alternatively, you can create your own entry and choose whether you want to monitor the health actively or passively. In active monitoring, the health of the member is checked by periodically—by default every 500ms— sending probes from the member to one or two servers that act as a beacon. In passive monitoring, the health of a member is determined based on the traffic passing through the member.

The example on this slide shows a new entry named **Corp_HC**. The entry contains two detect servers 198.18.1.1 and 198.18.1.2, both of which are used to monitor the health of **port1** and **port2**. The results show that the members are alive (green arrow), report no packet loss, and have average values for delay and jitter over the internet.

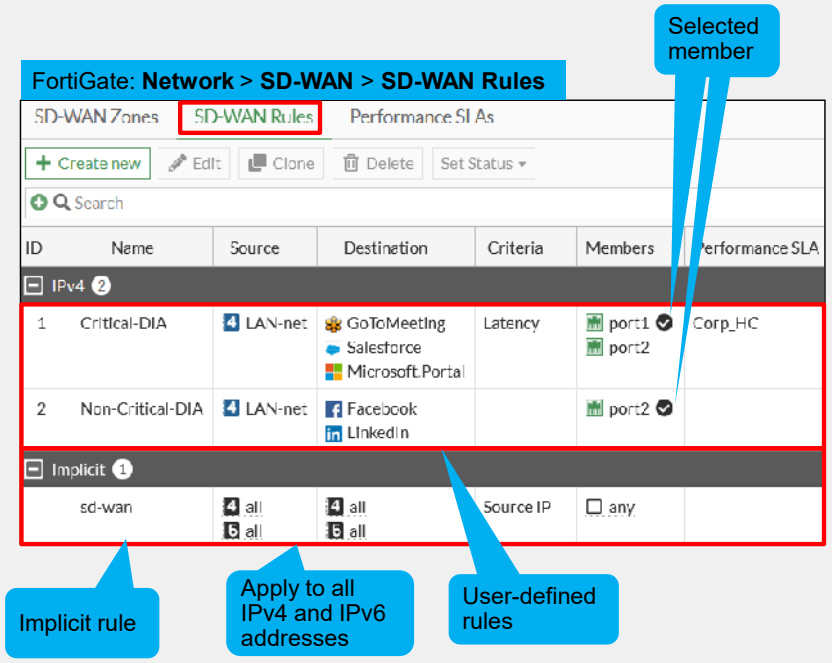


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Rules

- Define steering rules based on:
  - Matching traffic criteria
    - Define pattern, ISDB, and application to match
  - Member preference
    - Define list of preferred members and zones to steer traffic to
  - Member performance
    - Define SLA to meet for members
- Evaluated from top to bottom
  - Rules are used to steer traffic
    - Firewall policy required
  - Implicit rule
    - Used if user-defined rules are not matched




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

After you configure the zones, members, and performance SLAs, it's time to define the traffic steering rules for SD-WAN on the **SD-WAN Rules** page.

When you configure an SD-WAN rule, you first define the application or traffic pattern to match. Then, you indicate the preferred members or zones, to steer the matching traffic to and in some cases, the performance metrics that the member must meet to be eligible to receive and forward the traffic.

SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom, using the first match. However, unlike firewall policies, they are used to steer traffic, *not* to allow traffic. When you use SD-WAN rules, you *must* configure corresponding firewall policies to allow the SD-WAN traffic.

FortiGate creates a default implicit SD-WAN rule. If no user-defined SD-WAN rules are matched, then the implicit rule is used. By default, the implicit rule load balances the traffic across all available SD-WAN members.

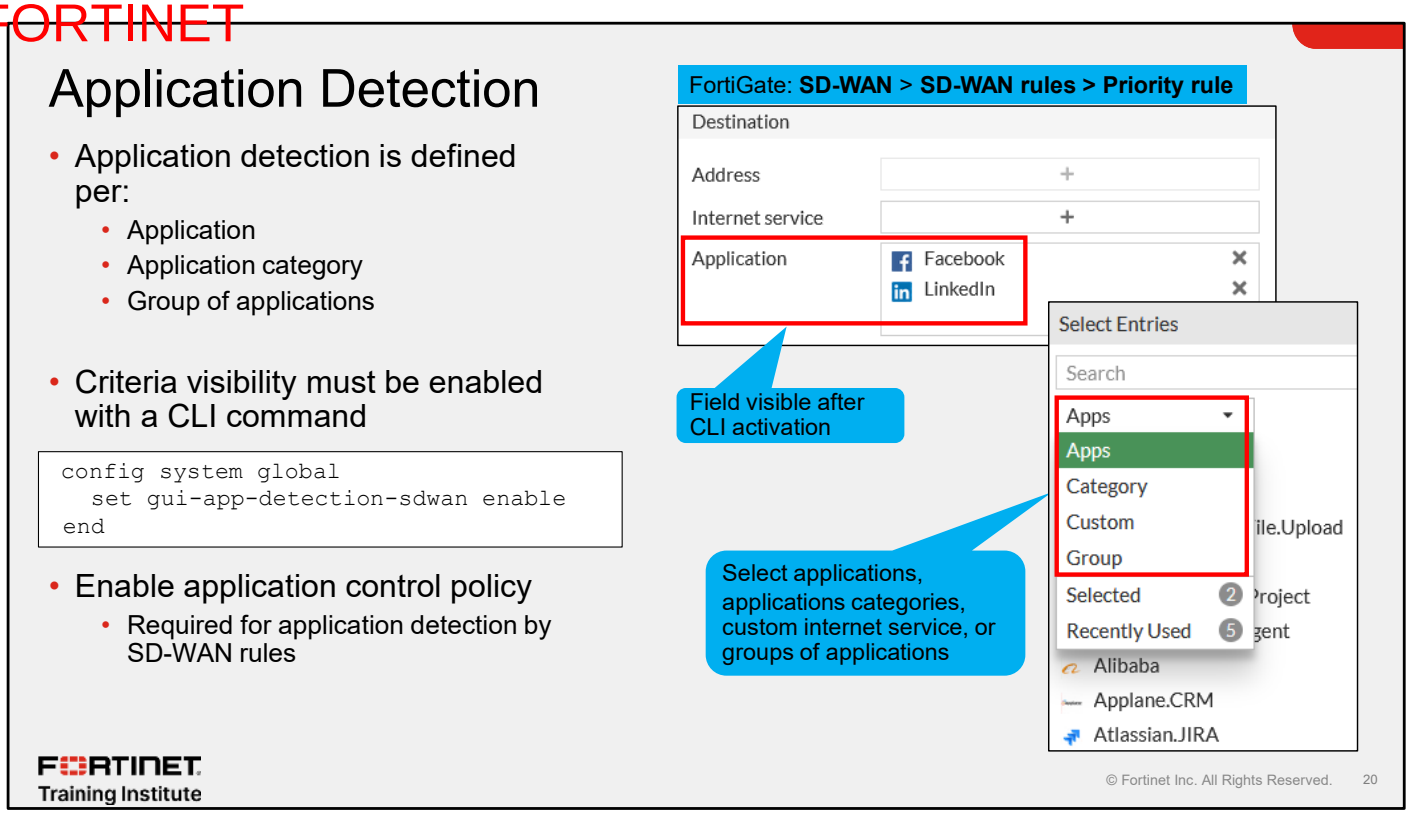
The example on this slide shows two user-defined rules named **Critical-DIA** and **Non-Critical-DIA**, which are used to steer traffic in a basic DIA setup. The **Critical-DIA** rule steers **GoToMeeting**, **Microsoft.Portal**, and **Salesforce** traffic to the member with the lowest latency, between **port1** and **port2**. The example shows that **port1** is selected because it is the member with the check mark beside it. The **Non-Critical-DIA** rule steers **Facebook** and **LinkedIn** traffic to **port2**.

The implicit rule, located at the bottom of the list, is used if neither of the two user-defined rules are matched. You can see that it applies to all IPv4 and IPv6 source and destination addresses. The icons beside the object names—4 and 6—distinguish IPv4 objects from IPv6 objects.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




For well-known applications, you can rely on FortiGuard services and define SD-WAN rules to steer traffic per application or application category. For instance, you can decide to direct leisure applications like games or Facebook to low-cost links and reserve high-quality, costly links for business traffic.

Visibility of application detection criteria is, by default, hidden on the FortiGate GUI. You must enable feature visibility on the CLI using the global command `set gui-app-detection-sdwan enable`. Note that if GUI visibility is disabled, configuration for application criteria remains active and configuration is still visible on the CLI.

When you define the rule destination per application you can select applications, application categories, custom internet services, or groups of those elements.

To determine which applications flowing through your network match the defined applications, use the CLI command `diagnose sys sdwan internet-service-app-ctrl-category-list <id>`.

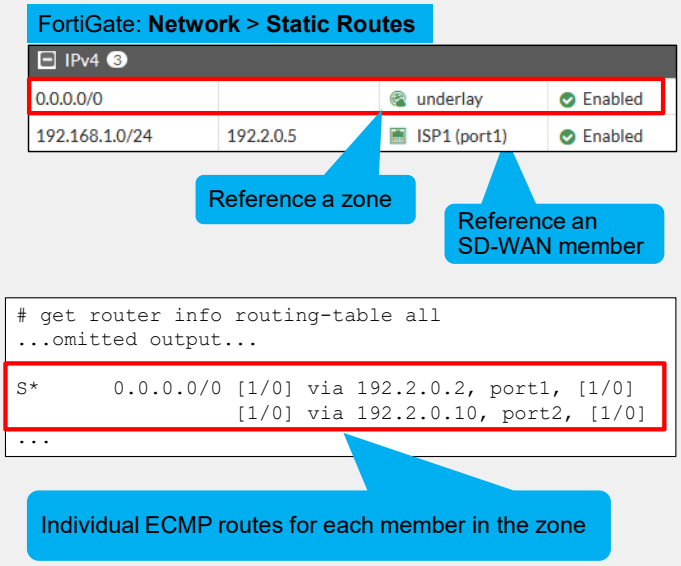


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Routing

- Valid route required for steering traffic to member
- Dynamic routing
  - BGP recommended
  - BGP required for ADVPN
- Static routes
  - Use cases:
    - Small topologies
    - To complement the dynamic routing protocol
  - Reference a zone
    - Common case, simplified configuration
    - Individual ECMP routes installed for each member in the zone
    - Gateway obtained from member configuration
  - Reference a member
    - More granular control
    - User-defined gateway




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

SD-WAN rules define the traffic steering policies in SD-WAN. However, traffic isn't forwarded to an SD-WAN member unless a valid route matches the destination address of the traffic through the SD-WAN member.

You can use static and dynamic routing in SD-WAN. Static routes are commonly used in small topologies or to define the default gateway. Fortinet recommends the use of dynamic routing with BGP for most SD-WAN topologies. Note that you need to use IBGP as routing protocol if you want to allow ADVPN.

This slide shows an example of a static default route configured for the **underlay** zone, which is used to route traffic in our basic DIA setup. When you configure static routes for SD-WAN, you usually reference an SD-WAN zone to simplify the configuration. However, you can also reference individual members instead, so you can have more granular control over traffic. When you reference a zone in a static route, FortiGate installs individual routes for each member in the zone. The individual routes are then displayed in the routing table as equal-cost multi-path (ECMP) routes.

Note that when you configure a static route that references a zone, you don't have to specify a gateway address because FortiGate retrieves it from the member configuration.

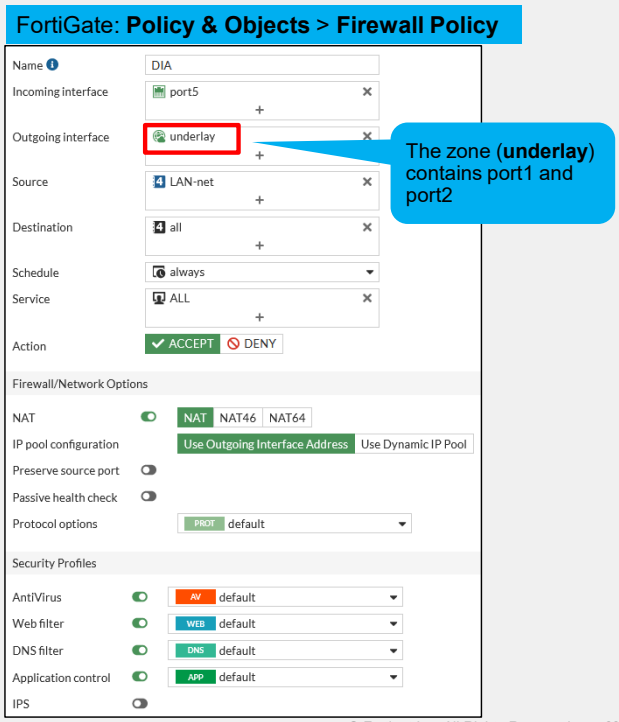


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Firewall Policies

- Steered traffic must be allowed by a firewall policy
- Reference zones only
  - Simplified configuration
- Can't reference a member directly
  - Create zones with single members




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

In addition to having a valid route, you must also have a firewall policy that allows the traffic steered by SD-WAN.

You configure SD-WAN firewall policies in the same way as regular firewall policies, except that when selecting an outgoing or incoming interface, you must reference an SD-WAN zone. When you reference a zone, you simplify the configuration by avoiding duplicate firewall policies.

You may need to reference a member in your firewall policy because you want to apply a different action on the traffic flowing through that member, such as applying different security profiles and NAT settings. Because you can't reference members in a firewall policy, a workaround is to place a single member in a separate zone, and then reference that zone in the firewall policy.

The example on this slide shows a firewall policy named **DIA** that references the **underlay** zone, which contains port1 and port2 as members. As a result, FortiGate allows DIA traffic steered over port1 or port2 provided it matches the firewall policy criteria, and it passes the security inspection configured on the policy.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN CLI Configuration

- Zone, member, and performance SLA:

```
config system sdwan
    set status enable
    config zone
        edit "underlay"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
        next
        edit 2
            set interface "port2"
            set zone "underlay"
        next
    end
    config health-check
        edit "Corp-HC"
            set server "198.18.1.1" "198.18.1.2"
            set members 1 2
        next
    end
...
```

- Rules:

```
...
    config service
        edit 1
            set name "Critical-DIA"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 16354 41468 16920
            set priority-members 1 2
        next
        edit 2
            set name "Non-Critical-DIA"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 16001
            set priority-members 2
        next
    end
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

This slide shows the equivalent CLI configuration for the basic SD-WAN DIA setup described so far. The SD-WAN configuration is found under `config system sdwan`. Under `config system sdwan`, there are separate configuration sections for each SD-WAN component.

The example shown on this slide divides the CLI configuration into two parts. The first part displays the zone, member, and performance SLA configuration. The second, the SD-WAN rules configuration. Note that FortiOS uses the terms `health-check` and `service` to refer to the performance SLA and rule configuration on the CLI, respectively. You will explore the CLI configuration in more detail in other lessons.

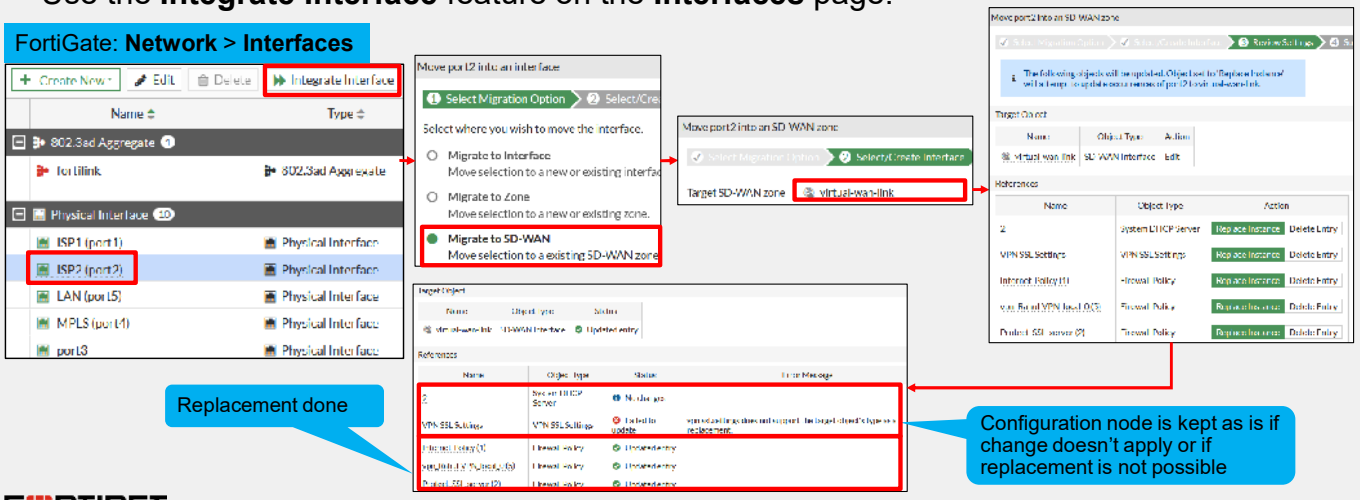


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Migrating Interfaces to SD-WAN

- Replace references to individual interfaces automatically with selected SD-WAN zone
- Save time and reduce service disruption
- Use the **Integrate Interface** feature on the **Interfaces** page:




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

Before adding an interface as an SD-WAN member, you must first remove any configuration references to the interface. This is fine if your configuration is simple, but if your configuration has many references, then the reference removal and addition process can be time consuming and disruptive to the network.

An alternative is to use the **Integrate Interface** feature available on the **Interfaces** page on the FortiGate GUI. When you use the integrate interface feature, you can instruct FortiGate to migrate an interface to SD-WAN. The result is that FortiGate automatically tries to replace the individual interface with the selected SD-WAN zone on every configuration object that references the interface. Note that if the change does not apply to a configuration node or FortiGate can't replace the reference, then FortiGate leaves the configuration node as is.

Note that this feature is particularly useful for companies transitioning to SD-WAN and who don't use FortiManager to manage their FortiGate devices. A typical use case is a single FortiGate used for local break out. You will see in another lesson how you can use FortiManager to manage FortiGate devices configured with SD-WAN.

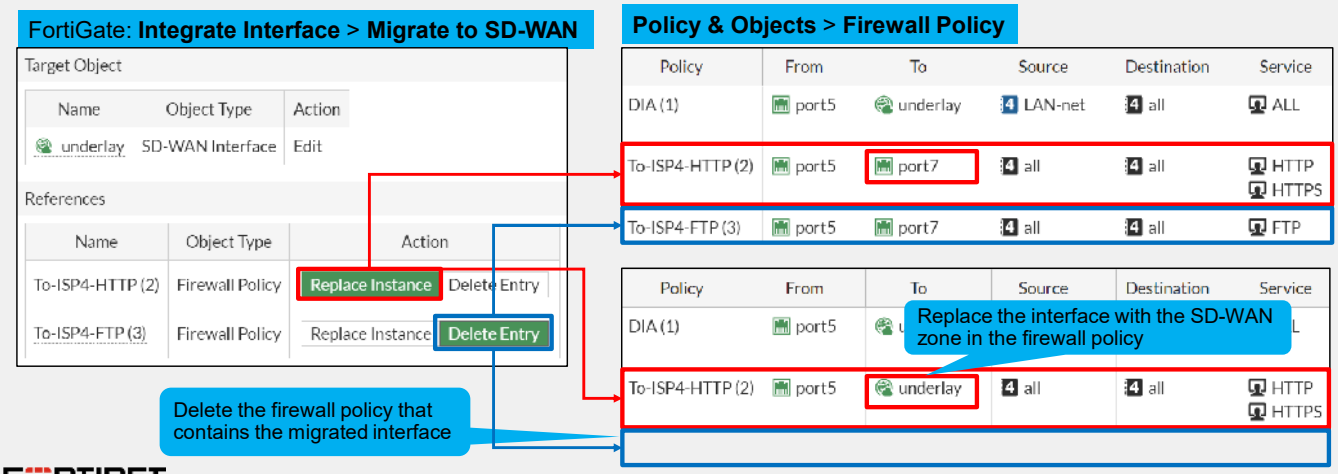


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Migrating Interfaces to SD-WAN—Firewall Policies

- What happens if the interface is used in a firewall policy?
  - FortiGate prompts the administrator with options for each policy:
    - **Replace Instance**: Replace the interface with the SD-WAN zone in the policy
    - **Delete Entry**: Delete the firewall policy




Remember that you cannot use SD-WAN members in firewall policies. You can use only SD-WAN zone and interfaces that are not SD-WAN members. What happens when you migrate an interface to an SD-WAN zone?

On interface migration, FortiGate prompts the administrator to select between two options:
- **Replace Instance**, which replaces the individual interface with the zone in the policy
- **Delete Entry**, which deletes the firewall policy that contains the migrated interface

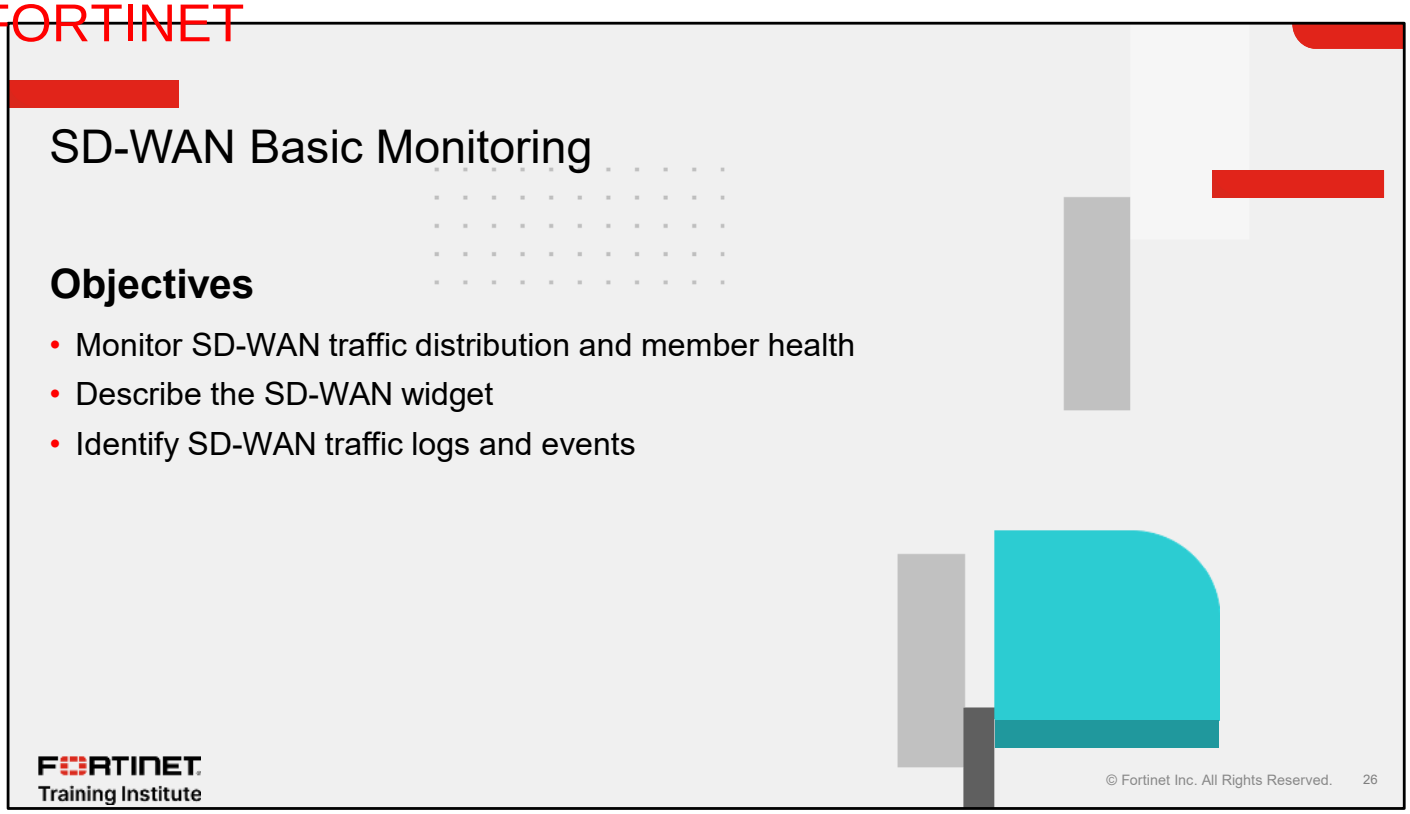
Note that when you select **Delete Entry**, FortiGate deletes the firewall policy, not just the migrated interface. The behavior is the same whether the policy contains one or multiple interfaces as the destination. In other words, FortiGate deletes the policy even if it contains destination interfaces that are not migrated to SD-WAN.

In the example shown on this slide, the administrator migrated an interface, **port7**, to the SD-WAN zone **underlay**. Before the migration, port7 was the destination interface of two policies—To-ISP4-HTTP(2) and To-ISP4-FTP(3). The administrator selects the action **Replace Instance** for policy ID 2 and the action **Delete Entry** for policy ID 3. Consequently, FortiGate replaces the destination on policy ID 2 and deletes the policy ID 3.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding basic monitoring of SD-WAN, you should be able to identify the different tools available on the FortiGate GUI to check SD-WAN traffic distribution, health, and events.

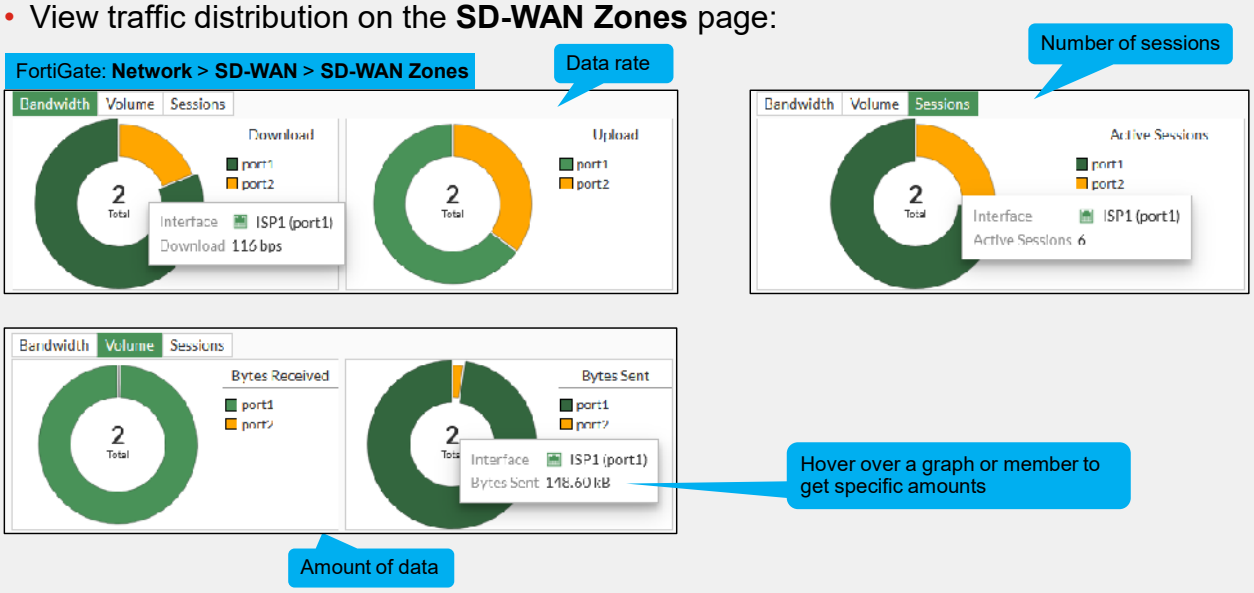


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Traffic Distribution

- View traffic distribution on the **SD-WAN Zones** page:




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

You can browse to the **SD-WAN Zones** page to monitor the traffic distribution over the SD-WAN members. The page contains graphs that display traffic distribution based on bandwidth, volume, or sessions. Note that bandwidth refers to the data rate, while volume refers to the quantity of data.

You can also hover over a member or the graph to display a specific amount of bandwidth, volume, or sessions. The example on this slide shows the corresponding traffic distribution graphs of the basic DIA setup.

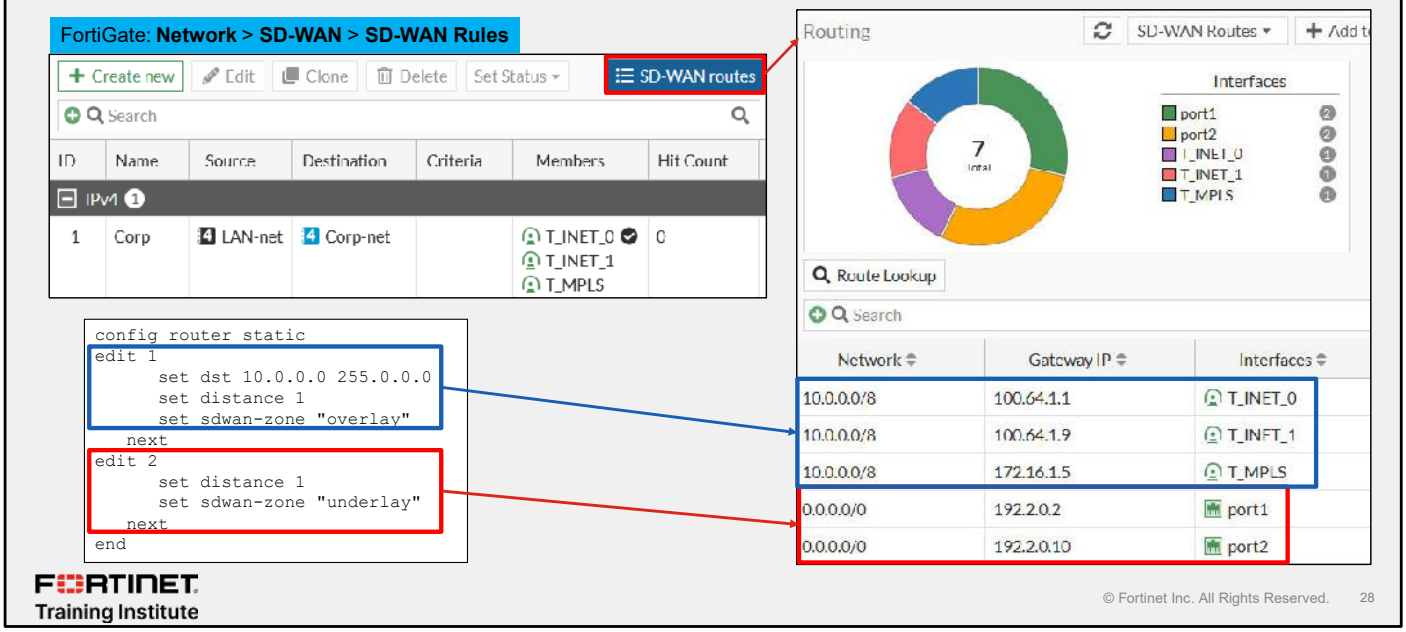


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# SD-WAN Routes

- View routes associated with SD-WAN members on the **SD-WAN Rules** page:




On the **SD-WAN Rules** page, you can directly access the **SD-WAN routes** page. This page displays details about the static routes defined per SD-WAN zone, with gateway IP address and outgoing interfaces for each member in the zone.

The example on this slide shows the routes corresponding to an SD-WAN configuration with two zones, overlay and underlay, three IPsec interface members in the first zone and two physical interface members in the second.

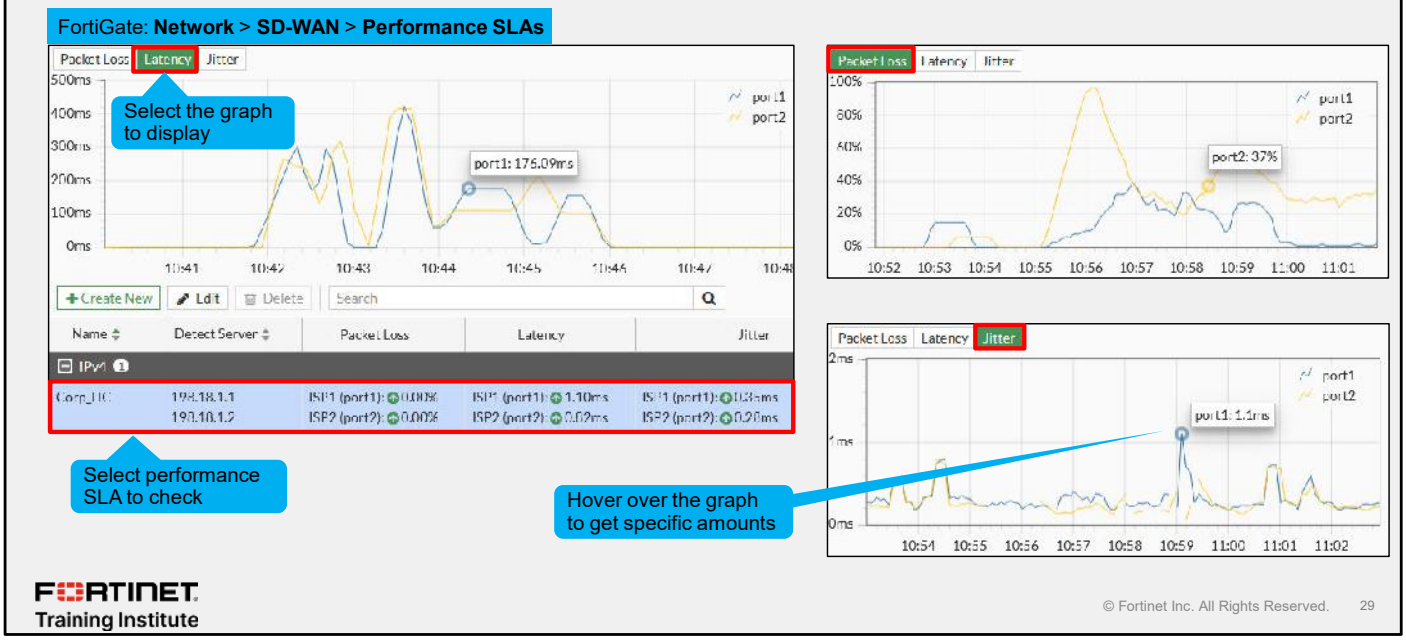


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Member Health

- View member health on the **Performance SLAs** page (last 10 minutes):




You can browse to the **Performance SLAs** page to monitor the health of your members.

You first select the performance SLA you want to check (Corp_HC in the example). The graphs on the page then display the packet loss, latency, and jitter of each member using the selected performance SLA. Note that the information shown in the graphs is limited to the last 10 minutes.

You can also hover over the graph to display a specific amount of packet loss, latency, or jitter. The example on this slide shows the corresponding health graphs for the two members used in the basic DIA setup.

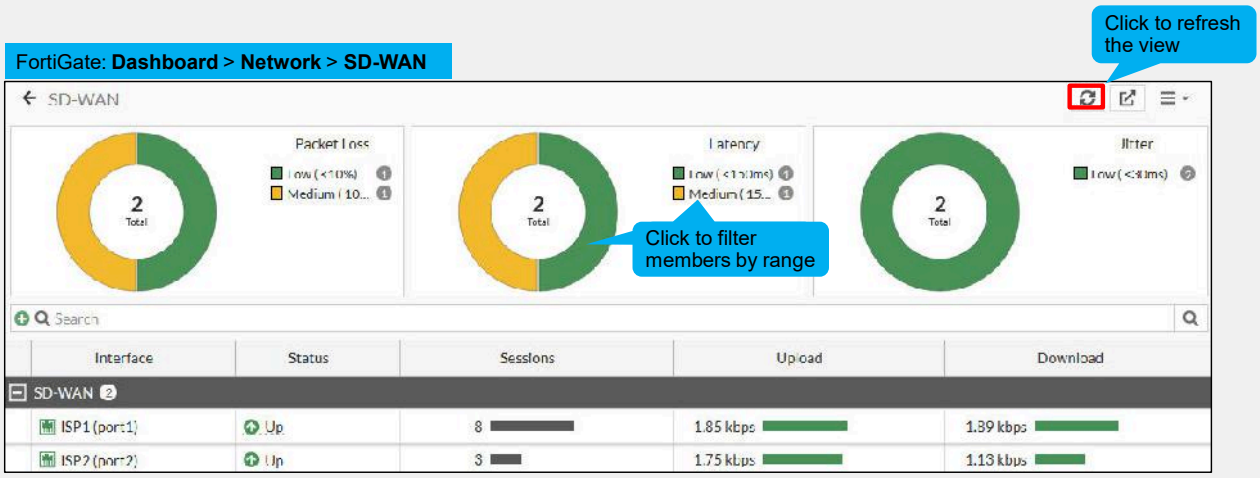


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# SD-WAN Widget

- Consolidated view of member health and use




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

The SD-WAN widget offers a consolidated view of both the health of a member and its use. The example on this slide shows two SD-WAN members configured: port1 and port2.

The graphs on the page summarize the health of the alive members and indicate how many of them fall within some predefined ranges of packet loss, latency, and jitter. The example shows that packet loss on port2 is within the low range, and its packet loss and latency are within the medium range. You can click a range to display the list of members that fall within that range.

Note that the SD-WAN widget view does not refresh automatically—you can use the refresh button to update the display.

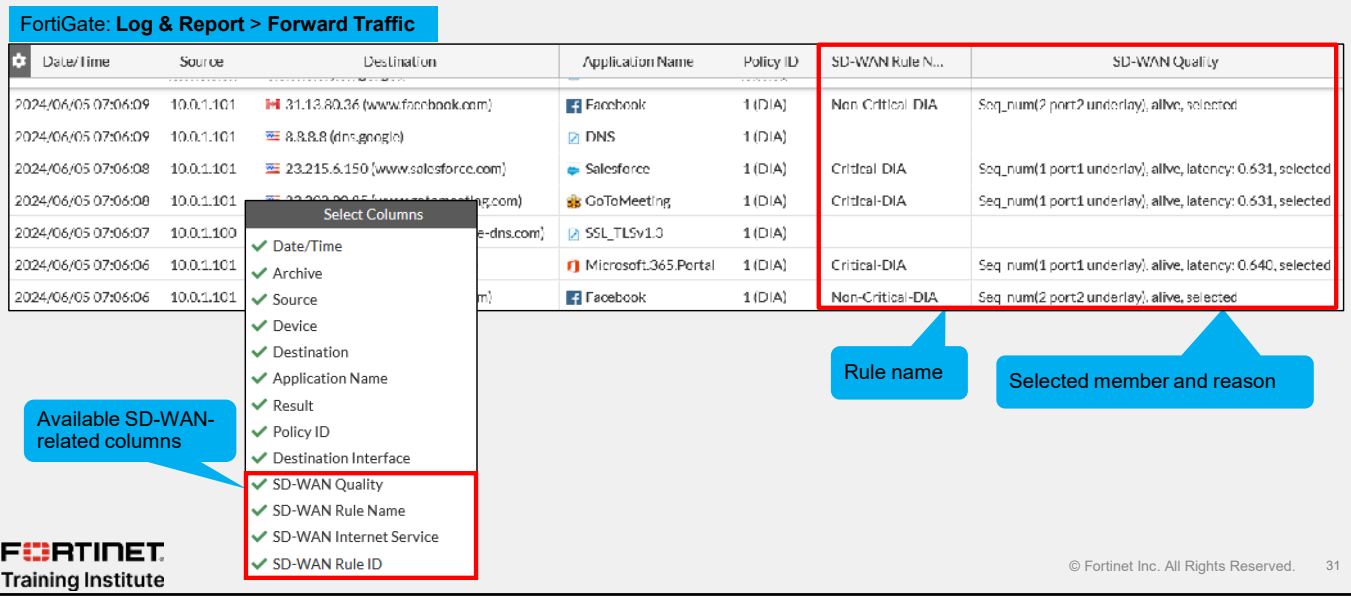


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Traffic Logs

- Enable SD-WAN columns to view SD-WAN-related information




The **Forward Traffic** logs page is useful to identify how sessions are distributed in SD-WAN and the reason. Make sure to enable the **SD-WAN Rule Name** and **SD-WAN Quality** columns, which are disabled by default. The former indicates the matched SD-WAN rule for a session, and the latter the member the session was steered to and the reason.

The table on this slide shows multiple sessions. FortiGate identified the first session in the table as a **Facebook** application, matched the **Non-Critical-DIA** rule, and sent it to port2. The **Non-Critical-DIA** rule instructs FortiGate to steer matching traffic to port2 only, provided the port is alive. This behavior matches the reason described in the **SD-WAN Quality** column for that session.

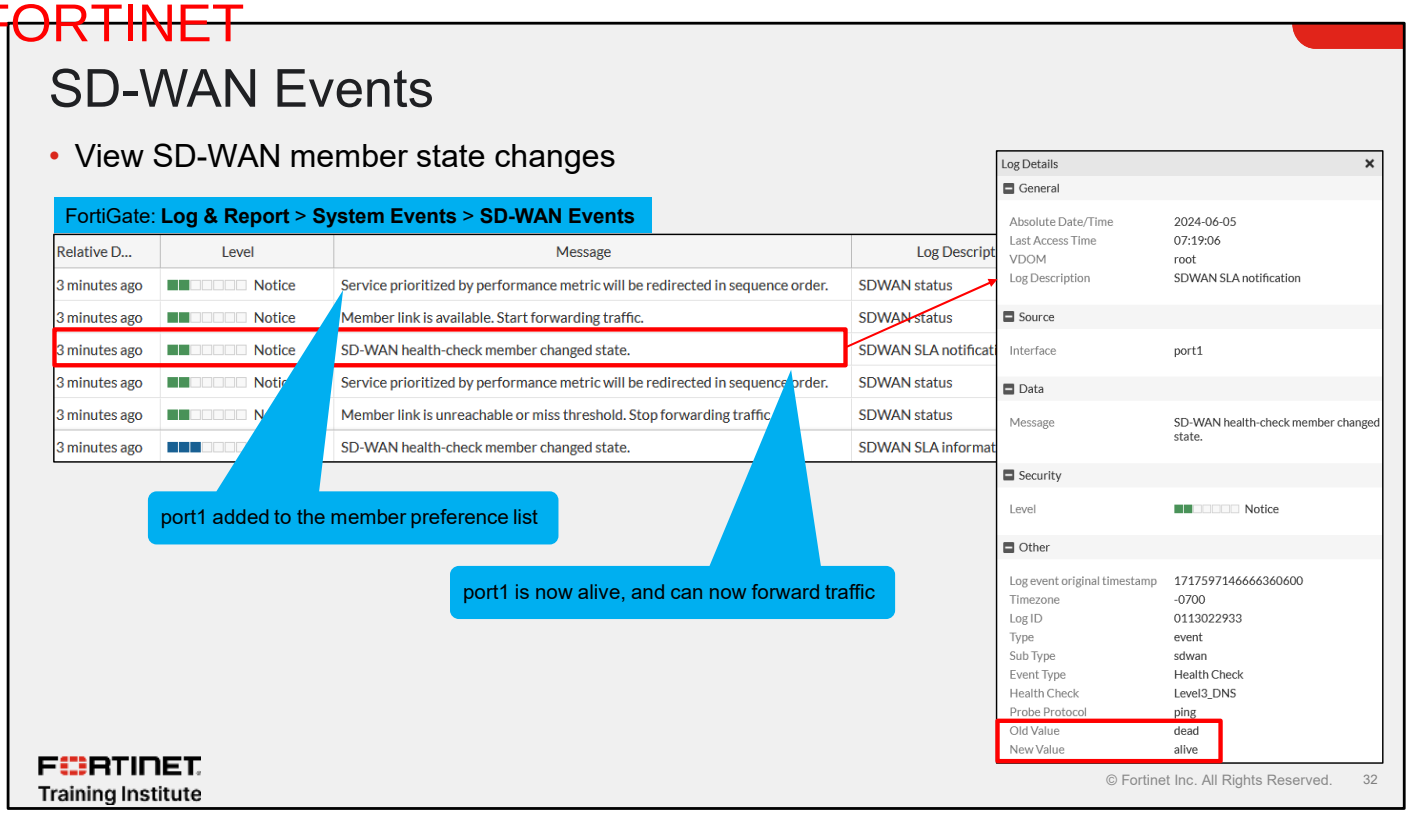
The second line reports a DNS session that doesn't match any SD-WAN rule—the SD-WAN fields are empty.

FortiGate identified the third session in the table as a **Salesforce** application, matched the **Critical-DIA** rule, and sent it to port1. The reason that FortiGate selected port1 was because it had the lowest latency.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




The **SD-WAN Events** subsection on the **System Events** page displays logs that report the state changes of SD-WAN members.

In most cases, you must click a log to fully understand the event. For example, the third log in the table indicates that the state of **port1** changed from **dead** to **alive**. Although the details of the second and first logs are not shown, the logs report that port1 is ready to forward traffic, and that the member preference in the rule that uses port1 (**Critical-DIA**) was updated to include port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe SD-WAN
- ✓ Identify architecture components and use cases
- ✓ Introduce SD-WAN main components: members, zones, and rules
- ✓ Configure a basic SD-WAN DIA setup using the FortiGate GUI
- ✓ Monitor SD-WAN traffic distribution, member health, and events using the FortiGate GUI
- ✓ Identify SD-WAN traffic logs and events

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

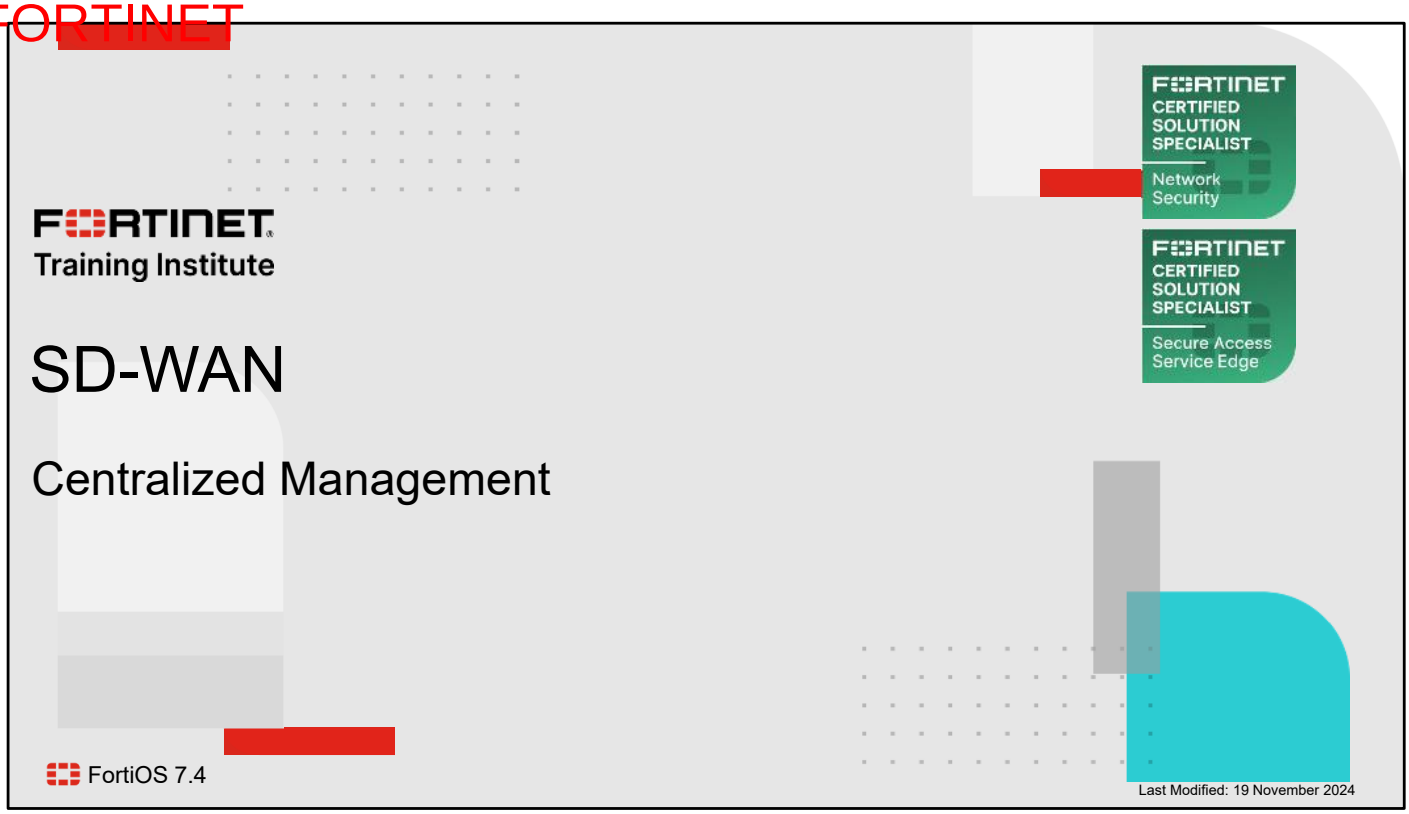
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned the most common use cases for SD-WAN, its main components, and how to configure and monitor a basic SD-WAN DIA setup.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

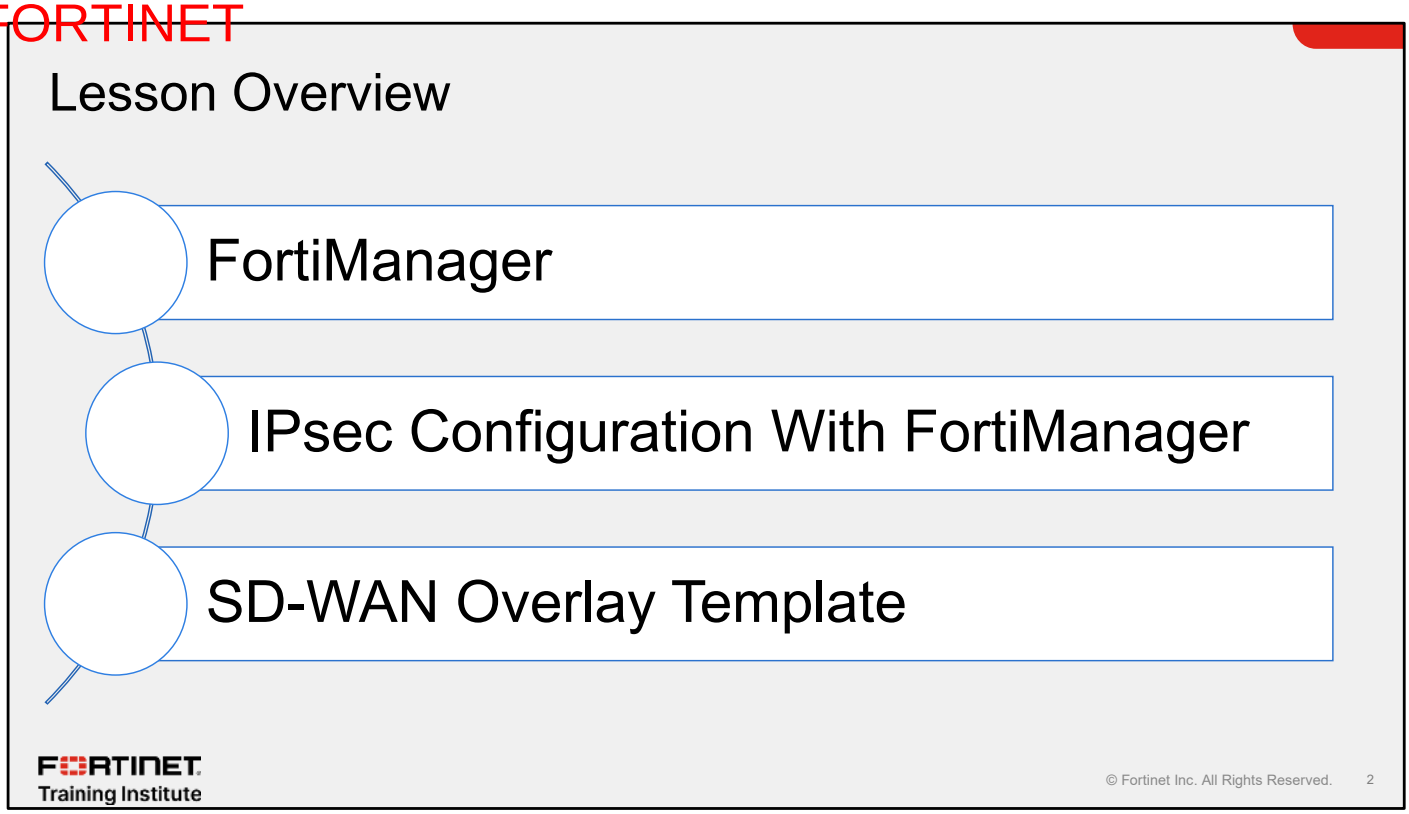



In this lesson, you will learn how FortiManager can help to deploy and maintain SD-WAN networks.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

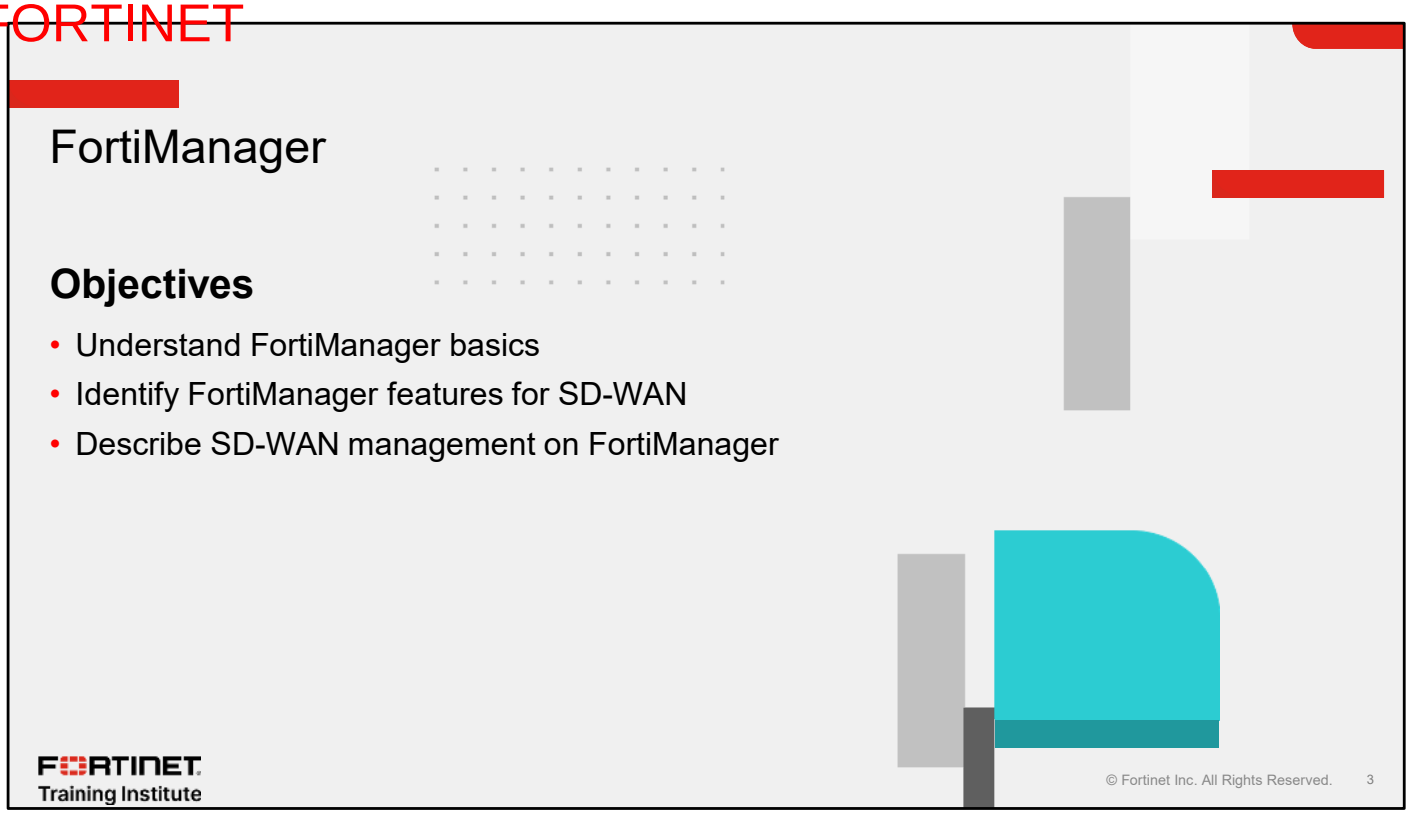



In this lesson, you will learn about the topics shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding how to deploy SD-WAN using FortiManager, you should be able to leverage the centralized features of FortiManager to reduce operation costs when deploying and maintaining SD-WAN across a large network.

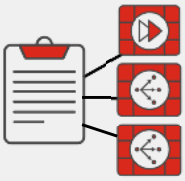


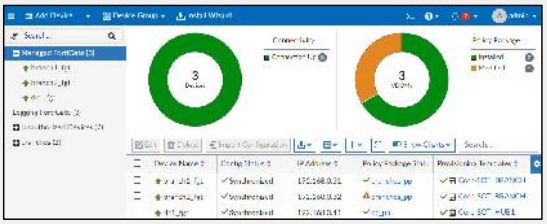
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## What Is FortiManager?

- Provides centralized management for SD-WAN
  - Single-pane-of-glass management





- Benefits for SD-WAN:
  - Provisioning of SD-WAN templates, CLI templates, and firewall policies across multiple devices
  - Per-device SD-WAN configuration support
  - SD-WAN status monitoring
  - Central repository for configuration revision control and security audits
  - Deploying and monitoring complex IPsec VPN topologies (IPsec overlays)
  - Guided SD-WAN overlay tunnels and BGP route deployment with SD-WAN overlay templates
  - Zero-touch provisioning for new SD-WAN sites
  - Support for scripts and JSON APIs to automate device provisioning and perform policy changes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

FortiManager is a key component for deploying SD-WAN across a large network. Centralized (single-pane-of-glass) management through FortiManager can help you more easily manage SD-WAN deployment across many devices and reduce the cost of operation.

How can FortiManager help you with your SD-WAN deployment?

- Provision SD-WAN templates, CLI templates, and firewall policies across multiple devices with the same configuration requirements.
- Enable you to configure SD-WAN on a per-device basis.
- Monitor SD-WAN status.
- Act as a central repository for configuration revision control and security audits.
- Deploy and monitor complex IPsec VPN topologies (IPsec overlays).
- Guide SD-WAN overlay tunnels and BGP route deployment with SD-WAN overlay templates.
- Perform zero-touch provisioning for new SD-WAN sites.
- Use scripts and JSON APIs to automate device provisioning and perform policy changes for SD-WAN.

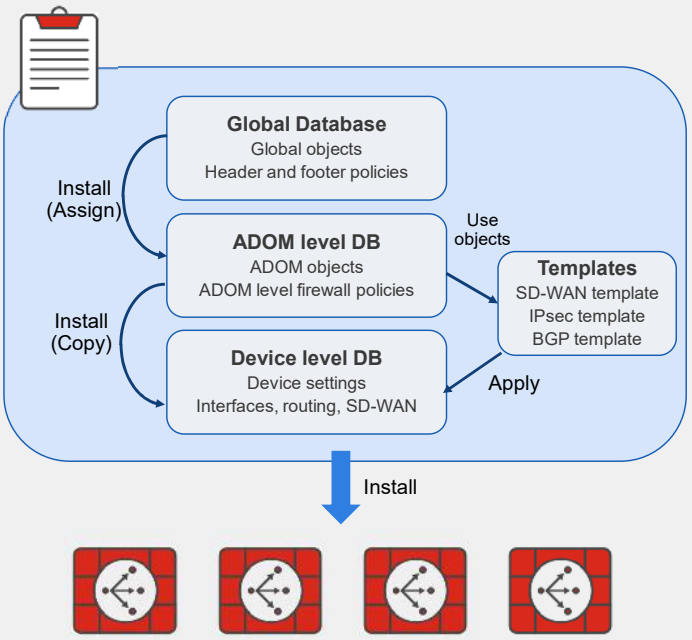


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Management Layers

- Global Database
  - Global objects
  - All header and footer policies
- ADOM layer
  - Common object database, devices, device groups, policy packages
  - Groups of devices sharing common objects
  - Default ADOM: root
- Device Manager layer
  - Name and type of managed devices, their IP addresses, revision history, and real-time status




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

To organize and efficiently manage a large-scale network, FortiManager has multiple management layers.

The global ADOM layer has two key pieces: the global object database and header and footer policy packages. Header and footer policy packages envelop the policies for each ADOM. Policy packages are often used in a carrier environment, where the carrier allows customer traffic to pass through their network but doesn't allow the customer to have access to their network infrastructure.

The ADOM layer is where policy packages are created, managed, and installed on managed devices or device groups. You can create multiple policy packages here. The ADOM layer includes one common object database for each ADOM. The common object database contains information, such as addresses, services, and security profiles. ADOMs enable you to create groupings of devices for administrators to monitor and manage. The purpose of ADOMs is to divide administration of devices by ADOM and to control (restrict) administrator access.

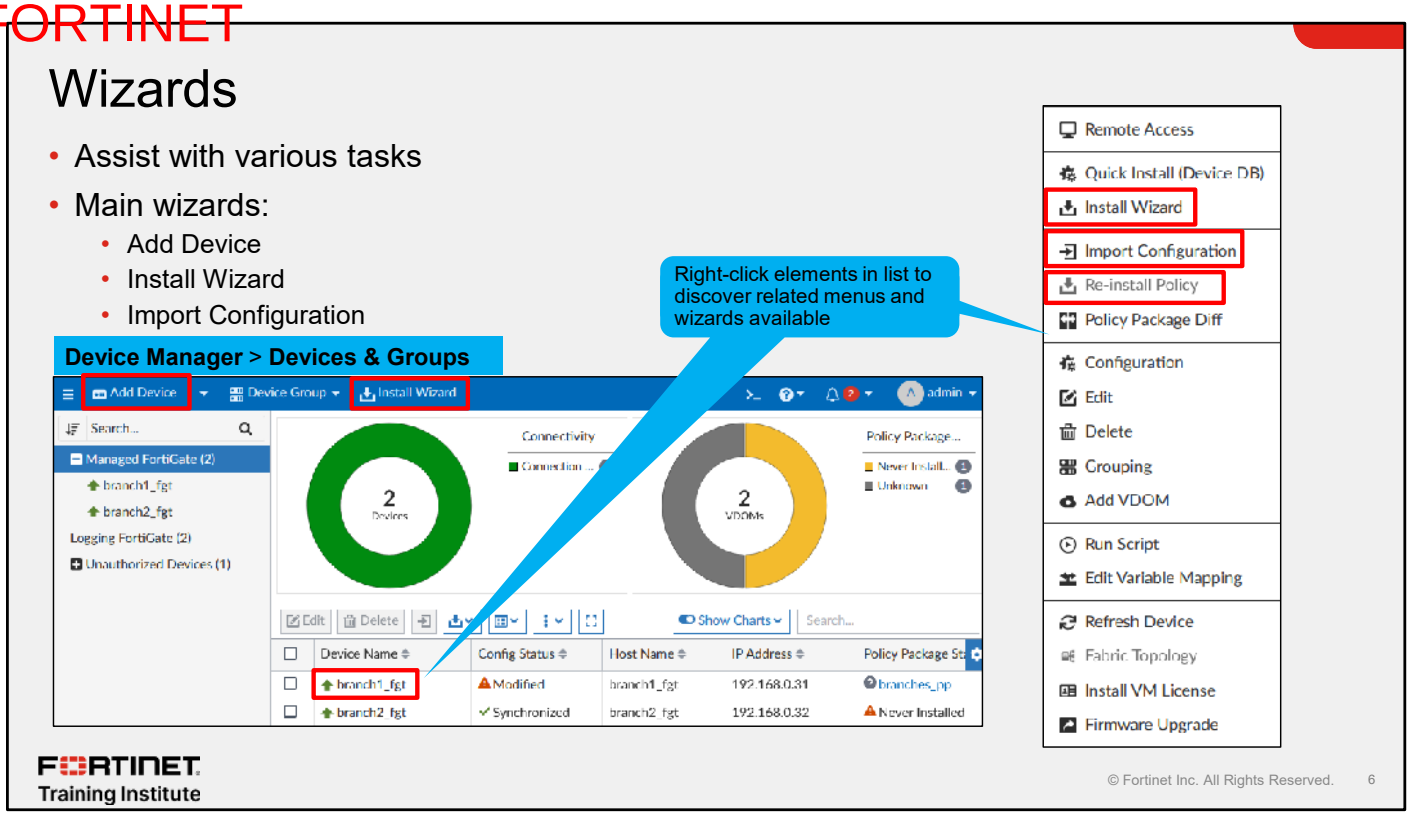
The Device Manager layer records information on devices that are centrally managed by the FortiManager device, such as the name of the device, type of device, model, IP address, current firmware installed, revision history, and real-time status.

The diagram on this slide presents a high-level overview of the FortiManager databases. Note that FortiManager can install configuration changes on a single FortiGate device or on multiple devices simultaneously.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




The **Device Manager** pane provides device and installation wizards to aid you in various administrative and maintenance tasks. Using these wizards can decrease the amount of time it takes to do many common tasks.

There are four main wizards on the **Device Manager** pane:

- Use **Add Device** to add devices to central management and import their configurations.
- Use **Install Wizard** to install configuration changes from the **Device Manager** pane or the **Policies & Objects** pane to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.
- Use **Import Configuration** to import interface mappings, policy databases, and objects associated with the managed devices into a policy package on the **Policy & Object** page. It runs with the **Add Device** wizard, by default, and you can run it at any time from the managed device list.
- Use **Re-install Policy** to perform a quick installation of the policy package. It provides the ability to preview the changes that will be installed on the managed device.

You can open the **Import Configuration** and **Re-install Policy** wizards by right-clicking your managed device in the **Device Manager**.

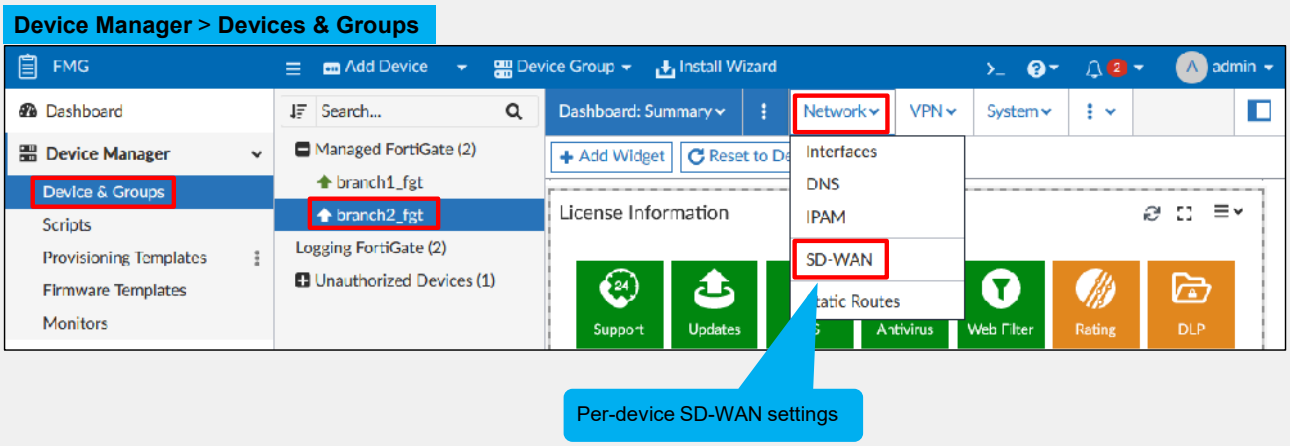


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Management—Per Device

- Apply settings on individual devices
- Devices have different SD-WAN requirements
- SD-WAN objects stored in device settings database




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

FortiManager offers two approaches for configuring SD-WAN: per-device management and central management.

In per-device management, you configure SD-WAN settings for individual devices. You make configuration changes on the SD-WAN page of the managed device, and then install them. The per-device management approach is useful when your devices have different SD-WAN configuration requirements and, therefore, you must maintain separate settings for each device.

The screenshots on this slide show the FortiManager pages where you apply per-device SD-WAN settings. On the **Device Manager** pane, click the managed device and, in the **Network** menu, select **SD-WAN** to access the per-device SD-WAN settings.

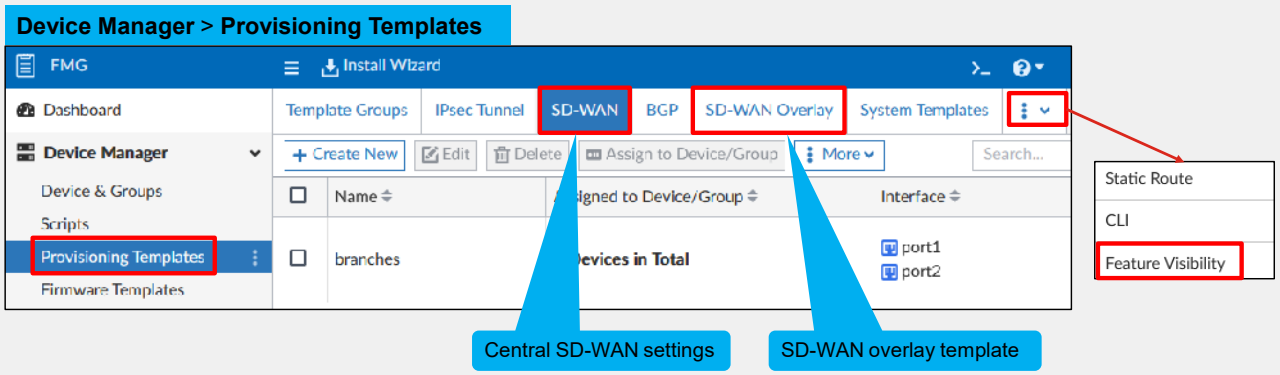


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Management—Central Management

- Apply templates on multiple devices
- Devices have the same SD-WAN requirements
- SD-WAN objects stored in the ADOM database




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

In a central management approach, you configure SD-WAN templates and assign them to one or more FortiGate devices. For each SD-WAN template, you define SD-WAN members, zones, performance SLAs, rules, and so on. This approach is convenient for deploying multiple devices that use similar configurations because it reduces the administrative overhead. That is, instead of applying a change on each managed device, you apply it on the shared template. Then, when you install the template changes, FortiManager pushes the change to all the target devices of the template.

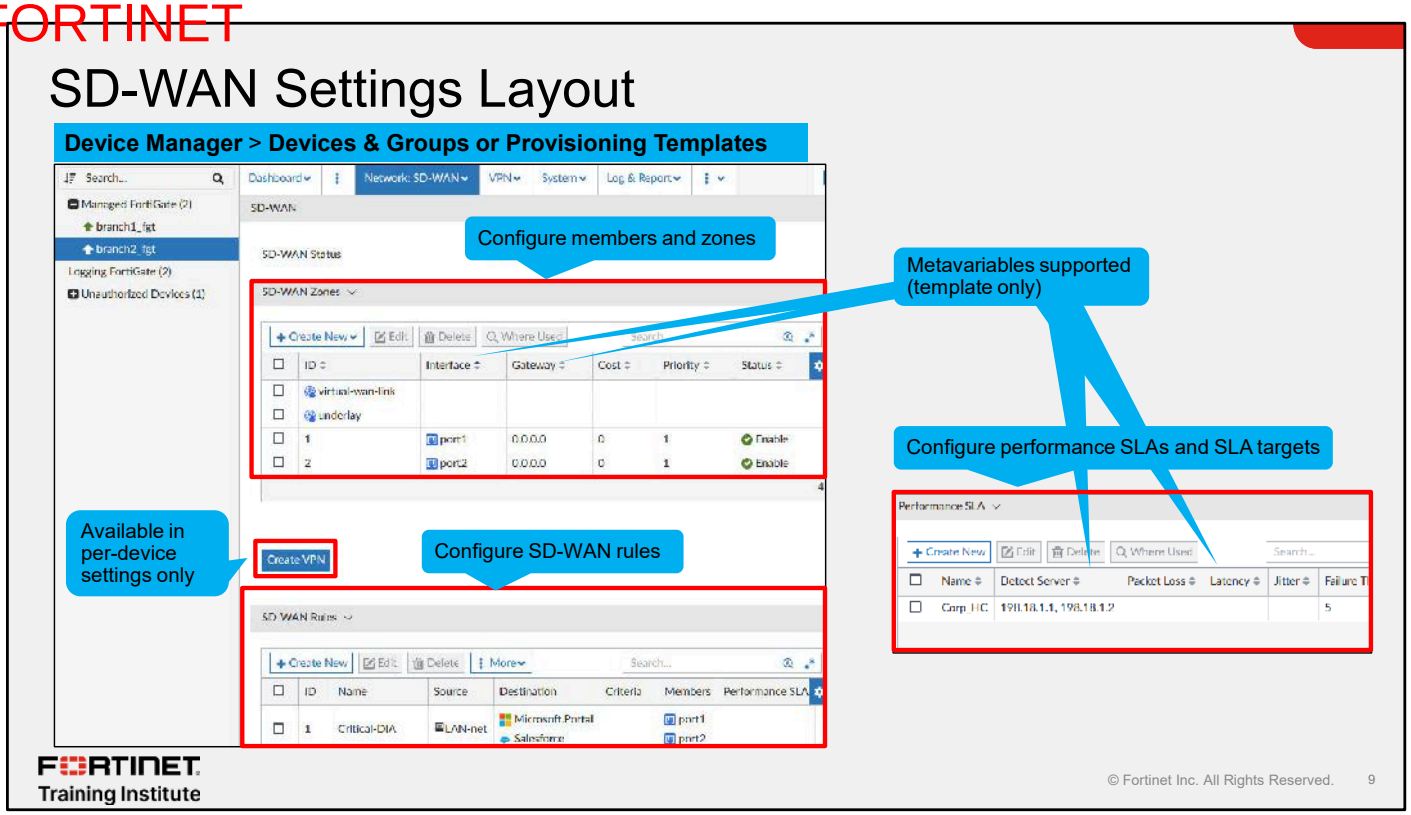
The screenshots on this slide show the FortiManager pages where you define central SD-WAN settings. You can find the SD-WAN central settings in the **Provisioning Templates** section on the **Device Manager** page. Note that the **SD-WAN Overlay** template tab is not visible by default. You can activate its display from the feature visibility menu.

The SD-WAN overlay template combines, in a guided approach, configuration of SD-WAN, IPsec overlay, and ADVPN templates. You will learn more about the SD-WAN overlay templates in this lesson.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




Whether you configure SD-WAN using per-device management or central management, the FortiManager pages for both approaches look almost the same. One difference is that the per-device settings page shows the **Create VPN** button, which enables you to quickly create an IPsec tunnel that can later be added as an SD-WAN member.

Another difference is that when you configure an SD-WAN member using an SD-WAN template (central management), you can use metadata variables in the **Interface Member**, **Gateway**, and **Health-Check Server** settings. Metadata variables enable you to define variables that can be assigned with different values per device. You will learn more about metadata variables in this lesson.

The way you configure SD-WAN settings using FortiManager is very similar to how you configure them on the FortiGate GUI. This slide shows an example of a configuration made using per-device management. Like FortiGate, there are three sections available on the GUI: **Interface Members**, **Performance SLA**, and **SD-WAN Rules**, and they serve the same purpose as on the FortiGate GUI.

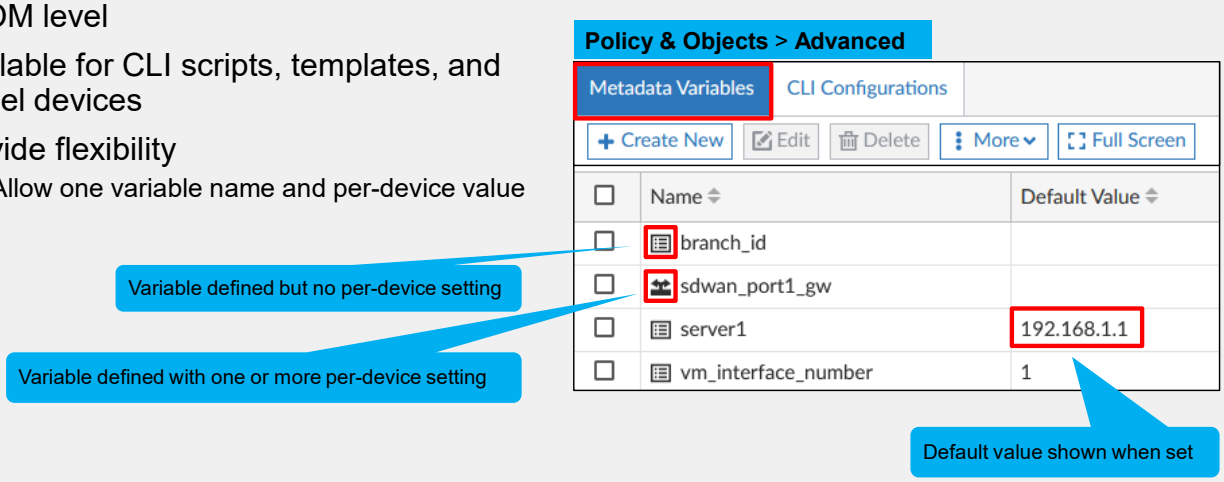


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Metadata Variables

- ADOM level
- Available for CLI scripts, templates, and model devices
- Provide flexibility
  - Allow one variable name and per-device value




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

Metadata variables are ADOM-level parameters—also available for Global ADOM for per-ADOM mapping. You can use metadata variables in CLI scripts, templates, or model devices. They provide required flexibility each time a parameter has different values on each devices.

You can access the **Metadata Variables** menu under **Policy & Objects** > **Advanced** to review, edit, and create metadata variables.

The metadata variable name can contain only letters, numbers, and underscores.

On upgrade from version 7.0 or earlier, FortiManager creates metadata variables at the ADOM level for metafields used in the ADOM.

If a metafield contains characters unsupported for metadata variable names, the name is modified, and every unsupported character is replaced with an underscore "_".

System-level metafields are kept on upgrade for reference. They remain visible under **System Settings** > **Advanced** > **Meta Fields**.

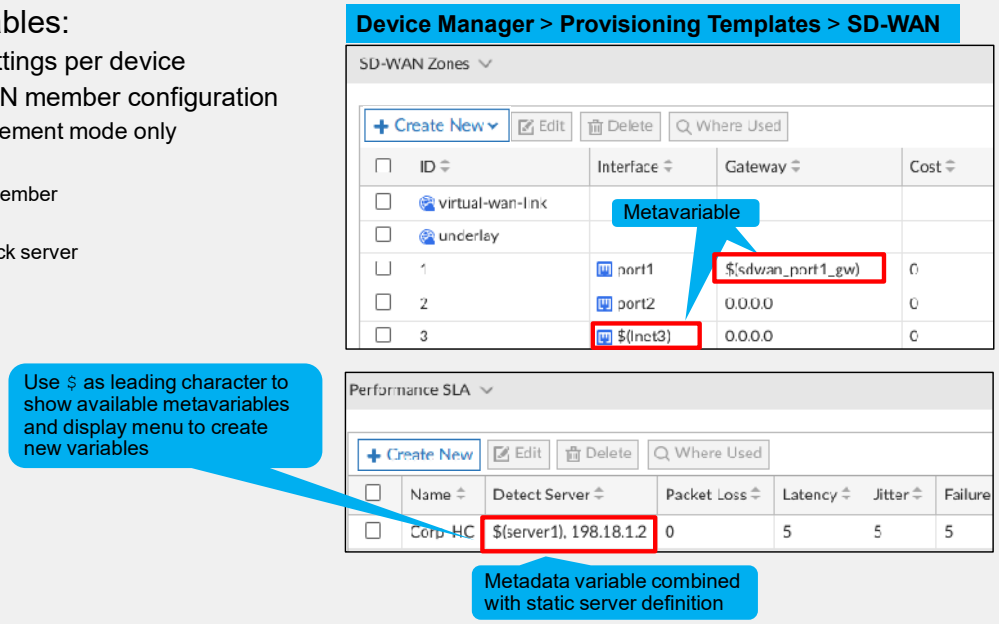


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Metadata Variables for SD-WAN Members

- User-defined variables:
  - Apply different settings per device
  - Useful for SD-WAN member configuration
    - Central management mode only
    - Available for
      - Interface member
      - Gateway
      - Health check server




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

The FortiManager metadata variables are user-defined variables that enable you to assign different values to a setting for a given device. They are particularly useful when you configure SD-WAN members using SD-WAN templates.

You can use metadata for the **Interface Member** setting. This allows you to use different interfaces on different devices without having to create separate templates. Another use case for metadata is the gateway setting of SD-WAN members. Even if you use the same interface name for the devices assigned to a template, their gateway is likely to differ. For this reason, you can define a metadata variable for the gateway setting that indicates the gateway IP address to push to the member on each device.

The example on this slide shows the use of two metadata variables for SD-WAN member configuration. The **sdwan_port1_gw** metadata variable is used to define a different gateway for **port1** on each managed device. That is, the gateway for **port1** on **branch1_fgt** and **branch2_fgt** will be `192.2.0.2` and `203.0.113.2`, respectively. For member ID **3** in the **underlay** zone, the **inet3** metadata variable is used to indicate the name of the interface to use as the member on each managed device. That is, **branch1_fgt** will use **port3** as the member, and **branch2_fgt** will use **port8**.

In **Performance SLA** section, health check servers for the Corp_HC entry are defined with one static server IP address, the same IP address for every device, and one metadata variable to adjust the health check server IP address according to device location.

To reference a metadata variable in the SD-WAN member configuration, type `$` at the beginning of the string so FortiManager shows a list of available metadata variables. On this pop-up menu, a "**+**" sign allows the user to create a new metadata variable, if required.

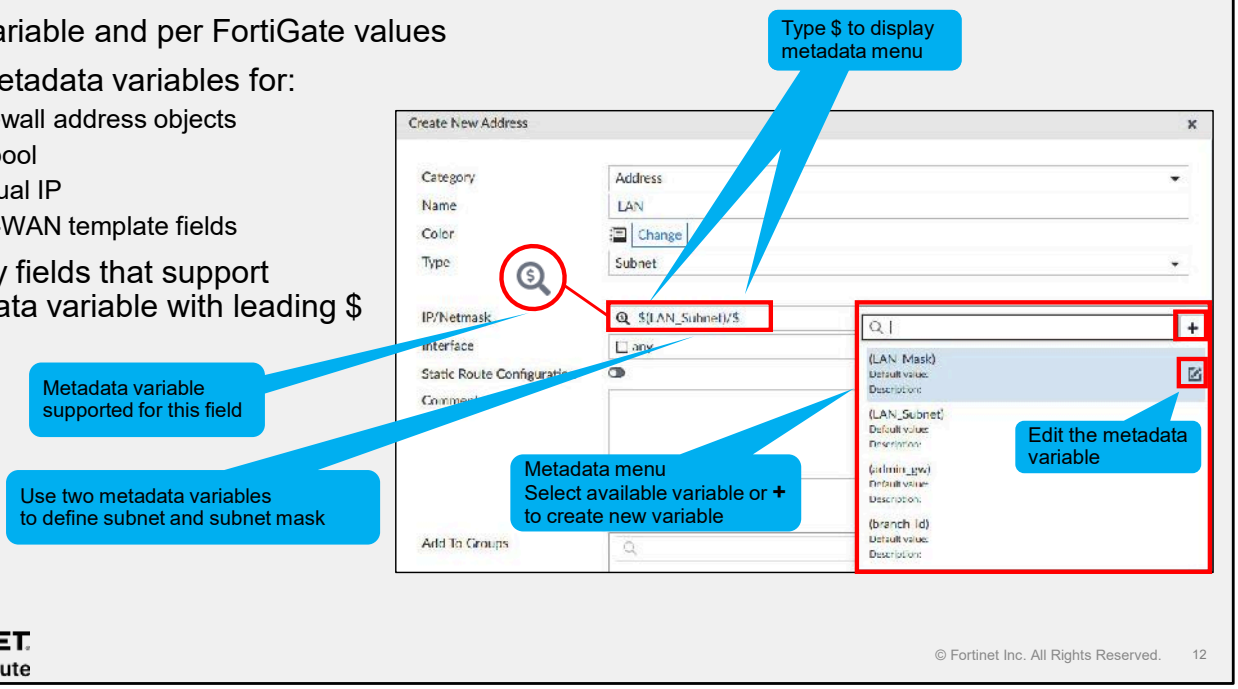


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Metadata Variables Uses

- One variable and per FortiGate values
- Use metadata variables for:
  - Firewall address objects
  - IP pool
  - Virtual IP
  - SD-WAN template fields
- Identify fields that support metadata variable with leading $




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

The magnifying glass with a $ sign indicates fields where you can use a metadata variable.

In the example shown on this slide, the user can enter the IP address and netmask as usual, or enter $ to display the metadata variable menu and select one metadata variable for the subnet and one metadata variable for the subnet mask.

Note that for fields **IP/Netmask**, it's mandatory to specify the IP subnet and the subnet mask separately. Valid options are:

- `Two metadata variables: $(LAN_Subnet)/$(LAN_Mask)`
- `One metadata variable and one user defined, fixed value: $(LAN_Subnet)/255.255.255.0`
- `Two user define values: 10.10.10.0/255.255.255.0`

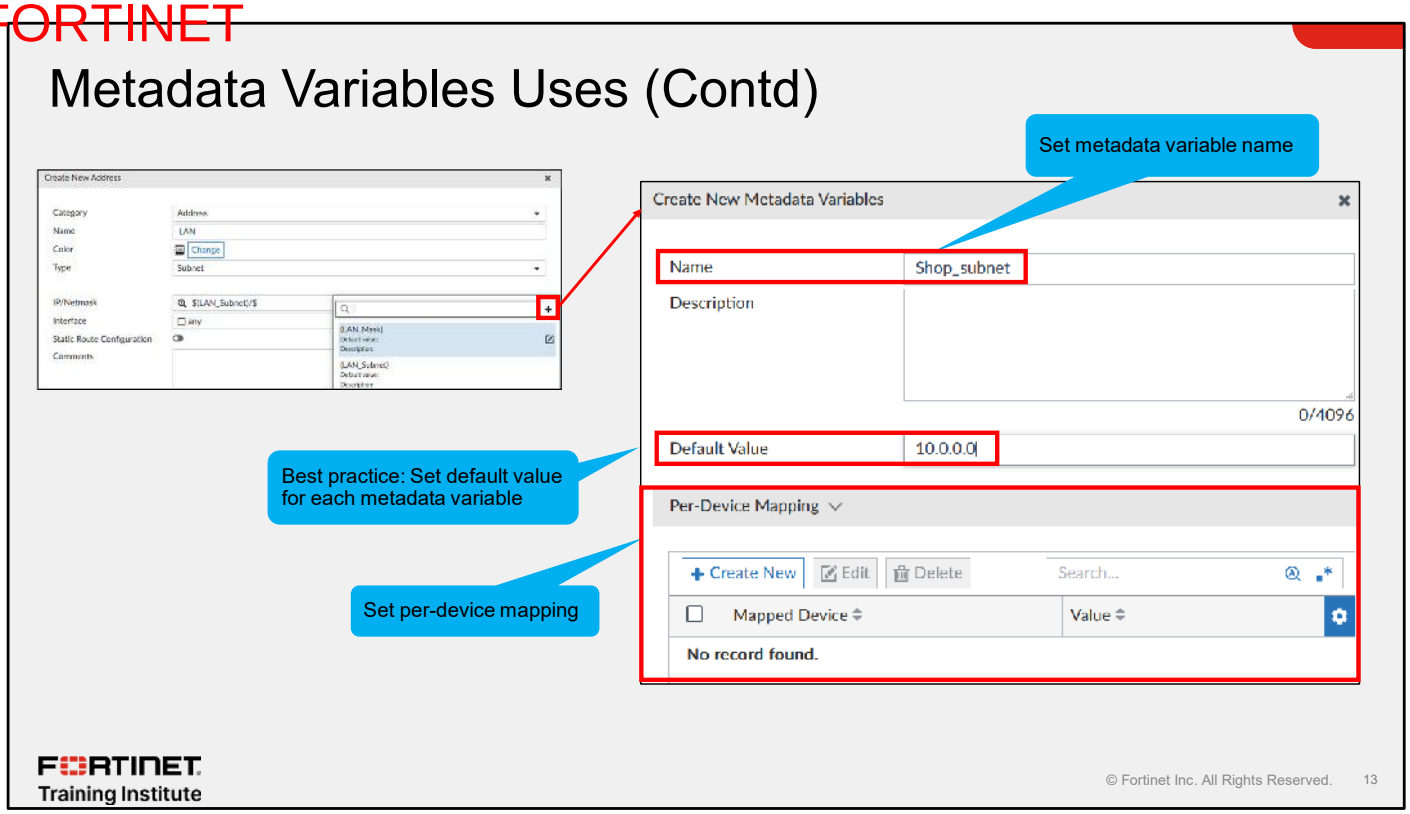
After you enter the $ sign in a field, a pop-up menu allows you to select a previously defined variable. You can create a new variable by clicking **+**, or edit an existing metadata variable by clicking the pen icon displayed when you hover over a variable.

To review and edit all metadata variables at the ADOM level, click **Policy & Objects** > **Advanced** > **Metadata Variables**.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




If you click **+** to create a new metadata variable, FortiManager shows a window where you can create a new variable and its per-device mapping. You can then define the variable name and its values.

It's a good practice to set a default value for each metadata variable you create. FortiManager uses the default value when installing the configuration on each FortiGate for which you didn't specify a per-device mapping. You can expand the **Per-Device Mapping** menu to set specific values for each mapped device.

Note that it's important to configure a default value or a mapping for each device to which the metadata variable applies. FortiManager cannot install a configuration that contains commands that use metadata variables for which it has no value for a device—default or per-device mapping.



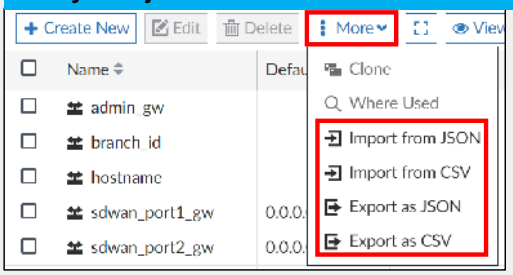
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Import and Export Metadata Variable Definitions

- Import metadata variables
  - Available formats : CSV, JSON
  - Allows
    - Easy provisioning of values for each managed device
    - Definition of new metadata variables

**Policy & Objects > Advanced > Metadata Variables**




- Export metadata variables
  - Available formats : CSV, JSON
  - Allows easy review of defined values
  - Can be used as a basis for files to import

- Example of CSV export file:

```
variable_name,default_value,description,device,VDOM,mapped_value
admin_gw,,,branch1_fgt,root,172.16.0.2
admin_gw,,,branch2_fgt,root,172.16.0.10
branch_id,,,branch1_fgt,root,1
branch_id,,,branch2_fgt,root,2
hostname,,,branch1_fgt,,branch1_fgt
hostname,,,branch2_fgt,,branch2_fgt
hostname,,,dc1_fgt,,dc1_fgt
```

- Example of JSON export file:

```
{ "adom": "root", "variables": [ { "name": "admin_gw", "mapping":
[ { "device": "branch1_fgt", "vdom": "root", "value":
"172.16.0.2" }, { "device": "branch2_fgt", "vdom": "root", "value":
"172.16.0.10" } ] }, { "name": "branch_id", "mapping": [ { "device":
"branch1_fgt", "vdom": "root", "value": "1" }, { "device": "branch2
_fgt", "vdom": "root", "value": "2" } ] }, { "name": "hostname",
"mapping": [ { "device": "branch1_fgt", "vdom": "", "value":
"branch1_fgt" }, { "device": "branch2_fgt", "vdom": "", "value":
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

When you define metadata variables for your managed device configuration, populating the value for each variable and each managed device from the FortiManager GUI can be tedious work for a large network. To help with this task, administrators can use the metadata variable import and export features.

The export feature displays a list of each metadata variable defined on FortiManager and the value defined for each device. With the import feature, you define the metadata variable values for each managed device and define new metadata variables.

The import and export features are compatible with CSV and JSON formats to accommodate various needs, such as manual or script value provisioning.



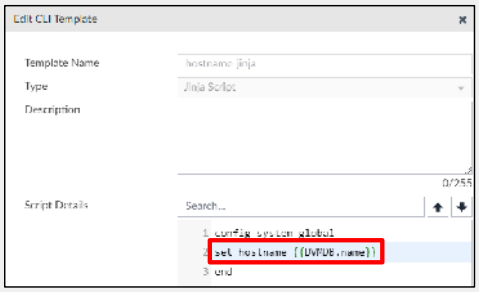
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Device Database Variables in Jinja Templates

- Alternative to metadata variables
- Natively available on FortiManager
- Available for Jinja scripts only
- Not compatible with CLI scripts

- Example of Jinja script with `DVMDB` variable:




| Device Database variables |
|---|
| Name: `{{DVMDB.name}}` |
| Serial: `{{DVMDB.serial}}` |
| OS type: `{{DVMDB.os_type}}` |
| Platform: `{{DVMDB.platform}}` |
| Version: `{{DVMDB.version}}` |
| Hostname: `{{DVMDB.hostname}}` |
| Description: `{{DVMDB.description}}` |

| System interface variables |
|---|
| Interface name: `{{intf.name}}` |
| Interface allow access: `{{intf.allowaccess}}` |
| Interface type: `{{intf.type}}` |
| Interface IP: `{{intf.ip}}` |
| Interface mode: `{{intf.mode}}` |
| Interface VDOM: `{{intf.vdom}}` |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

Device database variables are natively available on FortiManager for each managed device. Jinja templates and scripts have direct access to these variable to support the generation of dynamic configurations. Therefore, the administrator doesn't need to define metadata variables that would duplicate the device database variables.

This slide shows an example of a Jinja script that uses the variable `DVMDB.name` to define the device host name. It also shows examples of variables that you can use in Jinja scripts. Refer to the *FortiManager Administration Guide* to get the complete list of supported variables.

Note that when you prepare a script on the FortiManager GUI and type `{{`, FortiManager displays only the list of metadata variables. To use variables from the device database, you must type them.

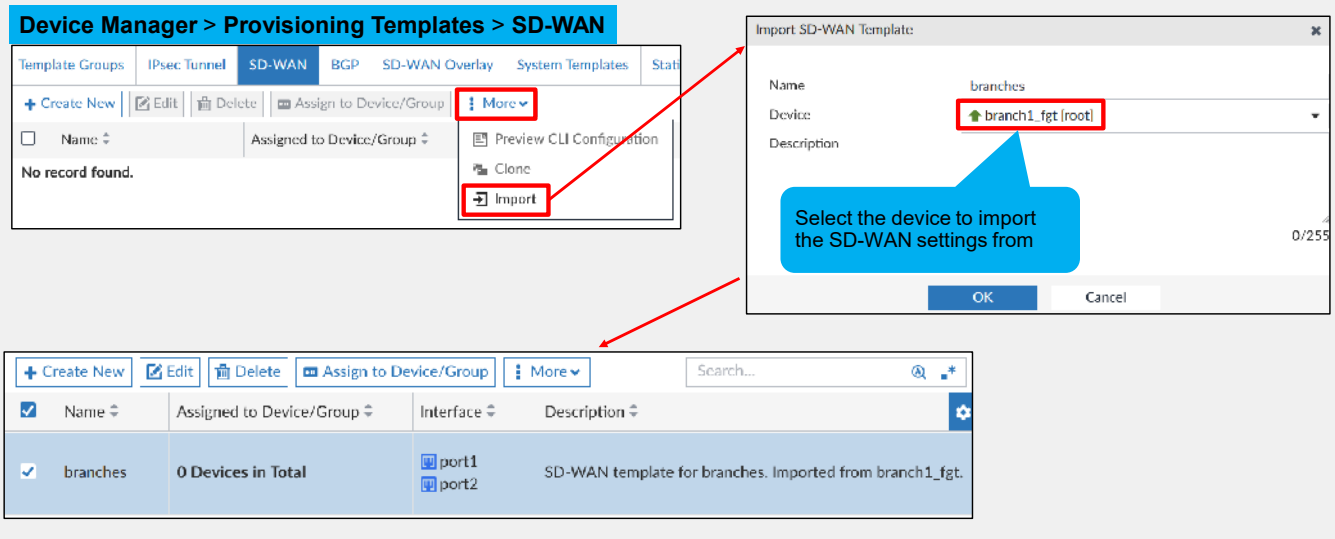


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Central Management—Importing Template Settings

- Importing SD-WAN settings from a managed device into a new template:







FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

For SD-WAN central management, you can import the SD-WAN settings of a device into an SD-WAN template in FortiManager. You can then use the template to deploy SD-WAN on other FortiGate devices that require the same configuration.

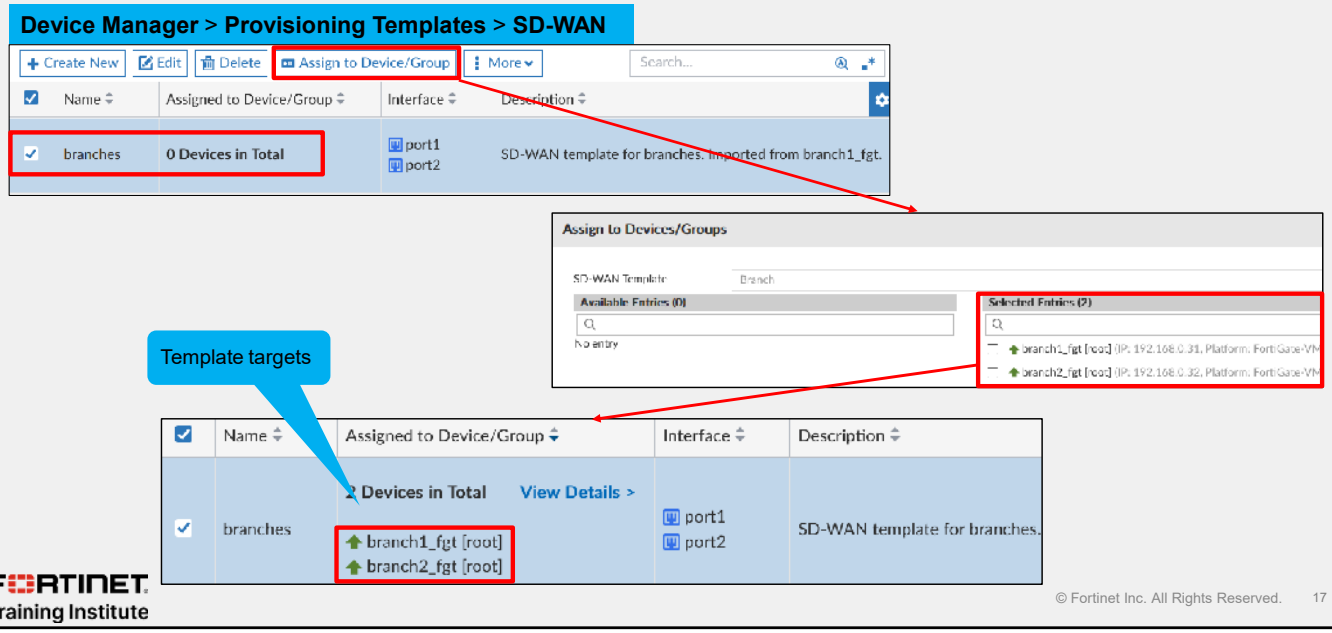


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Central Management—Assigning a Template

- Assigning an SD-WAN template to one or more devices:




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

After you configure a new template or you import its settings from a managed device, you can then assign the template to one or more devices or device groups.

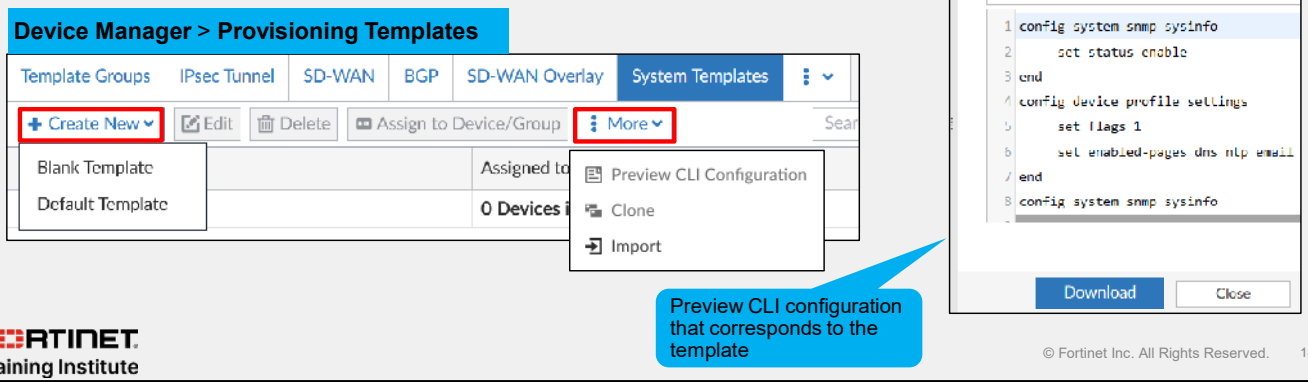


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Provisioning Templates—System Templates

- Subset of model device configuration—system-level settings
  - Configure or modify common settings
- You can:
  - Create new templates
  - Inherit the system settings and CLI settings of a managed device using the import feature
  - Associate already managed devices with a profile
  - Preview the CLI configuration




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

In addition to configuring an SD-WAN template, you may also need to configure a system template and one or more CLI templates. A system template enables you to create and manage common system-level settings for the managed device, such as **DNS**, **Alert Email**, **Admin Settings**, **Log Settings**, **SNMP**, and others.

You can create a new device profile and configure the settings in the widgets in that profile. You can use the **More** icon and **Import** to import the settings from a specific managed device, which inherits the system-level settings of that managed device. Alternatively, you can clone an existing profile and adjust the settings to address new needs.

You can apply these configured profiles to multiple devices within the same ADOM, which facilitates identical device-level settings across many devices. Use the **Assign to Device/Group** tab to associate devices with a profile, or to view the list of devices already assigned to a profile.

The **Preview CLI Configuration** menu displays the CLI commands that correspond to the parameters configured in the profile.

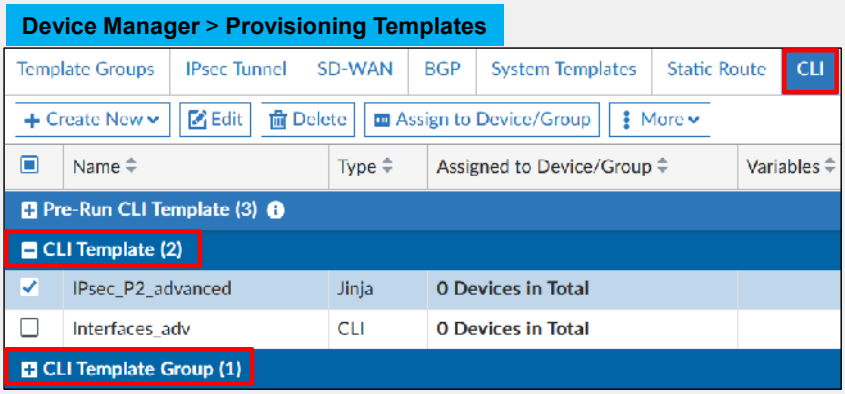


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Provisioning Templates—CLI Templates

- CLI scripts or groups of CLI scripts
  - Content of script is enforced when pushing the configuration to managed device
  - One CLI template or CLI template group per device
- Useful for:
  - Configuring advanced settings
  - Referencing metadata variables




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

CLI templates enable you to create CLI scripts or a group of CLI scripts that you can assign to managed devices. FortiManager then enforces the content of the script when pushing the configuration to managed devices.

CLI templates are useful for pushing advanced CLI settings, or settings that reference metadata variables.

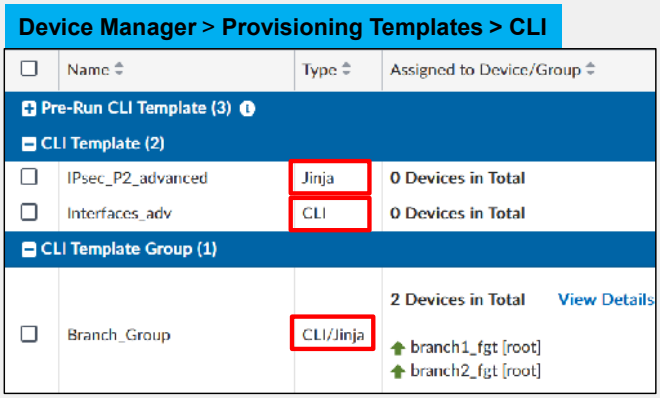


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Provisioning Templates—CLI Templates (Contd)

- CLI template type
  - CLI script
    - FortiGate CLI commands
    - Metadata variables referenced with $
  - Jinja
    - Jinja2 is a full-featured template engine
    - Advanced scripting options
    - Python-like syntax
    - Metadata variables referenced with {{
- Can mix both types in template group
  - Scripts applied in top-down order




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

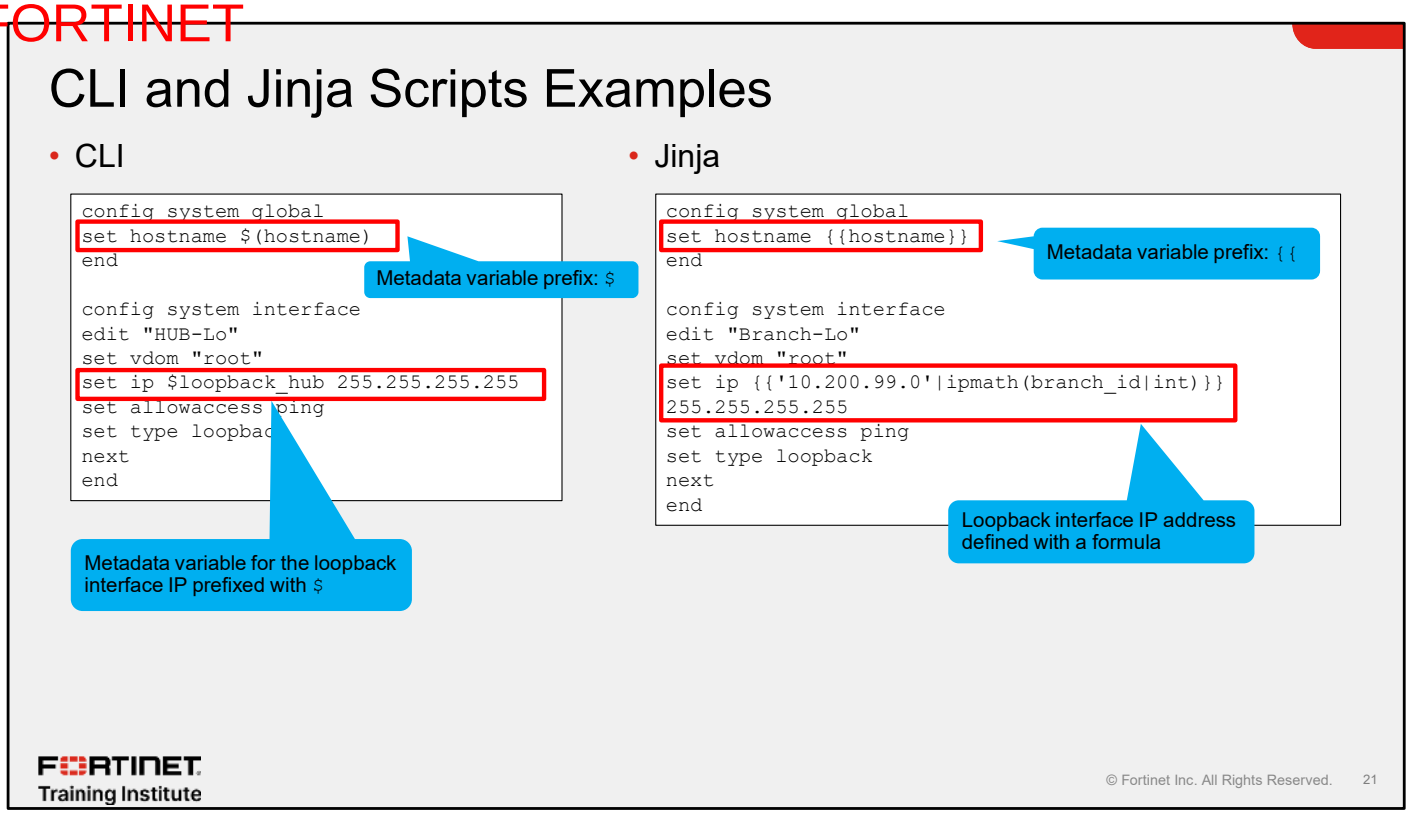
On FortiManager you can create two types of scripts: CLI scripts and Jinja scripts. For CLI scripts, you will use the FortiGate CLI commands and the $ sign to reference metadata variables. This type of script is very easy to use but does not offer advanced programming functions. With Jinja scripts, you can use Python-like syntax to configure advanced scenarios. Note that for Jinja scripts, you must reference metadata variables with a double brace symbol: {{.

You can use a template group to assign multiple CLI scripts to managed devices. The template groups can contain a mix of CLI and Jinja scripts and are applied in a top-down order.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




This slide shows two script examples. Both the CLI and the Jinja script configure the device hostname and a loopback interface but with different syntax.

The CLI script defines the `hostname` and the `loopback` IP address with metadata variables prefixed with `$`.

The Jinja script also uses a metadata variable to define the hostname, but according to the Jinja syntax, it frames the variable with `{{`. For the loopback IP address, it uses an arithmetic operation—`ipmath`—to build the IP address from the prefix provided—`10.200.99.0`—and the device `branch_id metadata variable`.

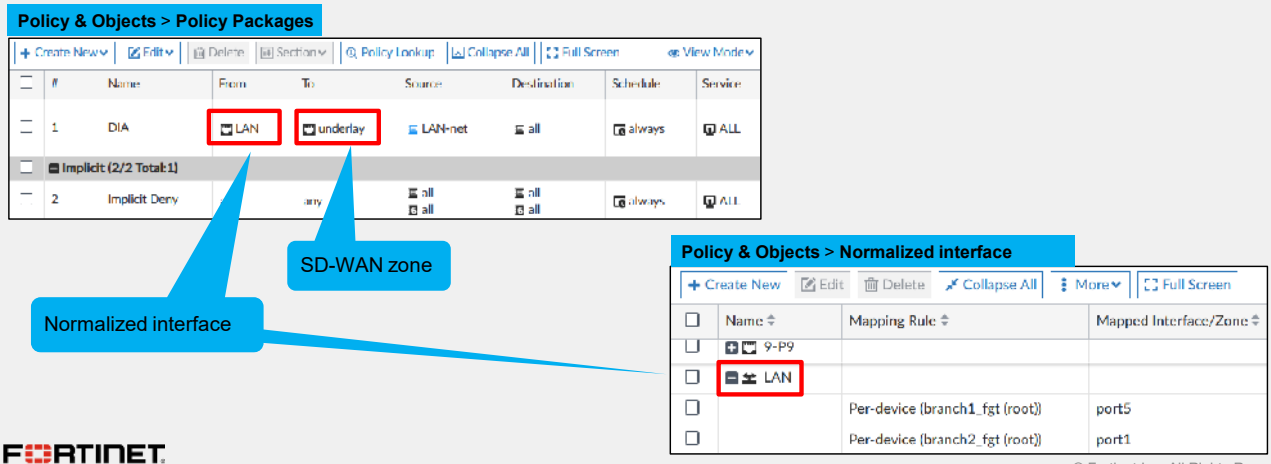


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Firewall Policies and Normalized Interfaces

- Configure firewall policy for SD-WAN
  - Create a policy package
    - Create firewall policy for SD-WAN zone
    - Select installation targets
  - Check mapping rules of normalized interfaces




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

When you configure firewall policies for SD-WAN, you must create a policy package. The policy package then contains one or more firewall policies that are assigned to one or more managed devices. Firewall policies for SD-WAN traffic must reference SD-WAN zones and not individual members. The other interfaces configured in the firewall policy are usually normalized interfaces, for which you must configure correct mapping rules.

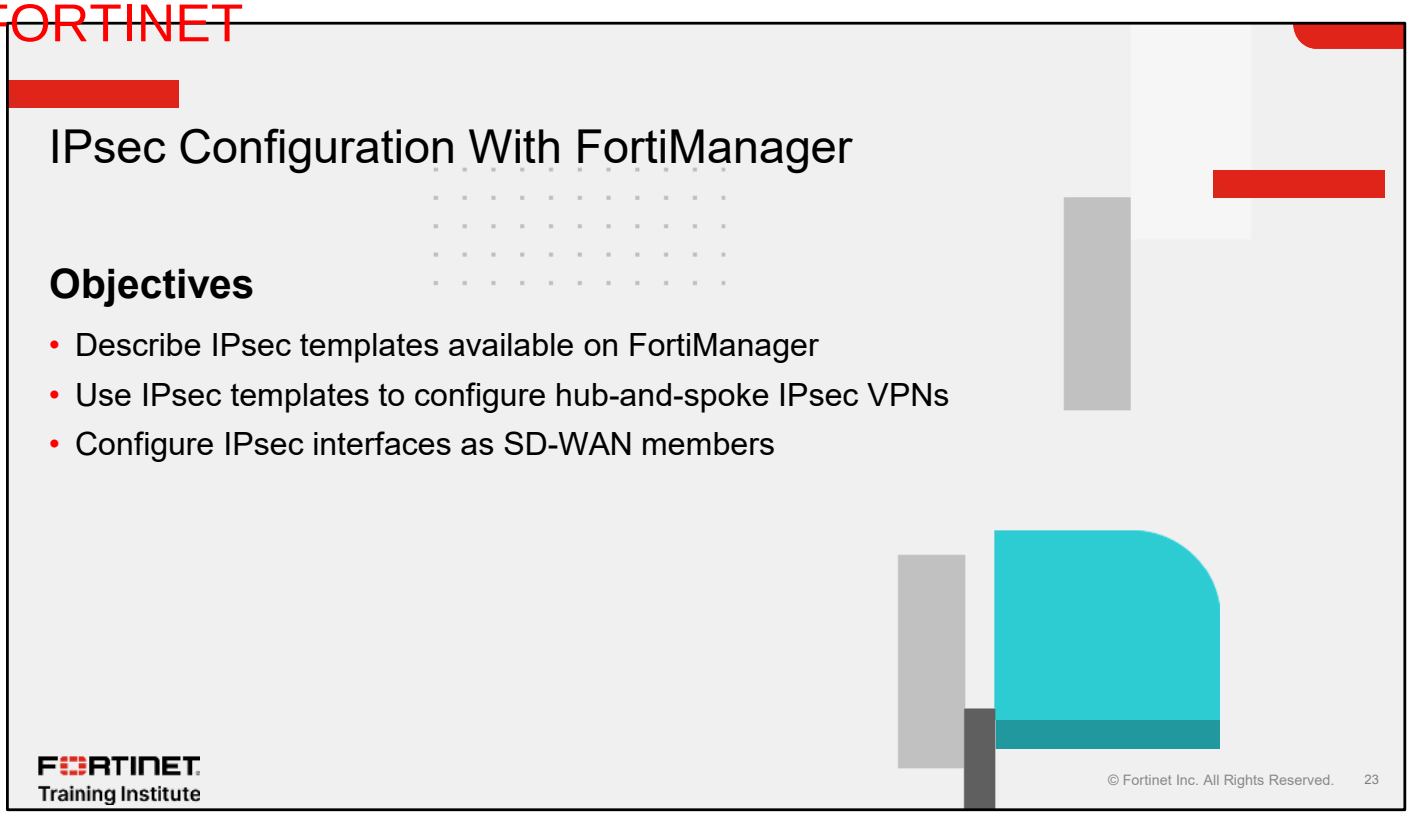
Normalized interfaces enable you to reference different interfaces on a per-device or per-platform basis. The goal is to be able to share objects, such as firewall policies, across multiple devices with different interface configurations. When FortiManager installs objects that reference a normalized interface, it reads the configured mapping rules, and then assigns the mapped interface to the pushed configuration of each target device.

In the example shown on this slide, the **branches-pp** policy package contains one firewall policy named **DIA**. The **LAN** normalized interface is configured as the incoming interface on the policy. **LAN** is mapped to port5 and port1 on **branch1_fgt** and **branch2_fgt** devices respectively.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the IPsec configuration templates available on FortiManager, you will be able to easily configure IPsec VPN tunnels on FortiGate. You will then see how to use the configured IPsec tunnels as overlays in SD-WAN.



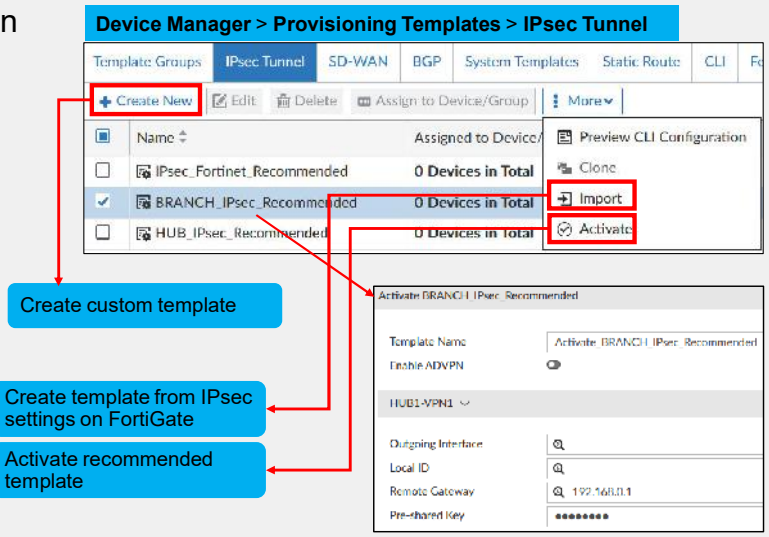
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# FortiManager IPsec Tunnel Templates

- Easy provisioning of IPsec tunnels
- Guidance for IPsec tunnel configuration
  - Use recommended parameters
  - Consistent settings between phase1 and phase2
- Applied to multiple devices
  - Simplified deployment
  - Same parameters at both ends of tunnels
- Available templates
  - IPsec_Fortinet_Recommended
  - BRANCH_IPsec_Recommended
  - HUB_IPsec_Recommended
- One template per device
  - One or multiple tunnels per template

- Template menu




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

On FortiManager, you can use the IPsec template to easily configure consistent IPsec settings on multiple devices.

There are various ways to prepare a template:

- Create a new template and manually define all required IPsec parameters (**Create New**).
- Import settings from a managed FortiGate with an already defined IPsec tunnel (**Import**).
- Use a Fortinet-recommended template (**Activate**).

Recommended templates allow you to prepare a template for IPsec tunnels using Fortinet-recommended settings for phase1 and phase2 parameters.

- The IPsec_Fortinet_Recommended template defines a template for a static point-to-point tunnel.
- The BRANCH_IPsec_Recommended template defines a template for a static tunnel (with a known remote IP address).
- The HUB_IPsec_Recommended template defines a template for a dynamic tunnel (an IPsec hub for dial-up tunnels).

This slide shows an example of the limited number of parameters that you must provide to prepare a branch tunnel configuration with the BRANCH_IPsec_Recommended template. Then, using these parameters, FortiManager prepares a template with the IPsec configuration ready to install on the device. You can still review the template and adjust it if necessary. As you already discovered for SD-WAN or CLI templates, metadata variables are useful to customize the template with values specific to each device.

If you are already familiar with FortiManager and have used the VPN Manager for your deployments, you can keep using it. However, for new deployments, you should use the IPsec recommended templates, or for a new SD-WAN deployment, the SD-WAN overlay template, which you will discover later in this lesson.

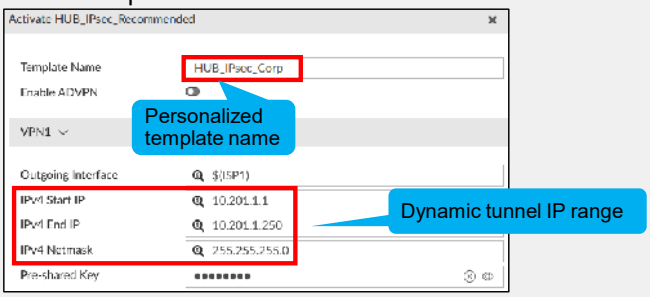


Vouchers & Dumps are Available | WhatsApp +201224560923

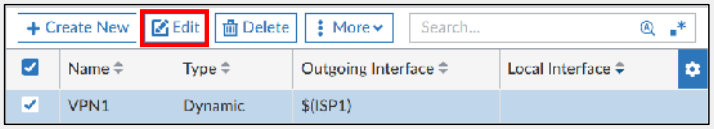
DO NOT REPRINT Brave-dumps.com
© FORTINET

## HUB_IPsec_Recommended Template

1- Fill template form

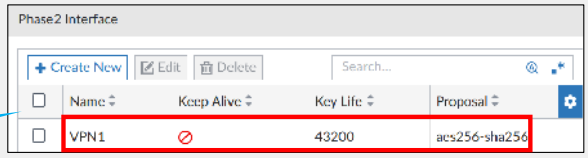



2- Edit prepared tunnel template




3- Review and adjust

- Tunnel name (default VPN1)
- Network parameters
  - Outgoing interface
  - Start IP, end IP
- Encryption proposal
  - Default: aes256-sha256
- Tunnel authentication method
  - Default: pre-shared key
  - Alternative: certificate authentication
- Phase2 settings
  - Default: keep alive disabled




Phase2 settings with HUB_IPsec_Recommended template

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

The HUB_IPsec_Recommended template prepares a template for a dynamic IPsec VPN tunnel with an outgoing interface, pre-shared key, and IP address range for the remote tunnel specified by the administrator.

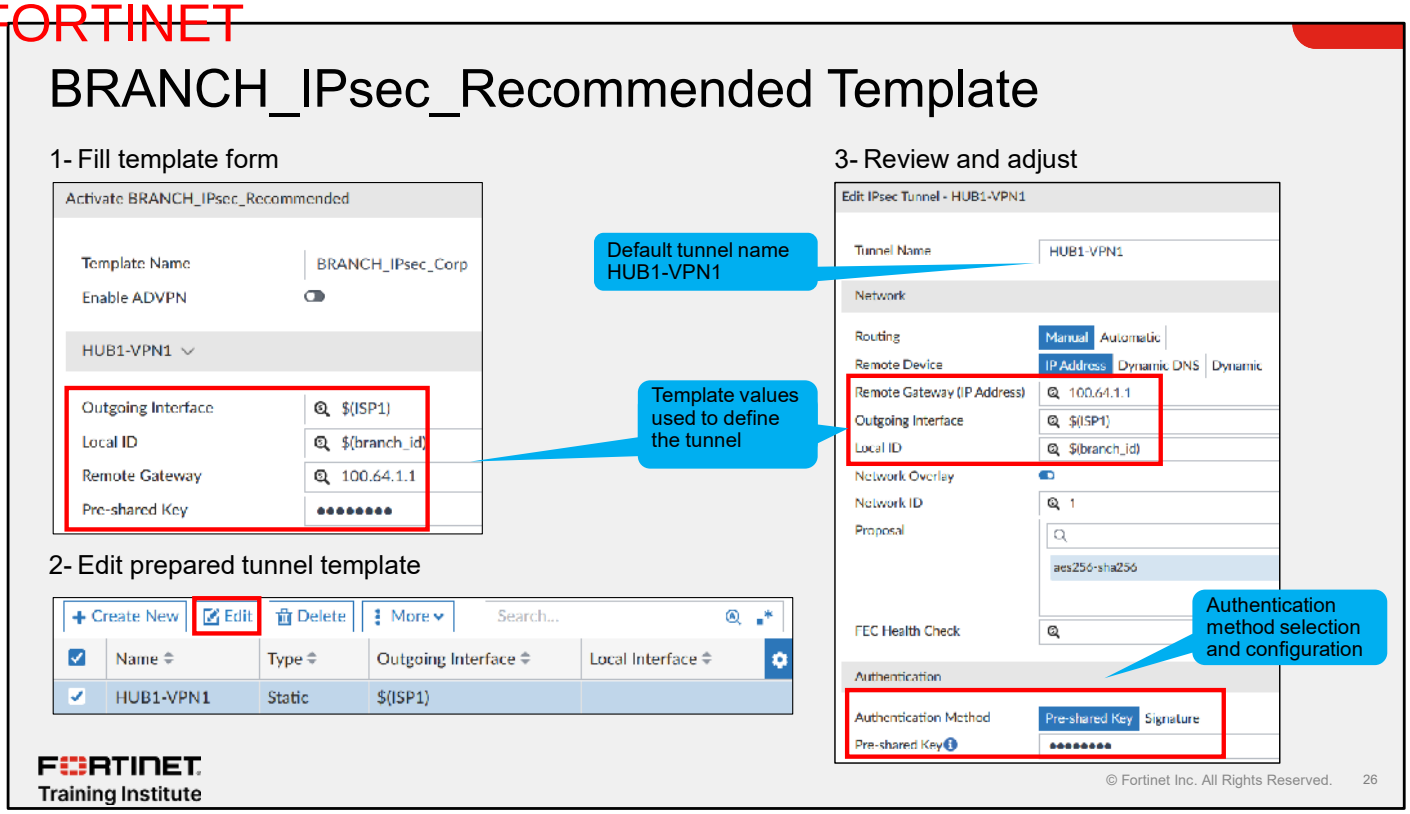
The tunnel name, network ID, and encryption proposal are automatically set with the values VPN1, ID1, and aes256-sha256. Of course, if required, you can edit and adjust the template.

Note that on template creation, **Keep Alive** is disabled. You can edit **Keep Alive** to enable it.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




The BRANCH_IPsec_Recommended template prepares a template for the static IPsec VPN tunnel. You must specify the IP address for the remote end of the tunnel. The template uses the outgoing interface, pre-shared key, and local branch ID specified by the administrator. The local ID must be unique for each branch site. It's therefore convenient to define it as a metadata variable.

The tunnel name, network ID, and encryption proposal are automatically set to HUB1-VPN1, ID1 and, aes256-sha256. The authentication method is set to pre-shared key and uses the password defined on the template form. If required, you can edit and adjust those values and any other parameter from the template.

Note that on template creation, the same as for the hub, **Keep Alive** is disabled. You can edit the template to enable **Keep Alive**.

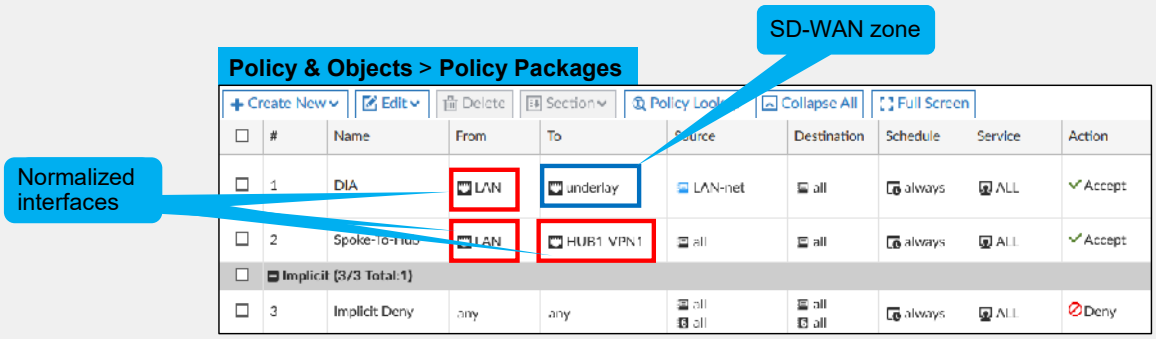


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## IPsec Interfaces and Firewall Policies

- Normalized IPsec interface configuration
  - Not required if IPsec interface is in SD-WAN zone
- Firewall policies reference
  - SD-WAN zones
  - Normalized interfaces: physical, IPsec, VLAN, and so on




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Normalized interfaces enable you to reference different interfaces on a per-device or per-platform basis, thus simplifying the configuration and deployment process for multiple devices. Usually, FortiManager requires you to normalize interfaces. However, it's not required if you plan to configure an IPsec interface as an SD-WAN member. This is because SD-WAN members don't use normalized interfaces. Another reason is that firewall policies for SD-WAN must reference SD-WAN zones, and not individual members.

If you *don't* plan to use an IPsec interface as an SD-WAN member, then you must normalize the interface so you can reference it on firewall policies, which are required for the tunnel to come up. After you configure the normalized IPsec interface, you can reference the interface on firewall policies.

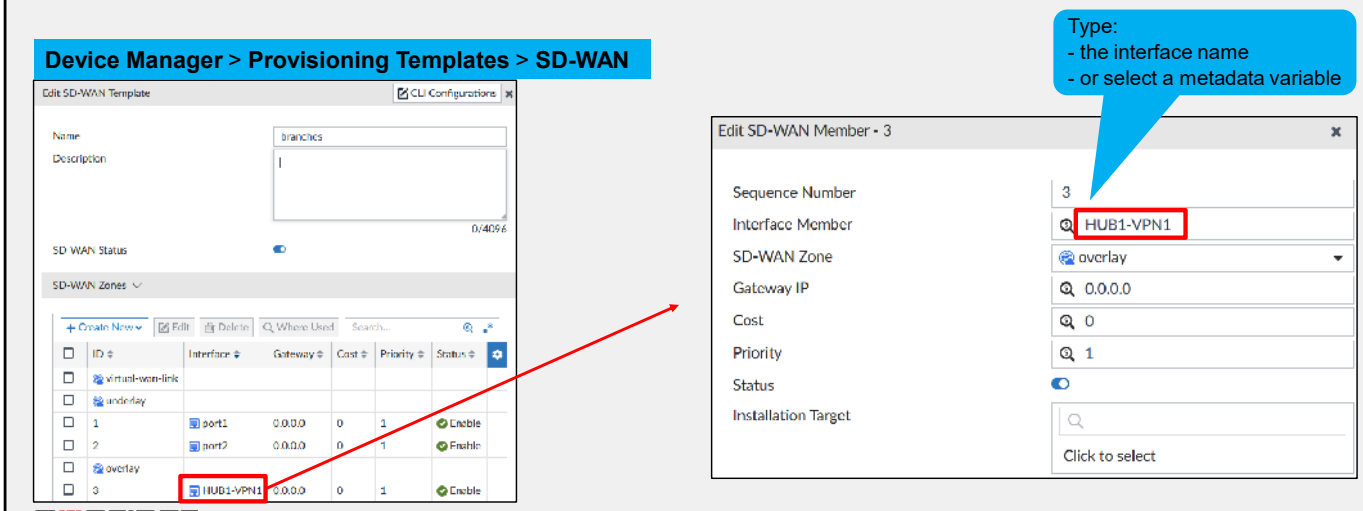


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## IPsec Interfaces as SD-WAN Members

- Add the IPsec interface as SD-WAN member
  - Type the device interface name or select a metadata variable
  - Remove references to individual members on firewall policies first




After you configure your IPsec tunnels, you can start using them as SD-WAN members. Just make sure to remove any existing references to the individual members on firewall policies. Otherwise, FortiManager can't install the SD-WAN configuration because you can't reference individual SD-WAN members on firewall policies. You can reference SD-WAN zones only.

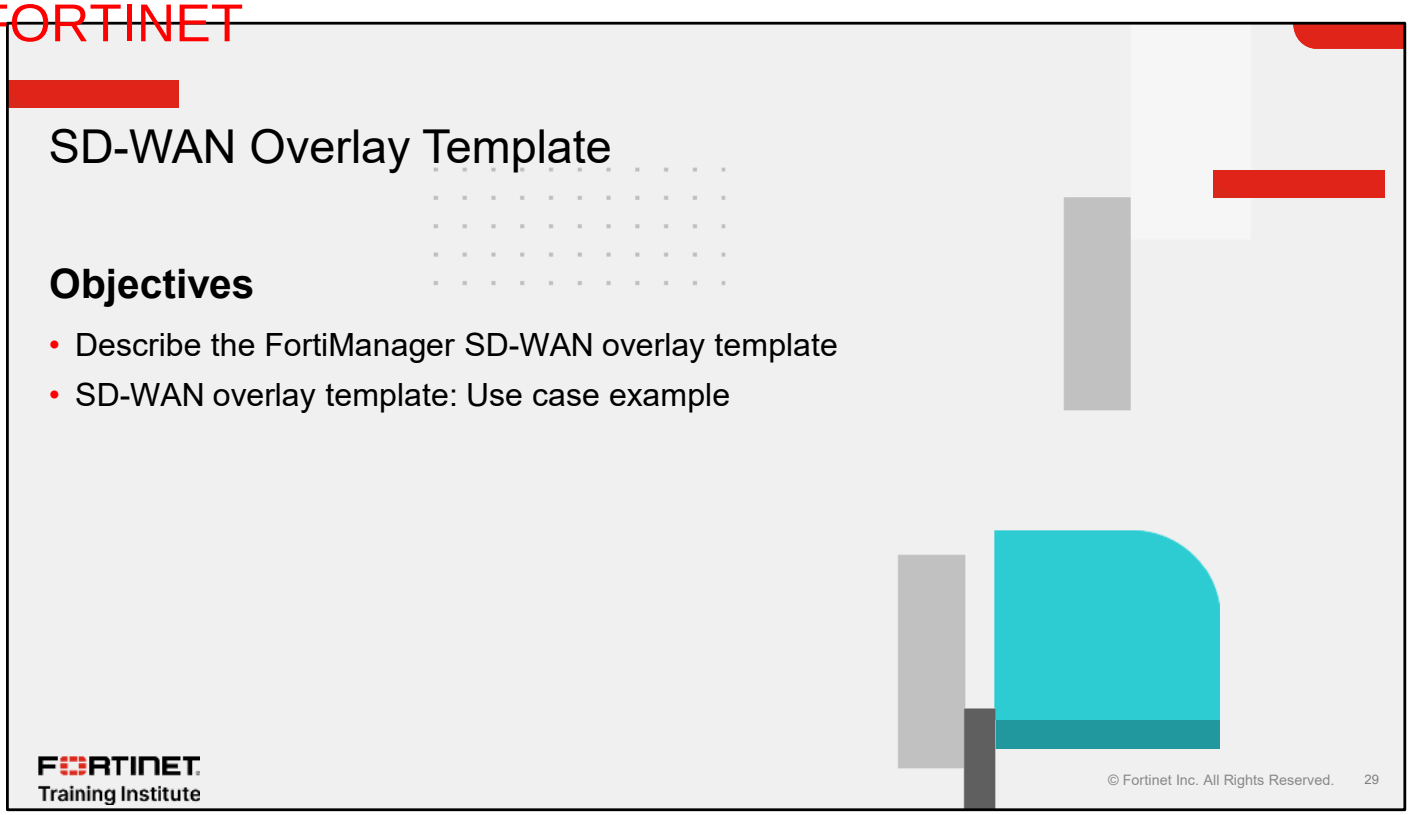
Note that SD-WAN members don't use normalized interfaces. Instead, you must type the name of the interface on the device or use a metadata variable.

In the example shown on this slide, **HUB1-VPN1** is the name of the IPsec interface on the device. The interface is configured as an SD-WAN member and placed in the **overlay** zone.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the FortiManager SD-WAN overlay templates, you will be able to configure and deploy a large SD-WAN topology and associated overlay IPsec network with reduced effort.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## FortiManager SD-WAN Overlay Template

- The SD-WAN overlay template simplifies the configuration and deployment of secured SD-WAN topology
- A wizard guides the administrator to define overlay configuration and routing for SD-WAN topology
- Available per ADOM
- Steps:
  1. Define network topology and subnets to use
  2. Initial basic device configuration (administrator settings, interface IP/subnet, and so on)
  3. Import devices to FortiManager
  4. **Follow SD-WAN overlay template wizard**
  5. Review configuration
  6. Install configuration to devices

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

Most SD-WAN deployments require complex overlay configurations for datacenter or cloud connectivity. FortiManager includes an SD-WAN overlay template with a wizard to automate and simplify the process using the IPsec and BGP settings recommended by Fortinet. The SD-WAN overlay template wizard guides you through the configuration steps and generates a set of consistent configuration templates for SD-WAN, overlay, and routing configurations for hubs and branch devices.

Note that you can't use VPN manager and an SD-WAN overlay template for the same network. When applicable, for a new deployment, you should use the SD-WAN overlay template. It provides a comprehensive approach and guides you through IPsec, BGP, and SD-WAN configuration.

Do the following to use an SD-WAN overlay template:

1. Define the network topology and subnets to use.
2. Preconfigure your network and SD-WAN devices with administrator settings, the interface IP address and subnet, and so on.
3. Import devices to FortiManager.
4. Use the SD-WAN overlay template configuration wizard to guide you.
5. Review the configuration templates generated.
6. Install the configurations on devices.

You can add more branch devices later to the branch device group.

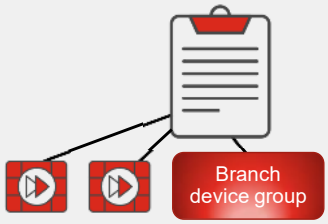


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Prerequisites and Network Planning

- Prerequisites
  - FortiGate devices that will form the hub (or hubs) must be managed by FortiManager
  - Create a device group for your branch devices
  - Configure the WAN, ISP links, and other interfaces on your imported devices
- Optional
  - Add branch devices to FortiManager
- Network planning
  - Allocate the overlay network address space (default template value 10.10.0.0/16)
  - Allocate the loopback IP address space (default template value 172.16.0.0/16)
    - The SD-WAN overlay template uses the loopback IP addresses only to define the health check
  - Select an AS number for BGP for the new SD-WAN overlay region (default template value 65000)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

Before you can define an SD-WAN overlay template, you must define the hub devices as FortiManager-managed devices—you can use model devices or discover physical devices—and configure the necessary links and interfaces.

You can define the branch devices as FortiManager-managed devices in this preliminary phase or later, but you must create a device group that contains the branch devices before you proceed further with the SD-WAN overlay template.

Network planning is an important phase. You must define the following elements before using an SD-WAN overlay template:

- Topology type
- Overlay network address space
- Loopback IP address space
- BGP AS number for SD-WAN overlay region

Note that FortiManager, with the SD-WAN overlay template, defines topologies with BGP per overlay and uses the loopback IP addresses only to define the health check.

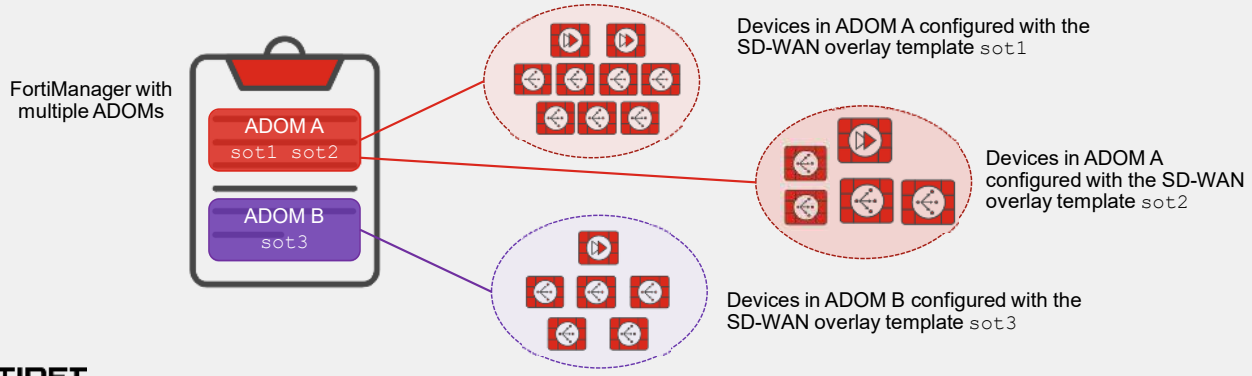


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# ADOMs and SD-WAN Overlay Templates

- FortiManager supports:
  - SD-WAN overlay templates in each ADOM
  - Multiple SD-WAN overlay templates in each ADOM
- Restrictions
  - All devices participating in an SD-WAN overlay template must be in the same ADOM
  - Each FortiGate device can be configured by only one SD-WAN overlay template




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

You can define multiple SD-WAN overlay templates on FortiManager to manage multiple topologies simultaneously. On a FortiManager with multiple ADOMs, you can create one or more SD-WAN overlay templates in each ADOM.

When you configure multiple SD-WAN overlay templates, the following restrictions apply:
- All devices configured by an SD-WAN overlay template must be in the same ADOM.
- Each FortiGate can receive a configuration from one SD-WAN overlay template only.

The diagram on this slide shows a FortiManager device with two ADOMs. The administrator configured ADOM A with two SD-WAN overlay templates—sot1 and sot2—and ADOM B with one SD-WAN overlay template—sot3. Template `sot1` defines a dual-hub topology; the templates `sot2` and `sot3` define single-hub topologies.

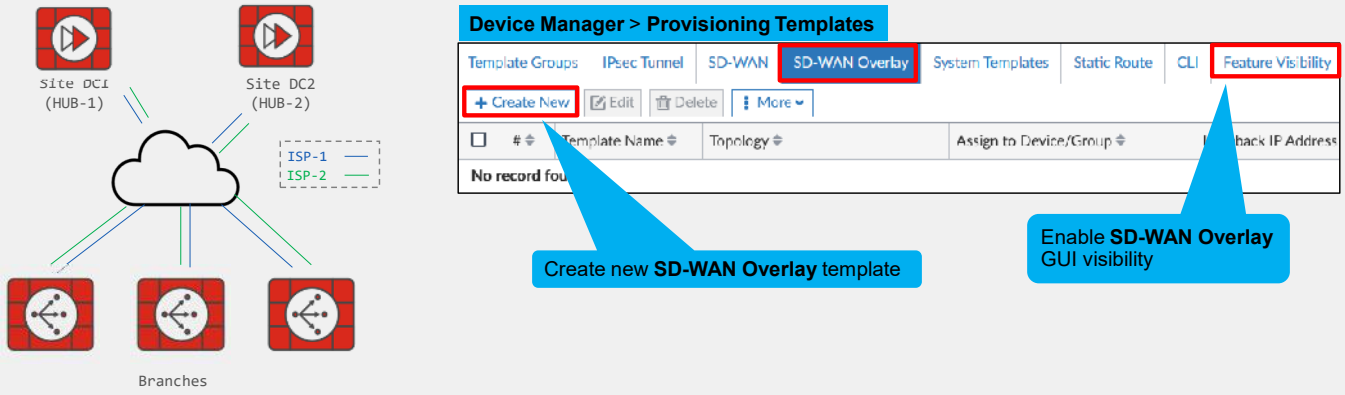


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Example

- Through the next few slides, you will see how to use an SD-WAN overlay template
- You will use the overlay template to create templates for a dual-hub topology with two underlay links on each device and ADVPN to allow shortcut tunnels between branches




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

The SD-WAN overlay template helps you to configure templates for single-hub and dual-hub topologies. Dual-hub topology offers options for **Primary & Secondary** topology where one hub is preferred over the other from the routing perspective, or **Primary & Primary** topology with both hubs equally considered.

Over the next few slides, you will explore how to use the wizard to create templates to configure devices for the topology shown in the diagram.

We will use following parameters:

- Dual Hub (Primary & Secondary)
- Two underlay links for each devices
- IBGP routing
- ADVPN

Note that the **SD-WAN Overlay** tab is not displayed by default. Use the **Feature Visibility** menu and select the provisioning template menus that you want to see.

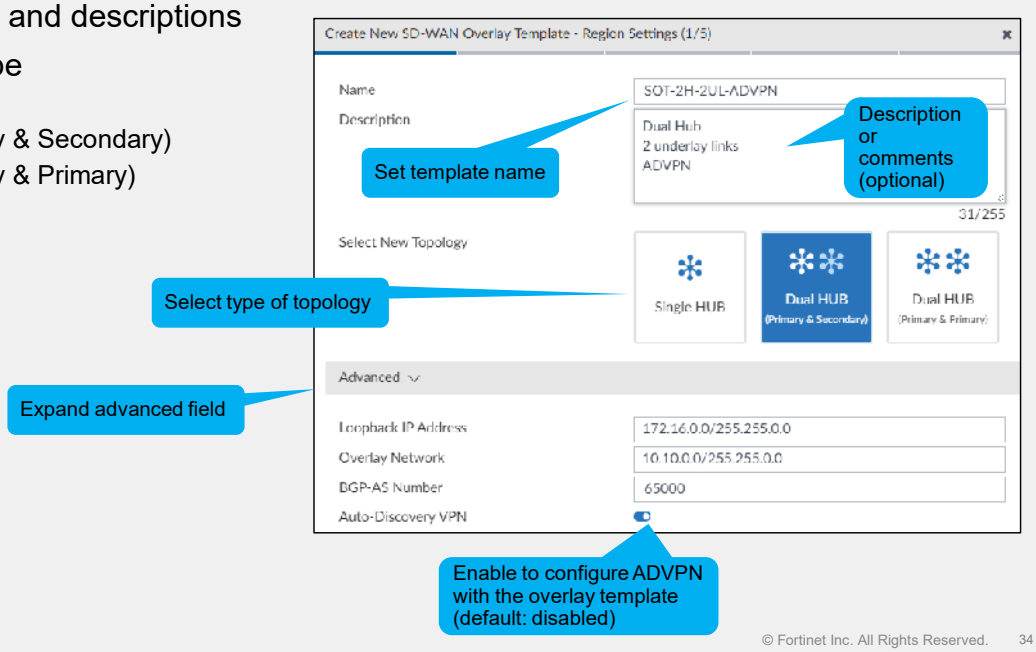


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Step1—Region Settings

- Set template name and descriptions
- Define topology type
  - Single HUB
  - Dual HUB (Primary & Secondary)
  - Dual HUB (Primary & Primary)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

First you set the template name and define the type of topology used, either single hub or dual hub and the type of redundancy—primary and secondary or primary and primary. For the template name, Fortinet recommends that you use a meaningful name and add a detailed description that you can later refer to. In the example shown on this slide, the template name summarizes the main characteristics that it configures.

In the **Advanced** section, apply settings for the network elements:

- Loopback IP Address
- Overlay Network
- BGP-AS Number
- Auto-Discovery VPN (default: disabled)

The SD-WAN overlay template guides you through a wizard. FortiManager adjusts the fields available on each page according to the option you selected on previous pages.

If you enable ADVPN in the SD-WAN overlay template, FortiManager enables the necessary settings in the IPsec templates. You will learn more about ADVPN in another lesson.

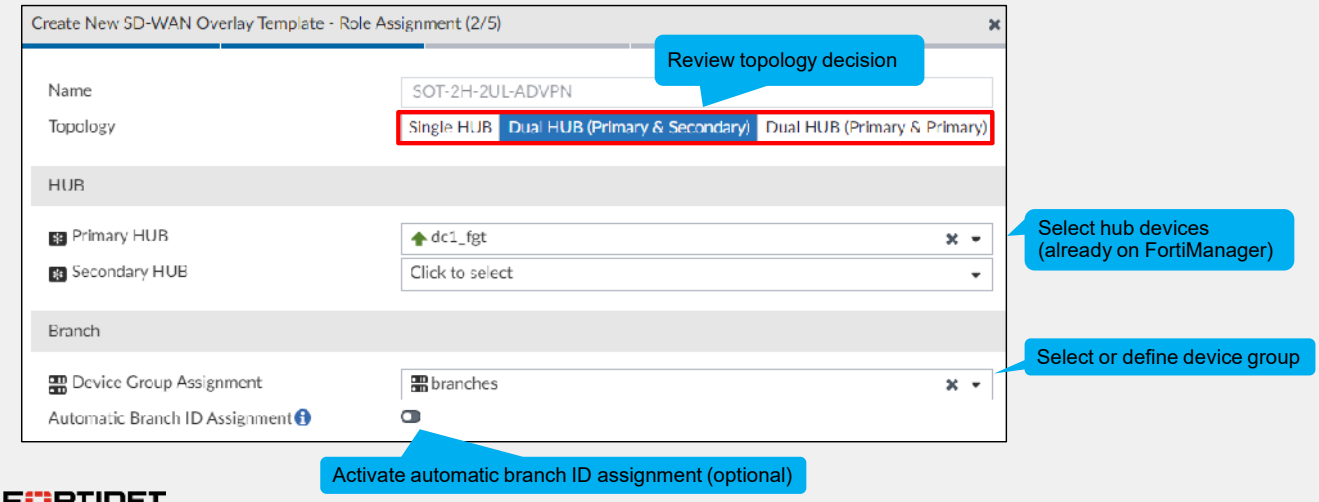


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Step 2—Role Assignment

- Define device roles
  - Select devices with a hub role
  - Select or define a device group for branch devices




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

In step 2, you review the topology definition and define the device roles.

For hub devices—two for a dual-hub topology—you must select from devices already discovered on FortiManager—or from model devices already defined.

For branch devices, at this stage, you must define a branch devices group. This group can be empty while you are working on the template. Later, you can add devices to the branch device group as the network evolves and new sites join the SD-WAN topology.

With the **Automatic Branch ID Assignment** selector, FortiManager assigns the branch ID for you. Keep the default value—unselected—to let the administrator define the ID assignment for each branch device.

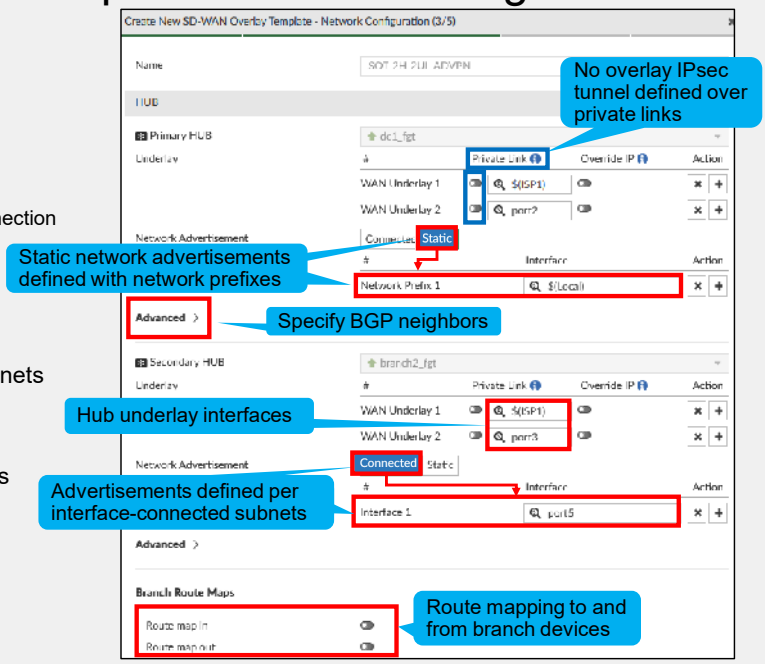


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Step 3—Network Configuration

- Part 1: Network settings for hubs
  - Define underlay interfaces
  - Define the type of link
    - **Private Link** deselected (default):
      - Creates an overlay IPsec tunnel
      - Use for unsecure link, such as internet connection
    - **Private Link** selected:
      - Does not create an overlay tunnel
      - Use for secure link, such as MPLS link
  - Define type of network advertisement
    - Connected: redistribute hub-connected subnets
    - Static: distribute specified subnets
  - Optional
    - Route mapping in/out, to and from branches
    - Specify BGP neighbors




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

Step 3 consists of network configuration for hub and branch devices.

At this stage, you will define the network interfaces used for underlay links, usually static definitions for hubs and metadata variables for branches.

The **Private Link** checkbox indicates a secure internal link. FortiManager will NOT define an overlay link through this interface. It creates SD-WAN members, assigns them to zones, and defines BGP settings only. The administrator should enable private links that are natively secure, such as an MPLS connection. Keep the default value—**Private Link** deselected—if you want to define an IPsec tunnel over the underlay interface.

You can also add additional underlay links at this stage (click **+**).

For network advertisements, you can decide between a connected subnets advertisement or a static network prefixes definition. For a connected subnets advertisement, you must select interfaces that correspond to subnets to advertise.

Branch route maps correspond to route maps that the hub applies to a branch neighbor group.

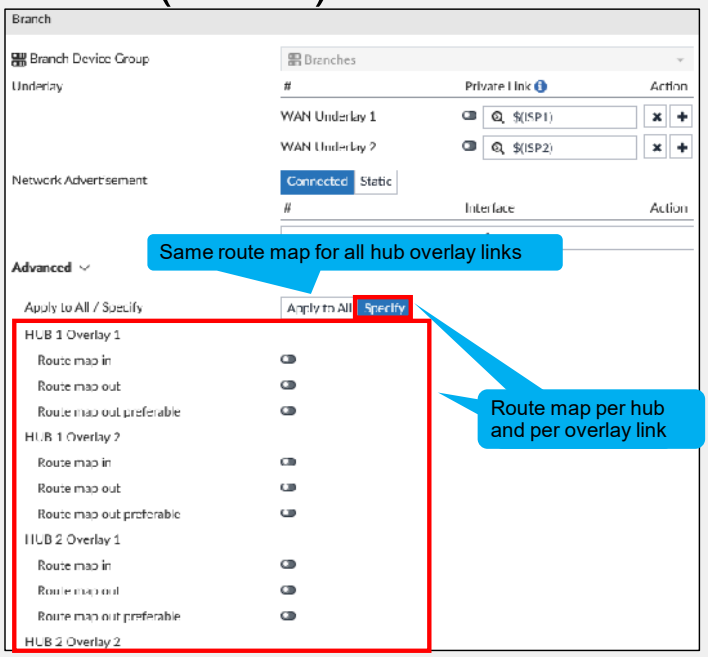


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Step 3—Network Configuration (Contd)

- Part 2: Network settings for branch devices
  - Define underlay interfaces
  - Define type of network advertisement
    - Connected: redistribute connected subnets
    - Static: distribute specified subnets
  - Define BGP route map
    - Route map in/out with hubs
    - Route map out preferable
    - Can be identical for all overlay or specified per hub and per overlay




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

Usually, to define WAN underlay interfaces for branch devices, you use metadata variables. This allows you to accommodate various types of branch sites and branch devices. Similarly, you can use metadata variables for connected subnet interface definitions.

In the **Advanced** section you can define route mapping per hub overlay link or globally for all links. You can define **Route map in**, **Route map out**, and **Route map out preferable** settings. You can define these settings similarly for all hubs and all overlay links, or refine per hub and per overlay link.

**Route map out** and **Route map out preferable** allow differentiated route map advertisements. If an SD-WAN member meets the SLA threshold, FortiGate applies the route map defined in the BGP neighbor's `route-map-out-preferable` option. If the SD-WAN member fails to meet the SLA, FortiGate applies the route map defined in the BGP neighbor's `route-map-out` option. This allows FortiGate to advertise the health of the SD-WAN member to its BGP neighbor by advertising different community strings based on SLA status. You will explore route map options in greater detail in another lesson.

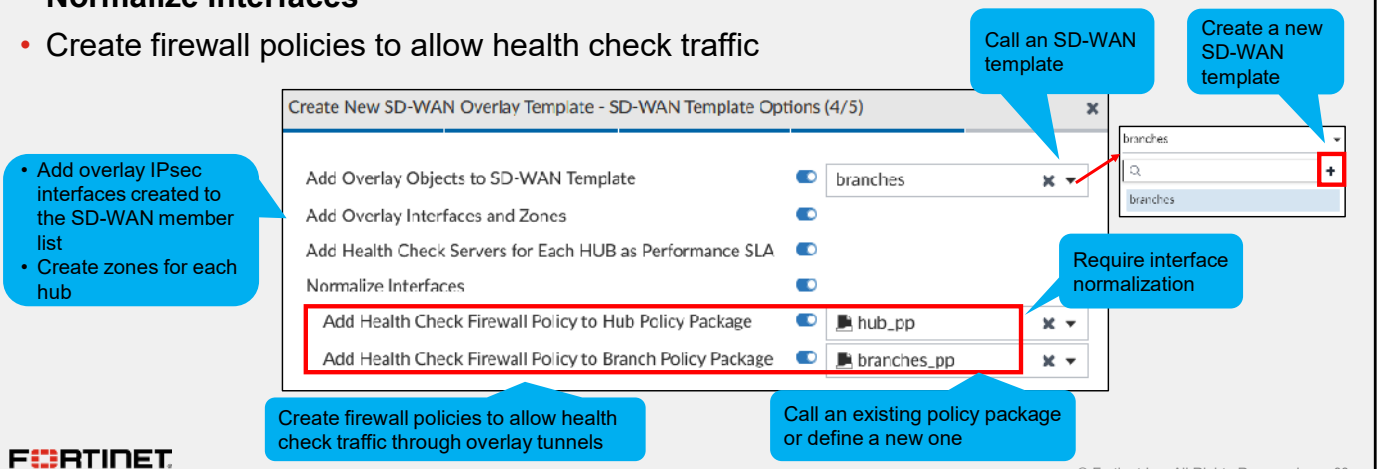


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Step 4—Template Options

- **Add Overlay Objects to SD-WAN Template**
- **Add Overlay Interfaces and Zones**
- **Add Health Check Servers for Each HUB as Performance SLA**
- **Normalize Interfaces**
- Create firewall policies to allow health check traffic




In step 4, you can select the SD-WAN template that the SD-WAN overlay template process uses. The process does not create it automatically. From this menu, you can you select an existing template or click **+** to create a new SD-WAN template. Additionally, you can enable or disable the **Add Overlay Interface and Zones** switch to add overlay IPsec interfaces created to the SD-WAN member list, and create zones for each hub.

If you enable **Add Health Check Servers for Each HUB as Performance SLA**, the process creates one performance SLA check for each hub loopback IP address. These SLA checks are defined with the default values detection protocol Ping, failure threshold 5, and recovery threshold 5. Once created, you can edit the SD-WAN template to review and adjust the values as required.

The **Normalize Interfaces** option automatically normalizes the SD-WAN zones that the template created, so that you can use them in firewall policies. It creates the following normalized interfaces: HUB1-Lo for HUB1, when applicable HUB2-Lo for HUB2, VPN1 and VPN2 for IPsec tunnels that the wizard created.

When you use the wizard to normalize the interfaces that it creates, you can activate the **Add Health Check Firewall Policy to Hub Policy Package** and **Add Health Check Firewall Policy to Branch Policy Package** to automatically create policies that allow health check traffic through the newly created IPsec tunnels.

The wizard does not create SD-WAN rules. You can add them later and refine them as requirements evolve.

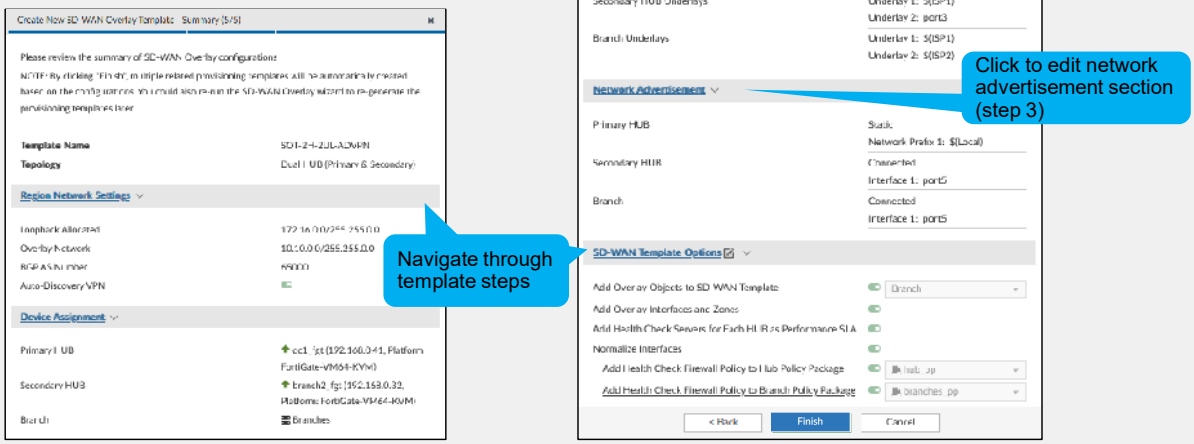


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# SD-WAN Overlay Template—Step 5—Summary

- Last step of the process
  - Review all settings
  - Go directly to section if changes are required
  - Validate to create templates




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

The last step, step 5, is a review phase.

You can review all settings and, if adjustments are required, go directly to the appropriate menu. Once you are happy with the settings, click **Finish**.

You will see the results on the next slide.

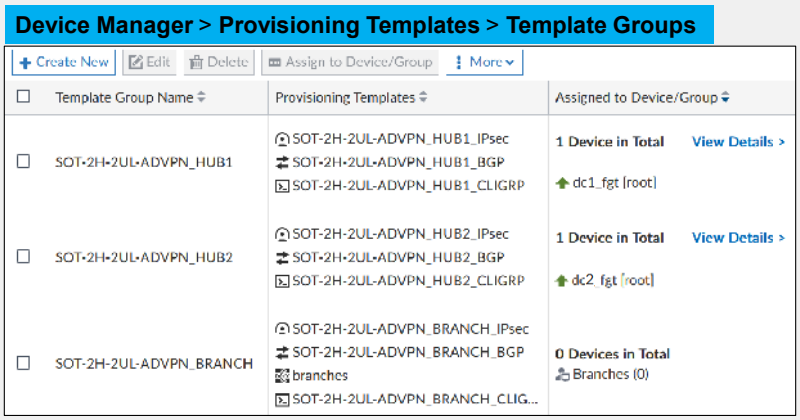


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Result

- SD-WAN overlay template generates multiple templates
  - BGP
  - IPsec tunnels
  - CLI
- For branches only
  - Update the SD-WAN template
- It groups templates per devices
  - HUB1
  - HUB2
  - BRANCH
- Administrator can
  - Review
  - Edit
  - Install on devices




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

The SD-WAN overlay template generates multiple templates, one per topic.

For branches and hubs, it creates BGP, IPsec, and CLI templates to accommodate all required configuration changes.

For the branch devices, it adds members and zones to the SD-WAN template defined.

The templates are grouped by device, and device assignment is done for you.

At this stage, you can review each template and fine-tune settings as required before you apply the configurations to devices.

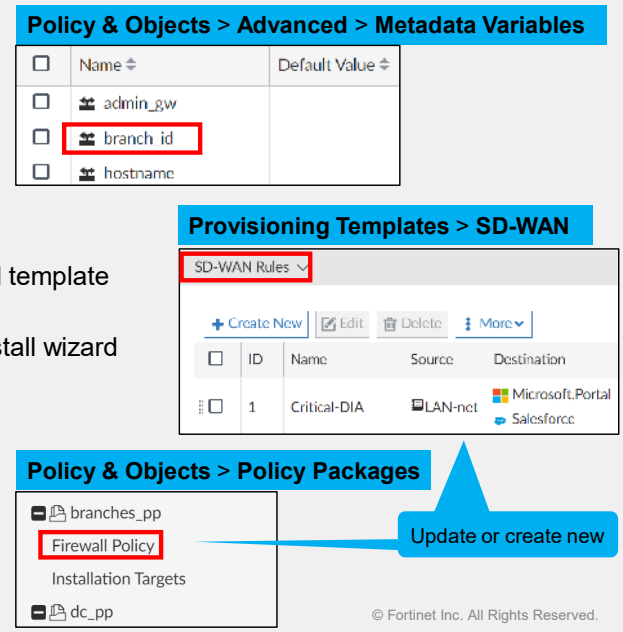


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Template—Post-Run Tasks

- Mandatory
  - Assign metadata variables to devices
    - Created by SD-WAN overlay template
      - Branch_id
    - User-created variables
      - Device name
      - Gateway
      - Interface IP
      - and so on
  - Configure the SD-WAN rules by editing the SD-WAN template
  - Create policy packages for branch and hub devices
  - Install the changes to SD-WAN devices using the install wizard
- Optional
  - Edit SD-WAN overlay template
  - Add new branch devices




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 41

After completing the SD-WAN overlay template wizard, you must complete some additional tasks.

The SD-WAN overlay template automatically creates a metadata variable called **branch_id**. If you didn't select the automatic branch ID assignment in step 2, you must define a unique branch ID value for each branch device. If you created additional metadata variables through the process, you should also define corresponding values for each device. Usually, you use metadata variables for device name, interface IP address, or gateway.

You will also edit the SD-WAN template to configure SD-WAN rules and define SLA criteria, create policy packages for your branch and hub devices, and then, install changes to the device with the install wizard.

Later, you can return to the SD-WAN overlay template to edit and modify settings. You can also add new branch devices to the device group.

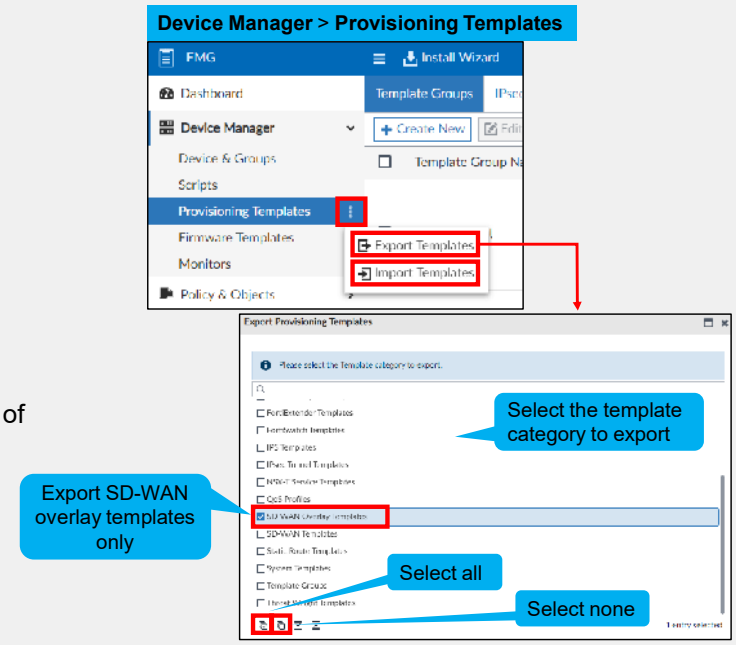


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Export and Import SD-WAN Overlay Templates

- Export
  - SD-WAN overlay template
  - BGP templates, IPsec templates, and so on
  - Export all templates from a category
- Import
  - To another FortiManager device
  - To a different ADOM on the same device
  - Import all templates from a category
- Requires export and import of the variables separately
  - Use CSV or JSON file for export and import of variables




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 42

If you want to move or duplicate an SD-WAN overlay template or any other type of template from one ADOM to the other or from one FortiManager device to another, you can use the export and import feature on FortiManager. This feature allows you to select one or more categories to export. However, you cannot specify the exact template to export. For example, if you defined two SD-WAN overlay templates on a FortiManager device, the export feature exports both of them.

You can export the template only. If the template uses variables, you must export and import the variables separately. For this task, you can use the feature export and import metadata variables feature that you learned about in this lesson.



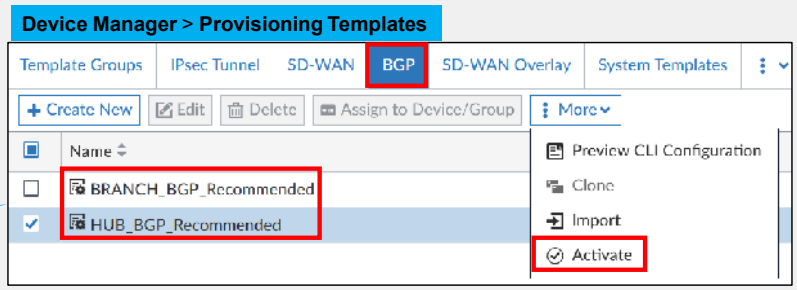
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Fortinet Recommended Templates

- Predefined template per topic
- Guide user for recommended settings
- Flexibility
  - Use recommended template for some topics
  - Use custom template for others
- Available recommended templates examples:
  - IPsec tunnel templates
    - BRANCH_IPsec_Recommended
    - HUB_IPsec_Recommended
  - BGP templates
    - BRANCH_BGP_Recommended
    - HUB_BGP_Recommended

Wizard to guide creation of template




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

The SD-WAN overlay template guides you through the creation of SD-WAN, BGP, and IPsec tunnel templates in a combined process. If you require guidance for some tasks only, you can use Fortinet recommended templates. They are available for IPsec and BGP.

To use a recommended template, select the desired template and activate it. It creates a personalized copy and, using a wizard, guides you through the configuration.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Understand FortiManager basics
- ✓ Identify FortiManager features for SD-WAN
- ✓ Describe SD-WAN management on FortiManager
- ✓ Describe IPsec templates available on FortiManager
- ✓ Use IPsec templates to configure hub-and-spoke IPsec VPNs
- ✓ Configure IPsec interfaces as SD-WAN members
- ✓ Describe the FortiManager SD-WAN overlay template
- ✓ SD-WAN overlay template: Use case example

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

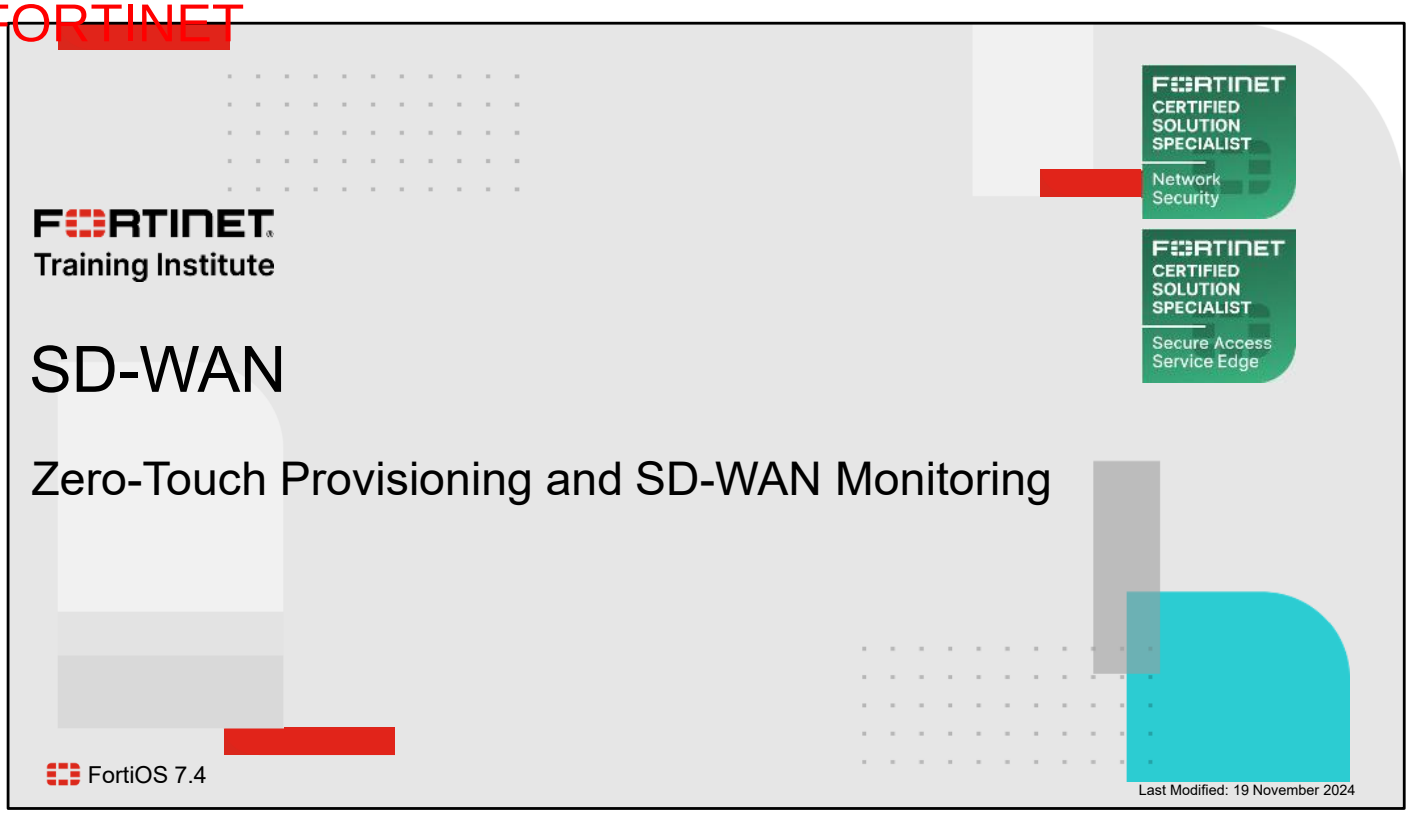
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned the most useful features available on FortiManager for deploying SD-WAN in large networks.



Vouchers & Dumps are Available | WhatsApp +201224560923

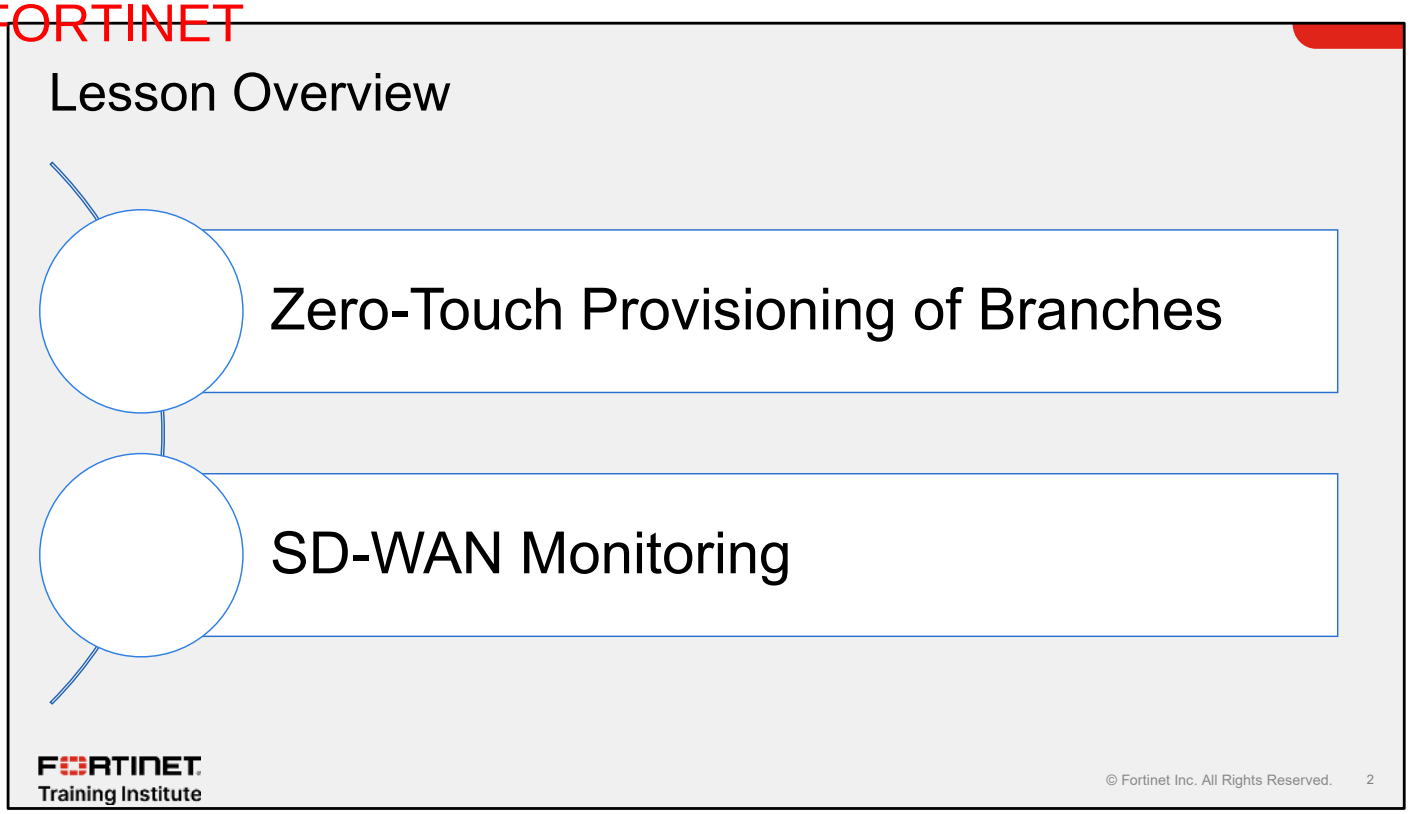
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn how you can use FortiManager to simplify your deployment of SD-WAN branch devices with zero-touch provisioning. Next, you will discover the tools available on FortiManager and FortiAnalyzer to monitor your SD-WAN deployment.


Vouchers & Dumps are Available | WhatsApp +201224560923

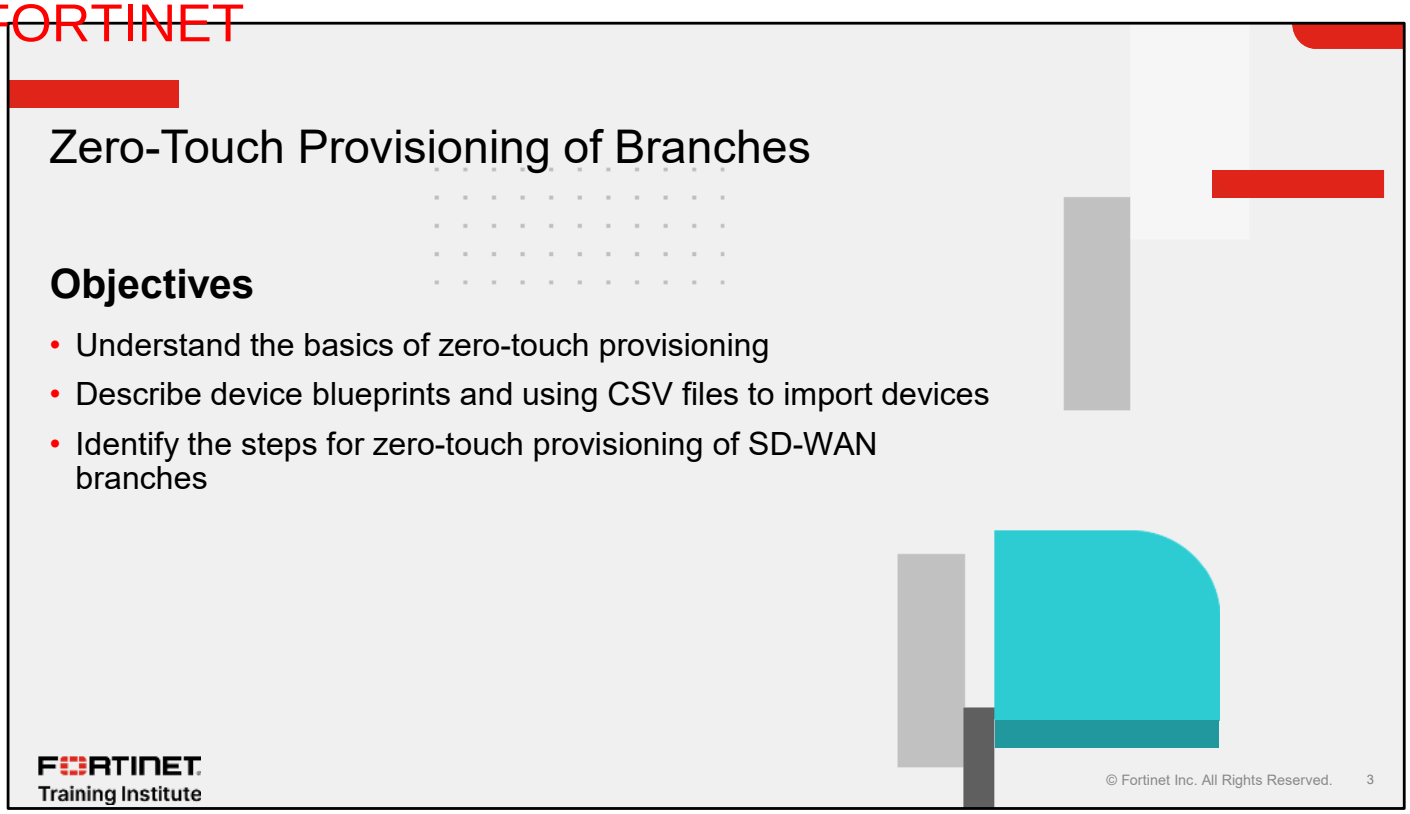
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the concept of zero-touch provisioning for your SD-WAN branches, you will be able to make large deployments easier and more efficient.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## What Is Zero-Touch Provisioning?

- Groups multiple techniques and tools to easily deploy FortiGate devices
- FortiManager provides detailed and personalized configuration to each FortiGate

- Two flavors
  - Zero-Touch Provisioning (ZTP): no preconfiguration of FortiGate required
    - Automated configuration of network settings with DHCP
  - Low-Touch Provisioning (LTP): limited preconfiguration of FortiGate required
    - Manual configuration of network settings and location of FortiManager




- Foundation for ZTP and LTP
  - Device blueprint
  - Provisioning templates
  - List of variable values for each device (CSV file)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

Usually, an SD-WAN project involves many FortiGate branch devices, and sometimes hundreds of devices. To simplify the deployment of those devices, you can use FortiManager and zero-touch provisioning (ZTP) or low-touch provisioning (LTP) techniques. ZTP or LTP deployments combine tools and features available on FortiManager, such as device blueprints, provisioning templates, and metadata variables with CSV files, to install a personalized configuration on each FortiGate device.

The difference between ZTP and LTP resides in the level of configuration that the administrator performs on the FortiGate device. With ZTP, the administrator does not perform any configuration on FortiGate. At power on the device obtains its IP address, netmask, and the gateway address from a DHCP server. At the same time, the DHCP server, using DHCP option 240/241, informs FortiGate about FortiManager. IP address and credentials. With LTP, the administrator performs basic configuration of FortiGate, such as the management interface IP address, default route, and FortiManager IP address and connection credentials. Then, FortiManager installs the detailed configuration on the FortiGate device, with detailed routing, SD-WAN rules, firewall policies, and so on.

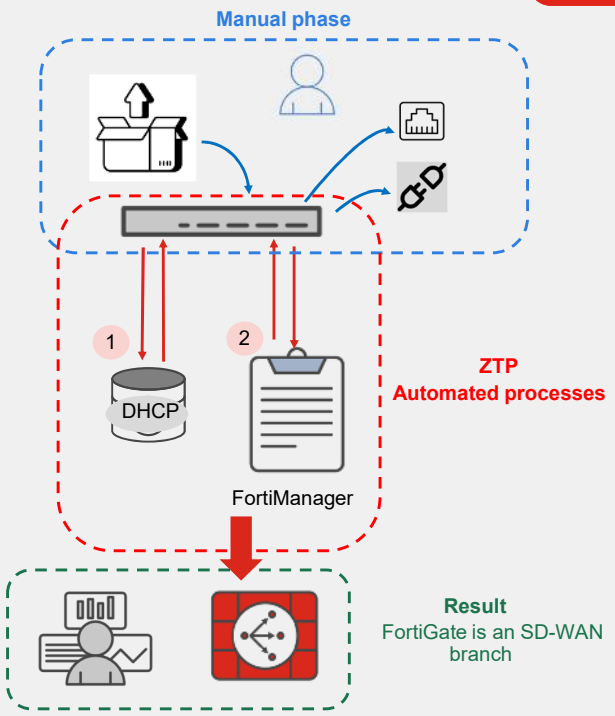
The foundation for ZTP and LTP includes the provisioning templates, which you learned about in the previous lesson, and device blueprints and CSV files, which you will learn about in this lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## ZTP Process—a New Branch

- Physically connect the FortiGate device
  - Power cord
  - Network interfaces
- Turn on the device
- Automatic process starts
  - DHCP
    - Retrieve interface IP address and gateway
    - Retrieve FortiManager IP address
  - Connect to FortiManager
    - Auto-accept the device
    - Auto-push
      - Firmware image
      - Configuration elements
- Check FortiManager monitors
  - Confirm the device settings and connectivity




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

This slide shows an overview of the ZTP process.

After the administrator completes the preparation work, which includes preparing templates, defining blueprints, and loading the model devices with a CSV file, the ZTP process can start. Anyone with limited, or even no knowledge of FortiGate can deploy a new branch. The only required tasks that must be done manually are unpacking the device, connecting the power cord and the network interfaces, and then turning on the device.

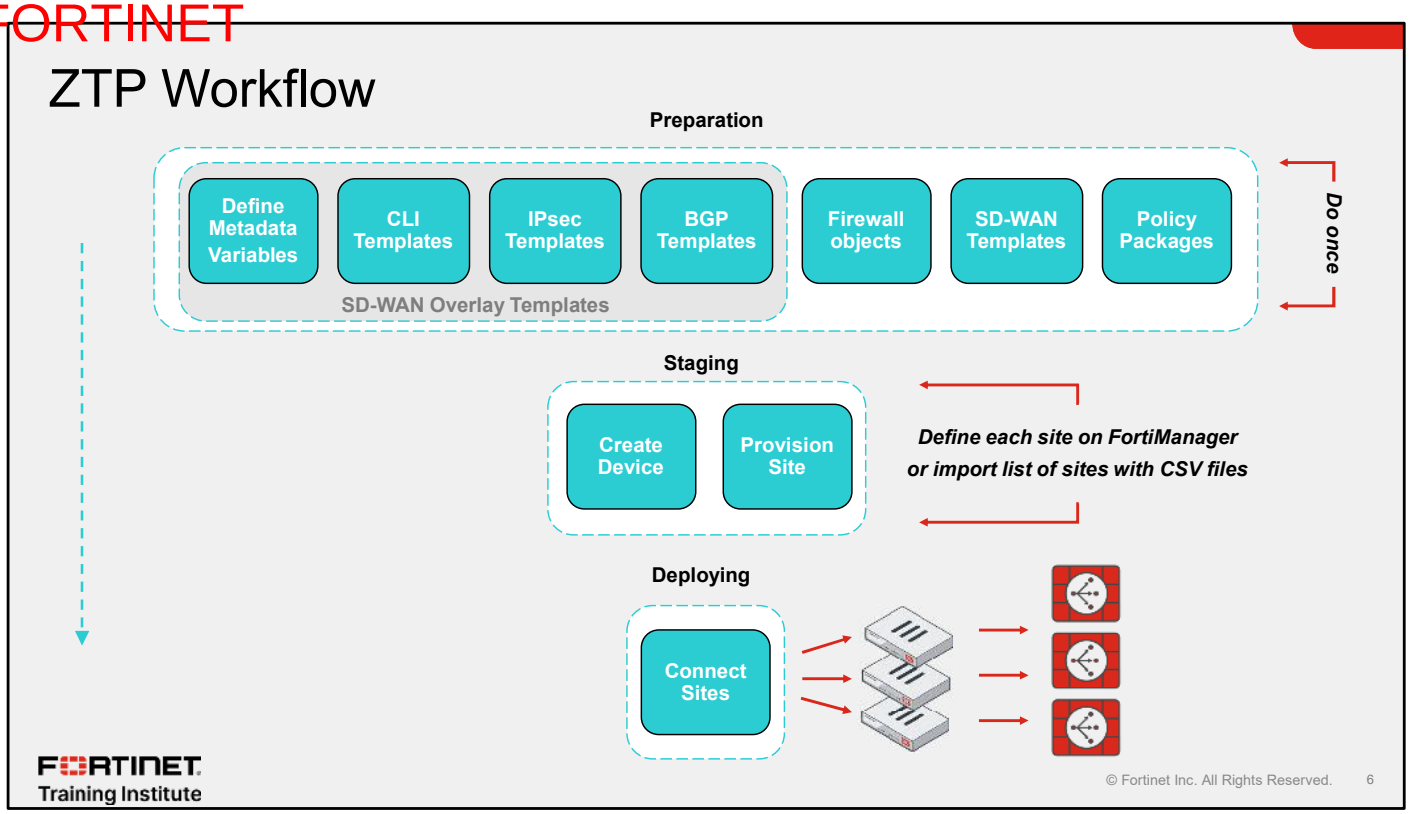
After the device is connected to the network, the configuration work starts automatically running in the background. First, FortiGate connects to the DHCP server and retrieve its basic network configuration, interface IP address and gateway address, FortiManager IP address. Then, FortiGate connects to FortiManager. FortiManager automatically authorizes the device; if required, installs a new firmware image; and then pushes the configuration elements that were specially defined by the administrator for this device. The new FortiGate device is now part of the network, and its configuration is ready with routing, firewall policies, and much more.

The ZTP process for a FortiGate VM differs only in the initial phase. Instead of unpacking the device, the administrator defines the VM device and installs the device license.

As precautionary measure, on the FortiManager monitors panels, the administrator should the review the device onboarding to confirm that the process was successful and that all settings appear as expected.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




The diagram on this slide summarize the steps required to configure ZTP deployments of SD-WAN branches.

First, the administrator defines the topology and prepares the configuration elements, such as the routing, overlay tunnels, SD-WAN template, policy objects, and policy packages. The SD-WAN overlay template can be very helpful in completing those tasks. The administrator needs to perform those configuration task only once for each SD-WAN deployment.

Then, the administrator provisions the sites on FortiManager, defining each of them with the device serial number and the device name. For this task, the administrator can prepare a CSV file, listing all devices with the corresponding variable values and, in a few clicks, load the file on FortiManager.

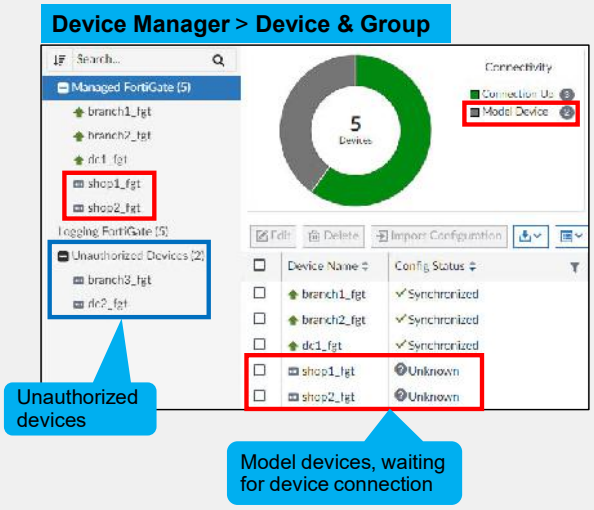
Lastly, when technicians connect each site, FortiManager automatically recognizes the sites and load the desired configuration on each one.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Device Blueprints

- Create a device model
  - Per hardware or VM device model
  - Store configurations to assign to devices not yet online
- After FortiGate powers on and connects to FortiManager
  - FortiManager checks whether corresponding device model exists
  - If yes:
    - FortiManager authorizes FortiGate for management
    - If there are multiple device models, make selections according to information in CSV file
    - Enforce firmware version if applicable
    - Configuration process starts
  - If no:
    - FortiManager adds the device to the unauthorized device list
    - No further action, waiting for the administrator




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Device blueprints can simplify new deployments that use multiple devices of the same type and with similar configurations. Device blueprints allow you to predefine various parameters for a FortiGate device model, such as firmware version, assigned templates, or policy packages.

You can use device blueprints in conjunction with an imported CSV file to specify the blueprint to use for each serial number, and define values for metadata variables for each device.

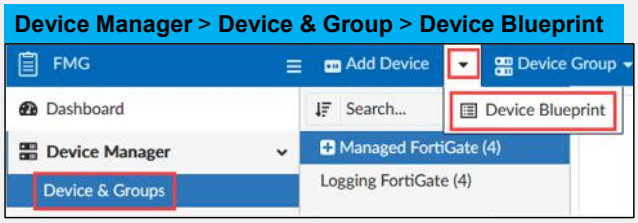
Device blueprints simplify the task of adding FortiGate devices to FortiManager. When FortiManager receives a connection request from an unregistered FortiGate device, and no corresponding blueprint exists, it adds the device to the unauthorized device list, and waits for the administrator to authorize and configure the device. If a blueprint for the device type exists, FortiManager automatically authorizes the device for management and applies the configuration and firewall polices as defined in the blueprint.

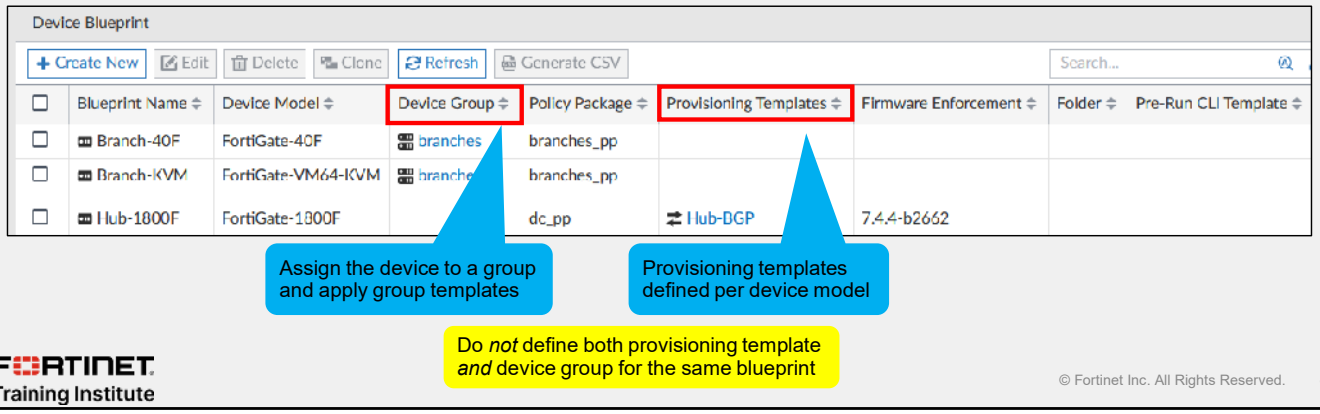

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Device Blueprint Configuration

- Define for each device model, as required
  - Enforce firmware version
  - Add device to group
  - Pre-run CLI template
  - Assign policy package
  - Assign provisioning template




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

You can define a device blueprint and check the device blueprint list as this slide shows.

For each device blueprint, you can define multiple parameters for each device model, such as:

- **Automatically Link to Real Device**: is also called auto-link, and is required for ZTP/LTP.
- **Enforce Firmware Version**: automatically upgrades or downgrades the device to the specified version, before applying other configuration changes to the device.
- **Enforce Device Configuration**: allows auto-link to push changes on FortiGate management interface during ZTP/LTP. Be careful with the configuration of the management interface because misconfiguration can break the connectivity between FortiGate and FortiManager.
- **Pre-Run CLI Template**: chooses a template that runs on the device before other provisioning templates.
- **Assign Policy Package**: selects the policy package for the device.
- **Provisioning Templates**: selects the provisioning templates or templates group to assign to the device.

Note that if you decide to assign the devices to a group, they will inherit all templates associated with that device group. Therefore, to avoid the risk of conflicting configuration instructions, you should either assign provisioning templates or add devices to the group to benefit from group templates. You should not do both on the same blueprint.

You can define multiple blueprints for a same model device. If you do so, to allow FortiManager to determine which template to assign to each device, you can load a CSV file that defines the template to use for each serial number.

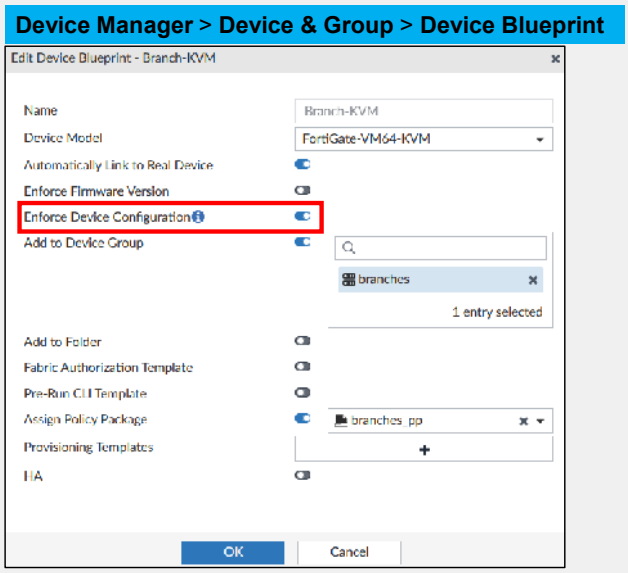


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Enforce Device Configuration

- Device blueprint option
- Enable
  - Allows FortiManager to change the configuration of the interface used by the FortiGate device to connect to FortiManager
  - Useful to adjust the interface configuration, such as set interface alias or interface speed
  - Warning: Misconfiguration can break the connectivity between FortiManager and FortiGate
- Disable
  - Prevent any configuration change of interface used to connect to FortiManager during ZTP/LTP process




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

**Enforce Device Configuration** is a parameter of the device blueprint wizard. It allows the administrator to define FortiManager behavior related to the interface used by FortiGate to connect to FortiManager. This setting applies only during the ZTP/LTP process.

For example, port1 is the interface used by FortiGate to FortiManager. The blueprint applicable to this FortiGate device assigns a CLI template that defines an alias for port1. If **Enforce Device Configuration** is enabled, FortiManager will set the alias a port1 attributes during the ZTP process. If disabled, FortiManager will not configure port1 with the alias.

You must be careful when enabling this parameter. Misconfiguration of the interface used by FortiGate to connect to FortiManager, such as setting an incorrect IP address or gateway, can break the connectivity between the two devices and cause the ZTP process to fail.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Declare Branch Devices Using a CSV File

- Why use CSV file?
  - Bulk import of devices to FortiManager
  - Easy CSV file creation
  - Simplify large deployments
- What does the file contain?
  - The serial number for each FortiGate device
  - To device blueprint to use
  - The value for each metadata variable used
- CSV file elements
  - Required
    - Device serial number
    - Blueprint
    - Device name
  - Required for VM models
    - Number of ports to provision
  - Required for SD-WAN template
    - Branch_id
  - Optional
    - Value for each metadata variable in use in referenced template or configuration element

**CSV file example ***

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | serial number | device blueprint | name | vm_interface_number | branch_id | admin_gw | sdwan_port1_gw | sdwan_port2_gw |
| 2 | FGVM01TM22000 | Branch-KVM | branch1_fgt | 10 | 1 | 172.16.0.2 | 192.2.0.2 | 192.2.0.10 |
| 3 | FGVM01TM22000 | Branch-KVM | branch2_fgt | 10 | 2 | 172.16.0.10 | 203.0.11.2 | 203.0.113.10 |
| 4 | FG30EI3U160006( | Branch-30E | shop1_fgt | | 11 | 172.18.0.1 | 198.0.1.1 | 198.10.1.1 |
| 5 | FG30EI3U160004 | Branch-30E | hop2_fgt | | 12 | 172.18.0.1 | 198.0.1.1 | 198.10.1.1 |

Required fields | For VMs | For SD-WAN branches | Values for metadata variables

FORTINET Training Institute

* displayed in excel for better readability

© Fortinet Inc. All Rights Reserved. 10

For a large SD-WAN deployment, adding each branch device one by one would be repetitive and time consuming. Fortunately, to simplify this step, FortiManager provides a CSV file import feature.

To use this bulk import feature, the administrator builds a CSV file. The file must contain some mandatory values, such as the device serial numbers, the device names, and the associated blueprints, as well as optional values for the metadata variables used in the configuration.

Additionally, according to the type of device and its usage, the file must contain the following values:
- For VM models, the number of interfaces
- For SD-WAN branches, the branch id—or use the auto assign branch ID feature
- For HA clusters, the cluster ID, the cluster name, the device HA priority, and the HA mode

The CSV file must be built with column headers and the corresponding list of values. The first columns must be: **serial number**, **device blueprint**, **name** and, for VMs, **vm_interface_number**. Additional, optional column names must match exact metadata variable names.

On file import, FortiManager sets metadata variable values for every predefined value and ignores columns that match already defined metadata variables.

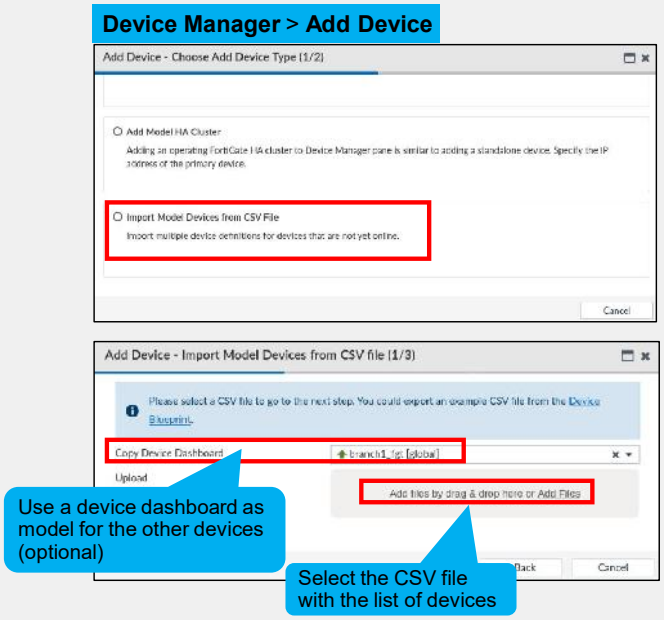
Note that the **Add Model Device** and **Import Model devices from CSV file** modes are intended for new FortiGate deployments, where no pre-existing configuration on the FortiGate device must be preserved. The configuration associated with the model device overwrites the configuration of the FortiGate device as part of the installation process, after FortiManager authorizes the FortiGate device.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Import Model Devices From CSV Files

- Simultaneously import multiple devices
  - Beginning of a project
  - Major extension
- FortiManager detects devices already in production
  - Trigger warning at file import
  - Ignore the corresponding line
- FortiManager provision the device
  - Ready to manage
  - Not placed in the unauthorized device list at initial connection




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

After you complete the CSV file preparation as described on the previous slide, you will import it on FortiManager using the **Add Device**, **Import Model Devices from CSV File** feature. Through the import process, FortiManager detects any serial number that corresponds to an already managed device. It prompts the administrator for a review and ignore the lines. By ignoring lines for devices that are already managed, FortiManager prevents potential configuration override on production device.

Optionally, when importing device models from CSV files, you can select a device, already managed by FortiManager, as the dashboard model. Then, FortiManager will define a similar custom dashboard for all devices onboarded from the CSV file.

On file import, FortiManager adds each device defined in the list and places them in the managed device list. When FortiGate makes it first connection to the FortiManager, it does not go through the unauthorized device list, it is directly recognized as a managed device.



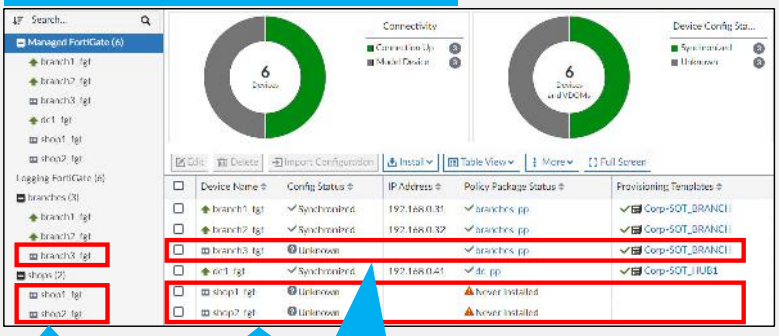
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Import Model Devices From CSV Files—Results

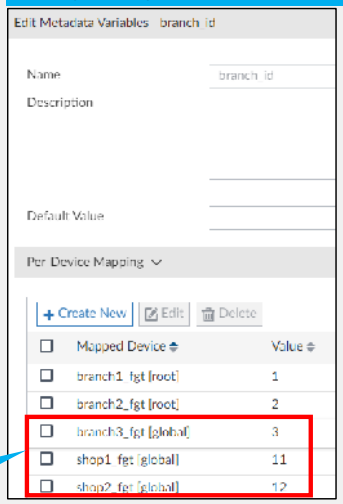
- Model devices created and ready to be managed

**Device Manager > Devices and Groups**




- Metadata variable updated with per-device mapping

**Policy & Objects > Advanced > Metadata**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

After you import model devices from CSV files, the model FortiGate devices are placed in the managed FortiGate list. You can identify them by the grey device icon.

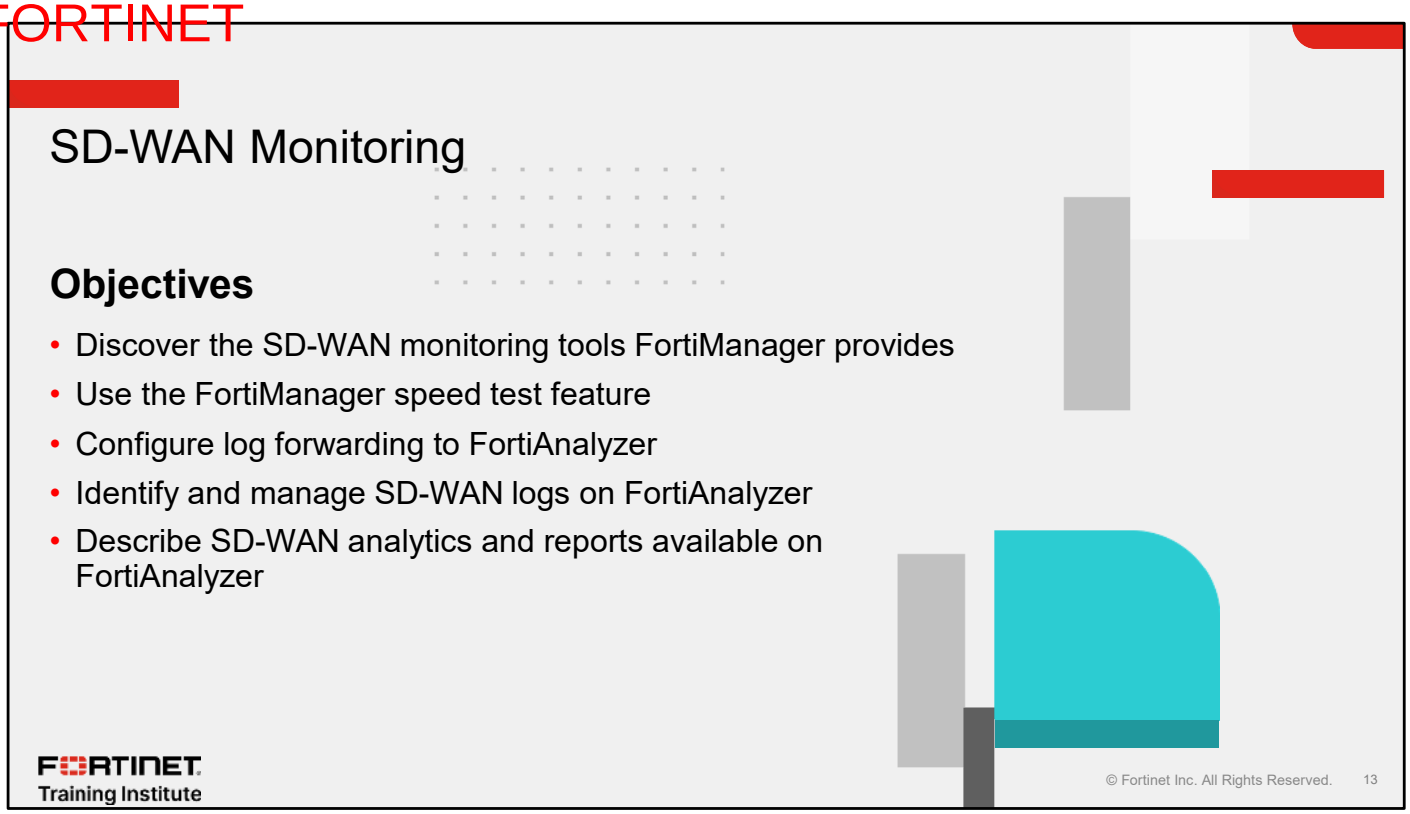
If defined in the CSV file, or in the device model associated to each device, you can also see the following information for each model device:

- Its device groups
- The assigned policy package
- The provisioning template
- The metadata per-device mapping value

Note that, if you install a policy package on a model device, FortiManager performs validation checks and installs the corresponding settings in the device database. Once it completes these tasks, FortiManager marks the policy package status with a green check.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the monitoring tools provided by FortiManager and the logging and reporting features available on FortiAnalyzer for SD-WAN, you will be able to monitor the health and performance of all FortiGate devices in your network easily and with centralized views.

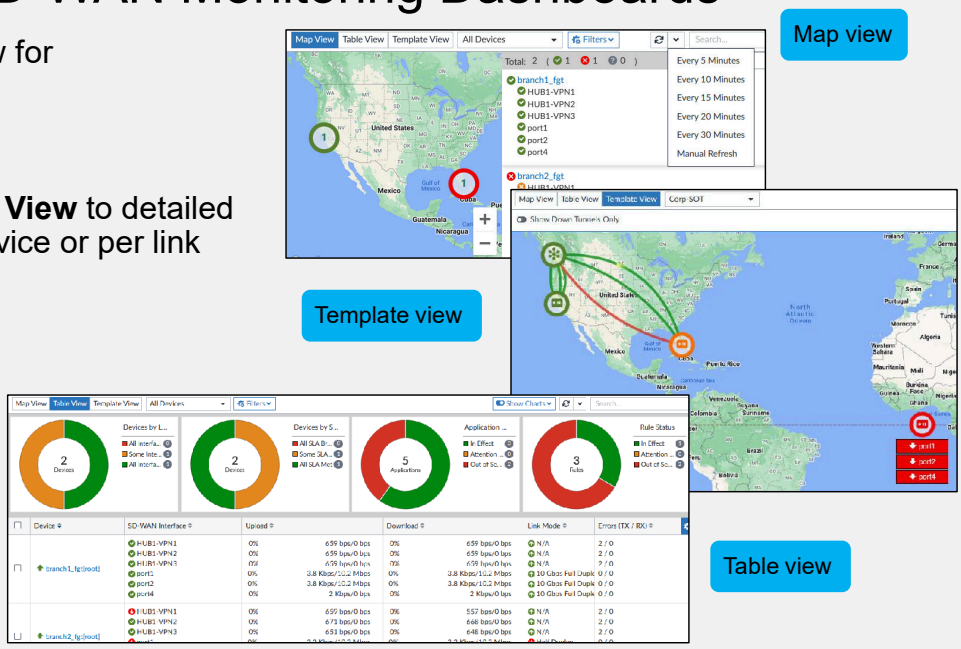


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# FortiManager SD-WAN Monitoring Dashboards

- Table and graphical view for
  - SD-WAN device status
  - SD-WAN link status
  - VPN tunnel status
- Easy to move from **Map View** to detailed information pane per device or per link
- Easy filter
  - Per unhealthy link
  - Per unhealthy device
  - Per rule status




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

FortiManager offers multiple dashboards so that you can view, on one page, the health, settings, and behavior of all managed SD-WAN devices. You will learn more about these dashboards in this lesson.

Some handy features are that are common to all dashboards, include the ability to:

- Click on a sector graph to filter devices with the same status.
- Double-click a device or link in a map or table to display a detailed information pane about the device or link.
- Easily filter the view to show only unhealthy links or devices.

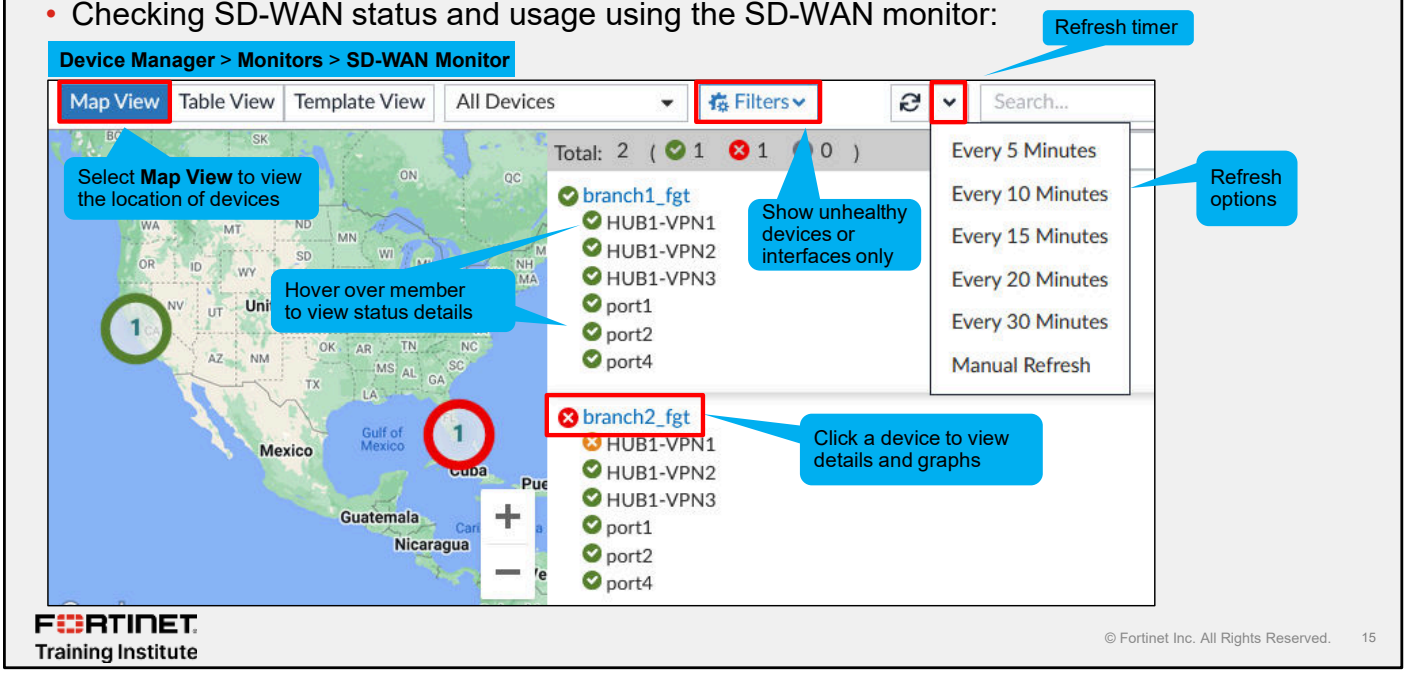


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Checking SD-WAN Status

- Checking SD-WAN status and usage using the SD-WAN monitor:




After you install the SD-WAN settings and relevant configuration on FortiGate, you can use the **SD-WAN Monitor** page on FortiManager to view the status of the FortiGate devices and their SD-WAN members. Filters allow you to display only unhealthy devices or links. Note that, by default, you must manually refresh the page to poll the latest status from the device. Alternatively, you can select an automatic refresh interval.

The **Map View** shows the location of devices on a map. The location is based on the location settings configured for the device on FortiManager.

Hover over a member to view its health and utilization details. Note that the member utilization percentage is calculated based on the values configured for the `estimated-upstream-bandwidth` and `estimated-downstream-bandwidth` interface settings. You will learn more about these settings in another lesson.

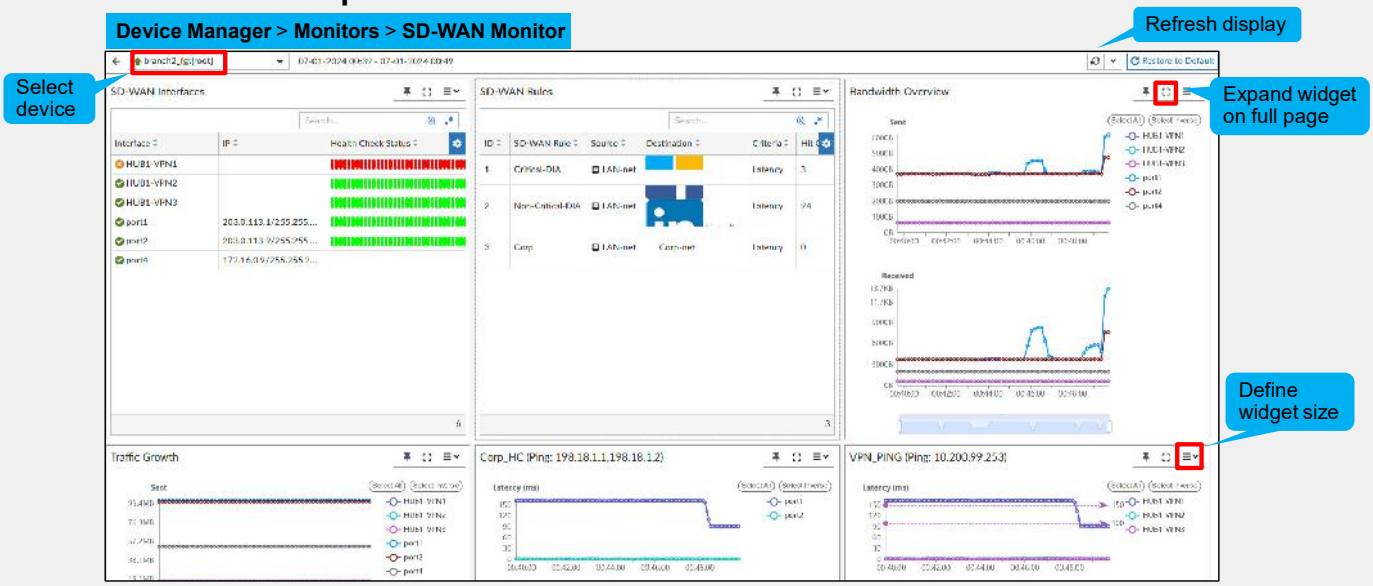
Finally, you can click a device to view historical graphs reporting on the member utilization and health. The next slide shows an example of those graphs.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Monitor—Device Details

- Click a device in **Map View** or **Table View** to see details




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

The example on this slide shows the graphs displayed when you click a device in the SD-WAN monitor **Map View** or **Table View**. FortiManager displays historical graphs reporting on the utilization and health of the SD-WAN members on that device.

You can customize the view by selecting the size of each widget, reorganizing the widgets, and configuring the page refresh frequency.



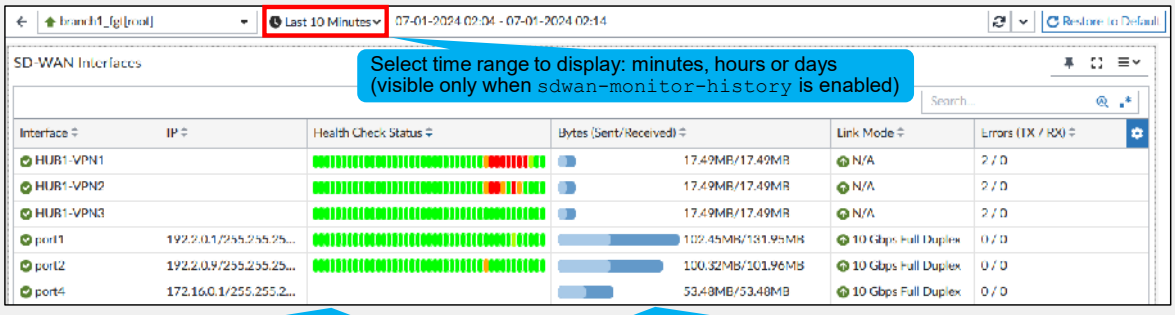
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Monitor—Device Details (Contd)

- Device details shows member utilization and health graphs
- Default display for past 10 minutes
- For statistics over an extended time period, enable the SD-WAN history monitor, and define the maximum number of storage days (default 180 days) with CLI commands:

```
config system admin setting
    set sdwan-monitor-history enable
    set rtm-max-monitor-by-days <nb of days>
end
```




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

By default, FortiManager displays the device and interface statistics for the past 10 minutes only. To collect and display data over an extended time period, you must enable data storage on the FortiManager disk using the following CLI commands:

```
config system admin setting
      set sdwan-monitor-history enable
end
```

You will be able to select the time period to display only if the history monitor is enabled. To help with forensics analysis, you can select to display the statistics for the last few minutes, hours, or days, or any manually defined time period.

Note that once you activate the feature, FortiManager stores the data on its disk for each managed SD-WAN device for up to 180 days. To avoid excessive disk usage, you can reduce the data conservation to only a few days with the following CLI commands:

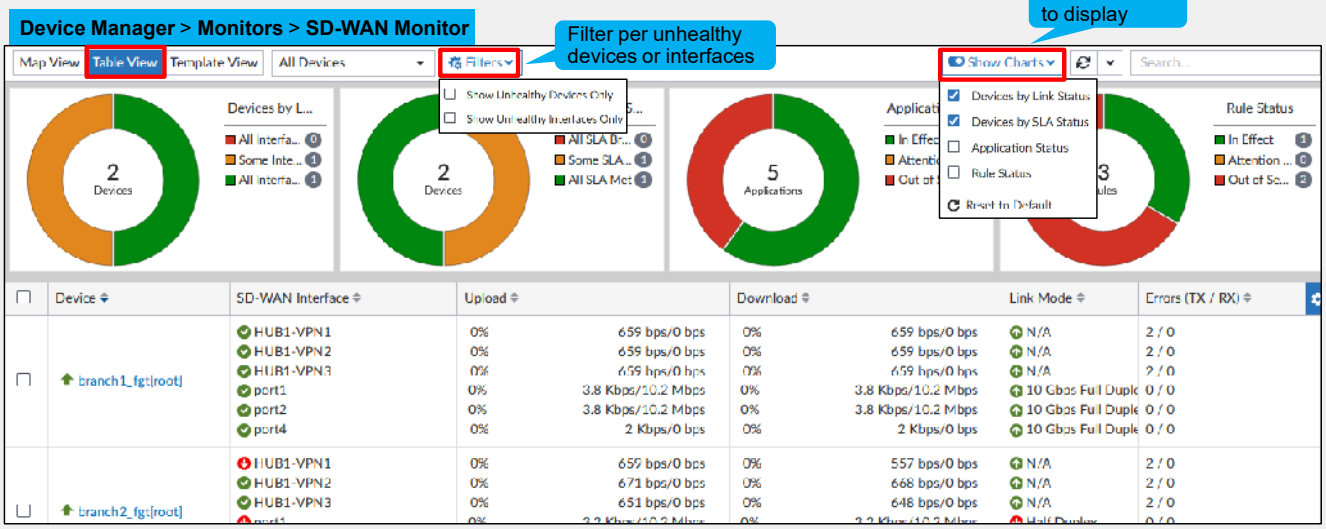
```
config system admin setting
      set rtm-max-monitor-by-days <nb of days>
end
```


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# SD-WAN Monitor—Table View

- Graphical summary view and table summary per device




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

The SD-WAN monitor **Table View** displays sector graphs to quickly visualize the number of devices for each link, SLA, application, and rule status. You can personalize the charts displayed on your dashboard. Click sectors from those graphs to filter the device list.

In the table, you get information about the SD-WAN interfaces for each device, such as interface names, link mode, and upload and download volumes

Click a device in the list to display the device details, as shown on the previous slides.

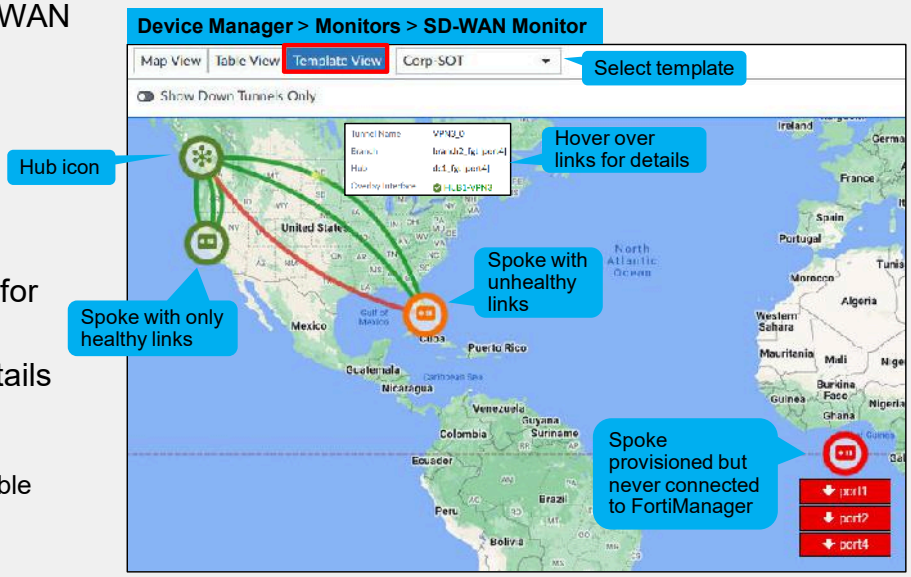


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Monitor—Template View

- Topology view for each SD-WAN overlay template
- Shows:
  - Hubs
  - Spokes
  - Provisioned devices
  - Link status
- Hover over links or devices for details
- Click links or devices for details
  - SD-WAN health-check table
  - IPsec VPN table
  - Static and dynamic routing table




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

With the SD-WAN monitor template view, you can visualize, on a map, all devices associated with an SD-WAN overlay template.

The template view shows on a world map:
- The hub devices represented by a star icon
- The spoke devices represented by a device icon
- The tunnels established between the devices

The line colors represent the tunnel status:
- Green: The tunnel is up
- Red: The tunnel is down

The device icon can take three colors according to the interface health check status:
- Green: All health checks pass.
- Orange: Some health checks pass.
- Red: All health checks fail.

The device position on the map corresponds to the longitude and latitude values provided by the administrator at device registration. If no data is provided, or if the device was provisioned but never connected to FortiManager, it is displayed with position 0-0, as this slide shows.

Hover over devices or links to display additional information. Click links or devices to view detailed information. For example, clicking a spoke device displays a pane with the SD-WAN health check table, underlay status table, static and dynamic routing table, and IPsec VPN table.

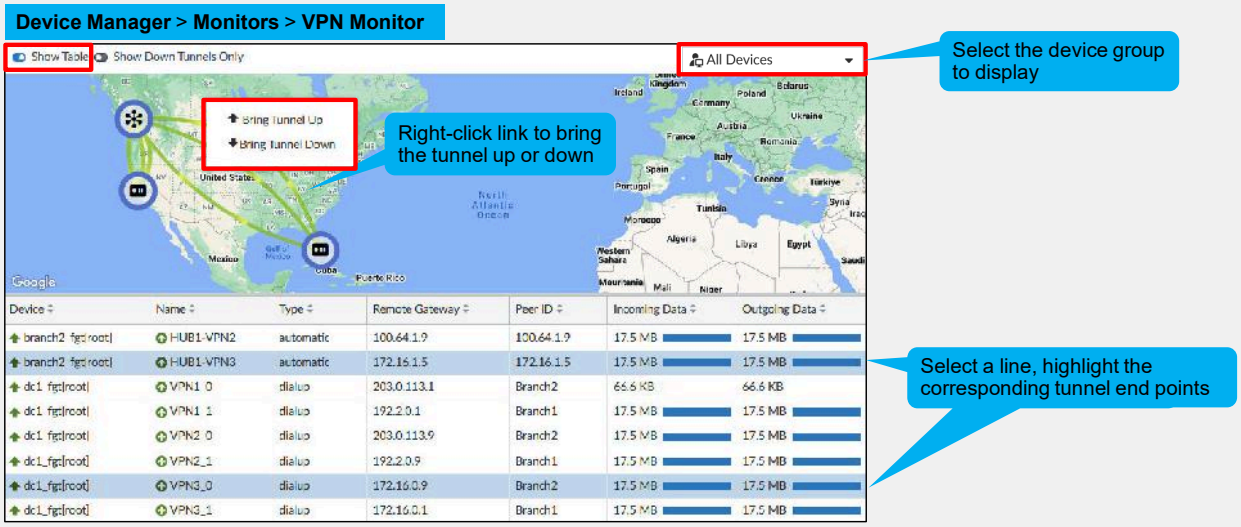


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Overlay Monitoring

- To see overlay tunnel details, on the **VPN Monitor** page, enable **Show Table**
- Select a line or a link on the map to force a tunnel down or up




The **VPN Monitor** page displays IPSec VPN tunnels created by IPsec templates and the SD-WAN overlay wizard with specific device icon identification for hub devices. On this page, you can monitor the tunnel status. You can force a tunnel up or down on the **VPN Monitor** page, by a right-click on links from the **Map View** as this slide shows, or by selecting a line in the tunnel list.

Note that in the table view, if you select a line, FortiManager automatically highlights the line that corresponds to the other end of the tunnel, as this slide shows.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

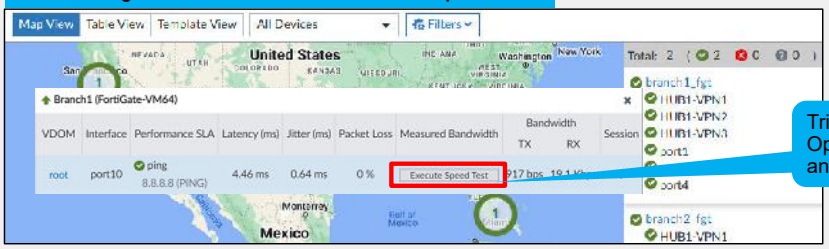
## Cloud-Assisted Speed Tests

- Cloud-assisted monitoring service
- Launch from FortiGate or FortiManager
- Requires license for each FortiGate
  - SD-WAN Network Monitor
- Available for SD-WAN members
- Interfaces with WAN role only
- Max 10 speed tests per interface per day

FortiGate: **System** > **FortiGuard**




**Device Manager** > **Monitors** > **SD-WAN Monitor** > **Map View**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

From the SD-WAN monitor map view, you can launch cloud-assisted speed tests for the SD-WAN interfaces and review the results. FortiGate performs those tests against Fortinet-maintained cloud servers globally. Usually, you use speed tests to determine the available bandwidth results for QoS policies and traffic shapers, to enhance network performance when links are congested. Because QoS and traffic shapers are generic methods used in various situations, this course doesn't cover them.

Note that the cloud-assisted speed test is a subscription service. FortiManager displays the **Measured Bandwidth** column and the **Execute Speed Test** button only when the service is available. This involves a FortiGate devices with a valid SD-WAN network monitor license and an interface with WAN role, set as an SD-WAN member.

Run cloud assisted speed tests on demand, with up to 10 speed tests for each interface and day. FortiGate uses the cached result values between those tests.

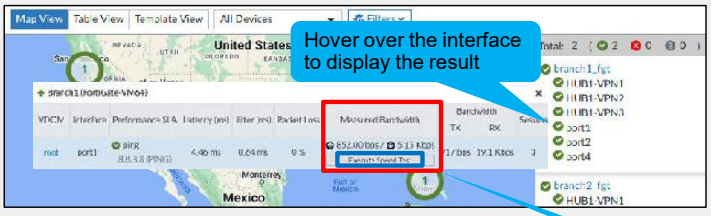


Vouchers & Dumps are Available | WhatsApp +201224560923

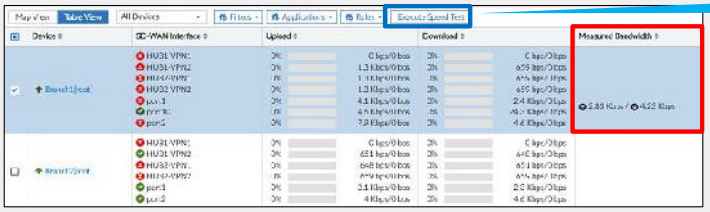
DO NOT REPRINT Brave-dumps.com
© FORTINET

# Speed Tests—Result Display

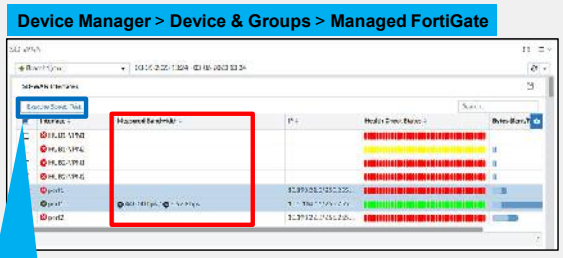
- On the **SD-WAN Monitor** page, **Map View**




- On the **SD-WAN Monitor** page, **Table View**



- Per FortiGate Device, on the **Network Monitor** dashboard




Trigger new test

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

This slide shows where you can review the cloud-assisted speed test results, and trigger a new test.

- On the SD-WAN monitor page **Map View**, hover your mouse over the interface to display detailed information, including the measured bandwidth. You can trigger a new speed test from the menu displayed.
- On the SD-WAN monitor page **Table View**, the **Measured Bandwidth** column shows speed test results for every interface already analyzed.
- In the **Managed FortiGate** list, you can navigate the **Network Monitors** dashboard by FortiGate device. The **Measure Bandwidth** column appears in the SD-WAN interface list for devices that have a valid Network Monitor license. Note that you must activate the SD-WAN display widget to see the SD-WAN interface list on the **Network Monitor** dashboard.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Hub-and-Spoke Speed Tests

- Hub (or spoke) as speed test server
  - Both units participate
- No license required
- Upload or download direction
- TCP or UDP protocol
- Results cached for future use
- Enabled with CLI commands
- Common use case: Adjust traffic shaper according to the speed test results

- Enable the speed test server

```
config system global
    set speedtest-server enable
    set speedtestd-server-port <integer> [default 5201]
    set speedtestd-ctrl-port <integer> [default 5200]
end
```

- Enable the speed test client

```
config system speed-test-schedule
    edit <interface>
        set dynamic-server {enable | disable}
        set ctrl-port <integer> [default 5200]
        set server-port <integer> [default 5201]
        set update-shaper {disable|local|remote|both}
   next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

In hub-and-spoke topologies, FortiGate allows you to perform speed tests between devices. This is a CLI-only feature that does not require an additional license. Configure one of your devices, usually the hub, as a speed test server, and configure another device as the test client. This slide shows the commands you use to configure this feature.

You can initiate speed tests from the hub or from the spoke side. When you initiate a speed test from the hub, FortiGate caches the results on the hub. When you initiate the speed test from the spoke, FortiGate caches the results on the spoke, and sends them to the hub.

Similar to cloud-based testing results, use the hub-and-spoke speed test results to apply QoS and traffic shaping on the interface. This feature is not required for SD-WAN topologies.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Hub-and-Spoke Speed Tests (Contd)

- Enable speed test on the interface
  - On the hub and on the spoke side
  - For each interface involved: underlay and overlay

```
config system interface
   edit port1
      set allowaccess speed-test ping https ssh
   next
   edit HUB1_VPN1
      set allowaccess speed-test ng https ssh
   next
end
```

Enable `speed-test` on overlay and underlay interfaces

- Bypass routing on SD-WAN member when speed test is ongoing
  - Optional
  - Allow SD-WAN to direct traffic to other members when a speed test ongoing
  - Preserve the speed the test results from the impact of traffic between the spoke and the hub

```
config system sdwan
   set speedtest-bypass-routing enable
end
```

Default setting: `disable`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

Each incoming speed test request must present the obtained access token to prevent random, unauthorized requests. Otherwise, FortiGate closes the connection immediately. As such, you must enable speed test access must on both the underlay and the IPsec overlay tunnel interfaces with the command `set allowaccess speed-test` as shown on this slide. If you configured the IPsec tunnel with `exchange-ip`, you mut enable speed test access also on the associated interface. Similarly, you must enable speed-test, on any interfaces involved, such as loopback interfaces

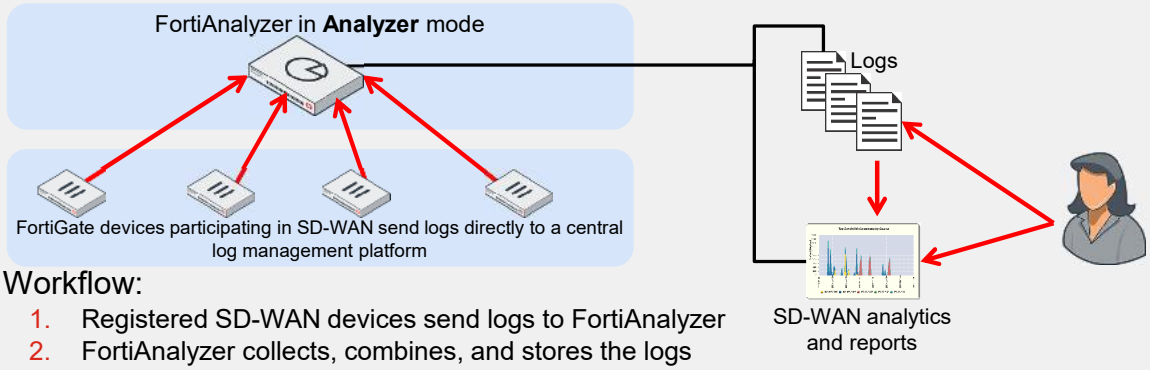
Optionally, you can configure SD-WAN to not steer traffic through a member when it participates to speed tests. With the command `speedtest-bypass-routing enable`, you instruct FortiGate to stop steering the traffic through an SD-WAN member that is used for a speed test. This applies the member is on speed test from the hub to the spoke.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## What Is FortiAnalyzer?

- Centralized log repository
  - Aggregates log data from one or more Fortinet devices, including SD-WAN logs
  - Creates a single view of SD-WAN events taking place on a range of devices




- Workflow:
  1. Registered SD-WAN devices send logs to FortiAnalyzer
  2. FortiAnalyzer collects, combines, and stores the logs
  3. Administrators:
     - View logs for SD-WAN
     - View analytics for SD-WAN
     - Configure, request, and view reports for SD-WAN (based on log data)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

FortiAnalyzer aggregates log data from one or more Fortinet devices, including FortiGate devices that participate in SD-WAN. FortiAnalyzer acts as a centralized log repository and provides a single channel for accessing your complete SD-WAN network data, so you don't need to access multiple SD-WAN devices several times a day.

The logging and reporting workflow operates as follows:

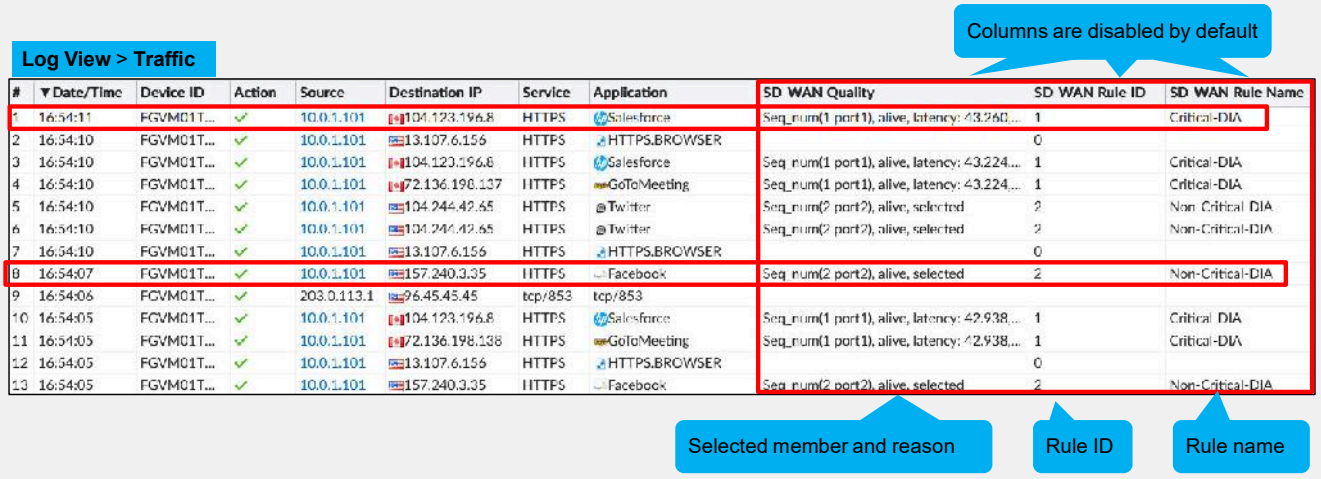
1. Registered SD-WAN devices send logs to FortiAnalyzer.
2. FortiAnalyzer collects, combines, and stores SD-WAN logs in a way that makes it easy to search and run reports.
3. Administrators can connect to the FortiAnalyzer GUI to view SD-WAN logs, analytics, and reports.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Traffic Logs

- Enable SD-WAN columns to differentiate SD-WAN sessions from non-SD-WAN sessions




| # | Date/Time | Device ID | Action | Source | Destination IP | Service | Application | SD-WAN Quality | SD-WAN Rule ID | SD-WAN Rule Name |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 16:54:11 | FGVM01T... | ✓ | 10.0.1.101 | 104.123.196.8 | HTTPS | Salesforce | Seq_num(1 port1), alive, latency: 43.260,... | 1 | Critical-DIA |
| 2 | 16:54:10 | FGVM01T... | ✓ | 10.0.1.101 | 13.107.6.156 | HTTPS | HTTPS.BROWSER | | 0 | |
| 3 | 16:54:10 | FGVM01T... | ✓ | 10.0.1.101 | 104.123.196.8 | HTTPS | Salesforce | Seq_num(1 port1), alive, latency: 43.224,... | 1 | Critical-DIA |
| 4 | 16:54:10 | FGVM01T... | ✓ | 10.0.1.101 | 72.136.198.137 | HTTPS | GoToMeeting | Seq_num(1 port1), alive, latency: 43.224,... | 1 | Critical-DIA |
| 5 | 16:54:10 | FGVM01T... | ✓ | 10.0.1.101 | 104.244.42.65 | HTTPS | Twitter | Seq_num(2 port2), alive, selected | 2 | Non-Critical-DIA |
| 6 | 16:54:10 | FGVM01T... | ✓ | 10.0.1.101 | 104.244.42.65 | HTTPS | Twitter | Seq_num(2 port2), alive, selected | 2 | Non-Critical-DIA |
| 7 | 16:54:10 | FGVM01T... | ✓ | 10.0.1.101 | 13.107.6.156 | HTTPS | HTTPS.BROWSER | | 0 | |
| 8 | 16:54:07 | FGVM01T... | ✓ | 10.0.1.101 | 157.240.3.35 | HTTPS | Facebook | Seq_num(2 port2), alive, selected | 2 | Non-Critical-DIA |
| 9 | 16:54:06 | FGVM01T... | ✓ | 203.0.113.1 | 96.45.45.45 | tcp/853 | tcp/853 | | | |
| 10 | 16:54:05 | FGVM01T... | ✓ | 10.0.1.101 | 104.123.196.8 | HTTPS | Salesforce | Seq_num(1 port1), alive, latency: 42.938,... | 1 | Critical-DIA |
| 11 | 16:54:05 | FGVM01T... | ✓ | 10.0.1.101 | 72.136.198.138 | HTTPS | GoToMeeting | Seq_num(1 port1), alive, latency: 42.938,... | 1 | Critical-DIA |
| 12 | 16:54:05 | FGVM01T... | ✓ | 10.0.1.101 | 13.107.6.156 | HTTPS | HTTPS.BROWSER | | 0 | |
| 13 | 16:54:05 | FGVM01T... | ✓ | 10.0.1.101 | 157.240.3.35 | HTTPS | Facebook | Seq_num(2 port2), alive, selected | 2 | Non-Critical-DIA |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

The **Forward Traffic** logs page is useful to identify how FortiGate distributes sessions in SD-WAN and the reason. Make sure to enable the **SD-WAN Rule Name** and **SD-WAN Quality** columns, which are disabled by default. The former indicates the matched SD-WAN rule for a session, and the latter indicates the member the session was steered to and the reason. You can also enable the **SD-WAN Rule ID** column and, when applicable, the **SD-WAN Internet Service** column. Note that SD-WAN rule ID 0 corresponds to traffic steered according to the default SD-WAN rule.

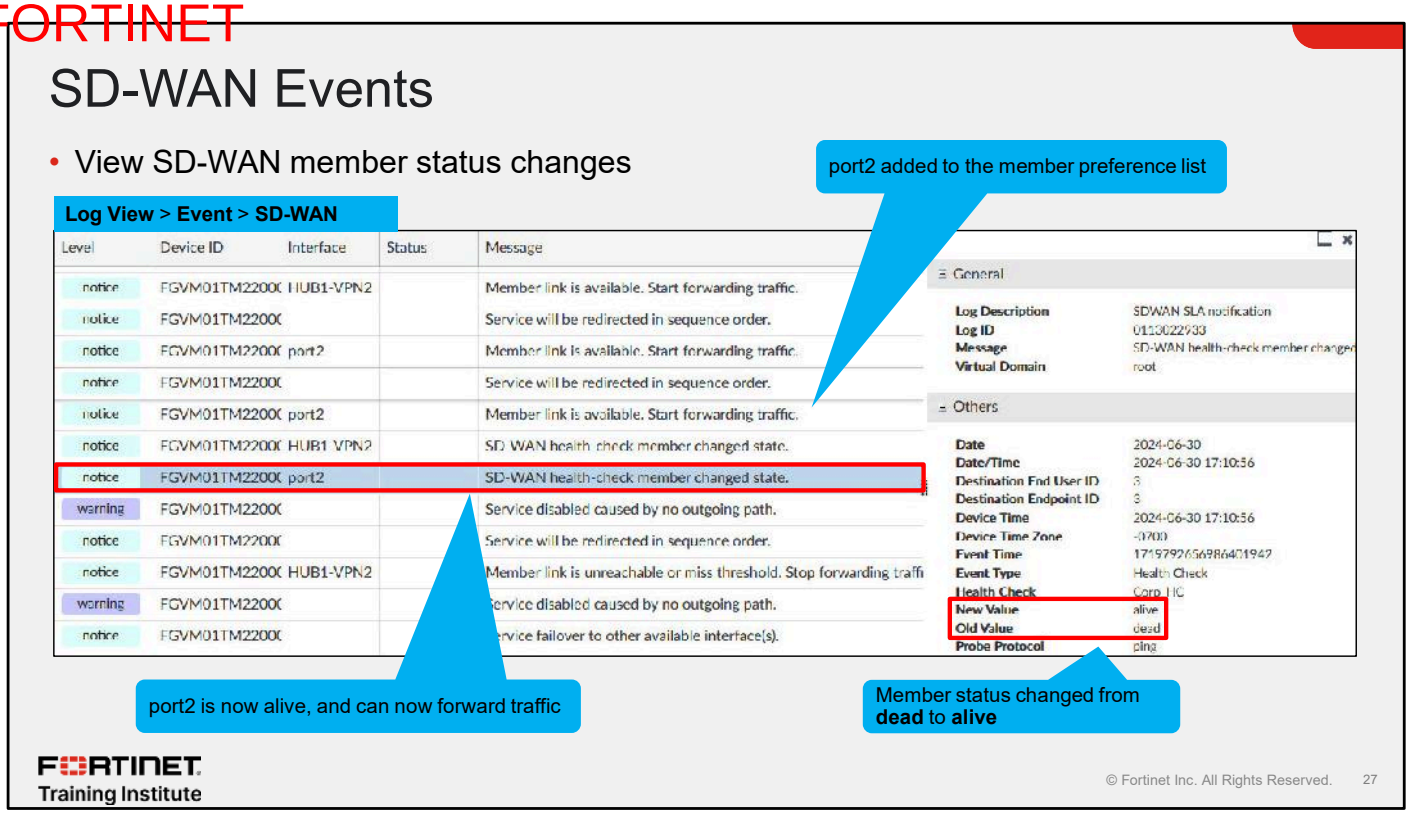
The table on this slide shows multiple sessions, including SD-WAN sessions and non-SD-WAN sessions. The SD-WAN sessions include information in the **SD-WAN Quality, SD-WAN Rule ID**, and **SD-WAN Rule Name**. The first session in this table is an SD-WAN session, and was identified as a **Salesforce** application. It matched the **Critical-DIA** rule and was sent to port1. FortiGate selected port1 because it had the lowest latency.

The eighth session in the table, which is also an SD-WAN session, was identified as a **Facebook** application, matched the **Non-Critical-DIA** rule, and was sent to port2. The rule **Non-Critical-DIA** instructs FortiGate to steer matching traffic to port2 only, provided the port is alive. This behavior matches the reason described in the **SD-WAN Quality** column for that session.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




Like on the FortiGate GUI, FortiAnalyzer places the SD-WAN event logs in a separate subsection: **SD-WAN**.

This slide shows several SD-WAN event logs. Click a log to view event details. For example, the details for the highlighted log indicate that the status of **port2** changed from **dead** to **alive**, which is why the log above it indicates that the port is ready to start forwarding traffic.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Events (Contd)

- Enable health check SLA status logs on FortiGate
  - For performance SLAs configured with SLA targets
  - Required by some FortiView graphs

**Device Manager > Provisioning Templates > SD-WAN > Performance SLA > Advanced Options**

| | |
|---|---|
| sla-fail-log-period | 10 |
| sla-pass-log-period | 10 |

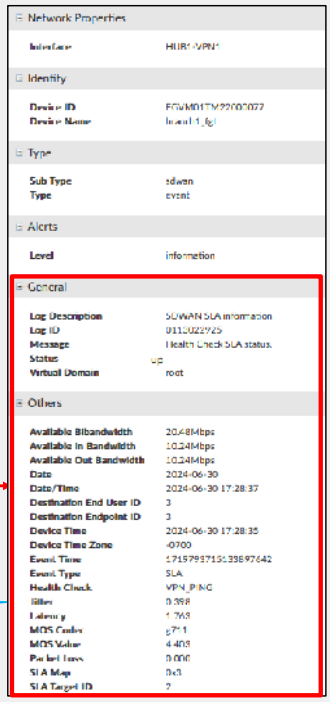
Default = 0 (no logs generated)

- Periodic health check SLA status logs in FortiAnalyzer:

**Log View > Event > SD-WAN**

| # | Date/Time | Level | Device ID | Interface | Status | Message |
|---|---|---|---|---|---|---|
| 5 | 2024-06-30 1 | information | FGVM01TM22000077 | HUB1-VPN1 | up | Health Check SLA status. |
| 6 | 2024-06-30 1 | information | FGVM01TM22000077 | HUB1-VPN1 | up | Health Check SLA status. |
| 7 | 2024-06-30 1 | information | FGVM01TM22000078 | HUB1-VPN3 | up | Health Check SLA status. |

Detailed member health and performance status




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

The analytics and reporting features of FortiAnalyzer are mainly based on the information contained in the logs received from devices. The data used by some of the SD-WAN FortiView graphs on FortiAnalyzer is taken from the health check SLA status logs generated by FortiGate. By default, these logs are not generated, and you must enable them if you want to take advantage of all the SD-WAN monitoring and reporting features provided by FortiAnalyzer.

On FortiGate, you enable the health check SLA status logs by configuring the `sla-fail-log-period` and `sla-pass-log-period` settings available on the performance SLA CLI configuration. On FortiManager, you can configure these settings under **Advanced Options** in the **Performance SLA** section.

`sla-fail-log-period` and `sla-pass-log-period` indicate the interval (in seconds) that health check SLA status log messages are generated when a member doesn't meet its configured SLA target and when it does, respectively. By default, both settings are set to `0`, which means that no logs are generated.

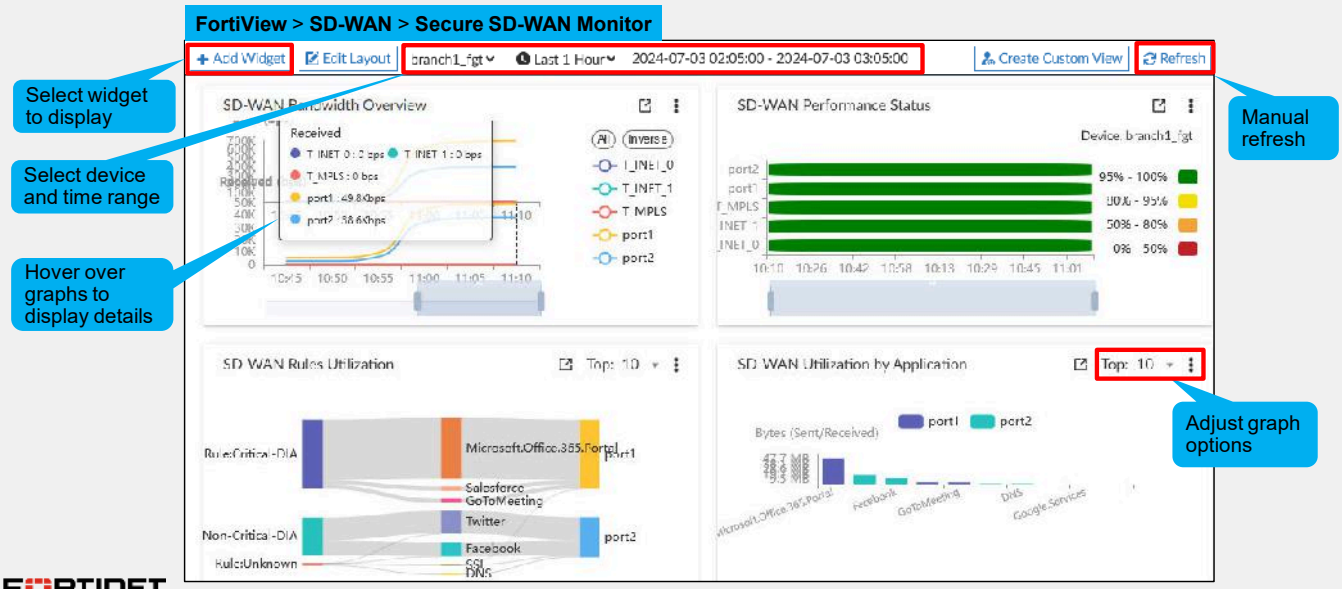
In the example shown on this slide, both settings are set to `10` seconds. As a result, FortiAnalyzer receives health check SLA status logs every 10 seconds for each SD-WAN member configured with an SLA target. Health check SLA status logs contain detailed health and performance information about members.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Secure SD-WAN Monitor

- Consolidated view of real-time and historical member health and utilization per device




FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view.

The **Secure SD-WAN Monitor** page on FortiView displays member health and utilization information for a particular device and time range using practical graphs. The example on this slide shows some of the graphs available on the page.

The **SD-WAN Rules Utilization** widget displays a Sankey type graph. It reports the rules utilization for each application and member. The example on this slide shows that the **Non-Critical-DIA** rule is used to forward **Twitter** and **Facebook** applications, and that the destination interface is **port2**. Hover over a graph to see details.

The **SD-WAN Utilization by Application** widget indicates the amount of traffic for each application, and the members that FortiGate steered the traffic to. The example on this slide shows that FortiGate steered all the **Facebook** traffic to **port2**.

Note that the graphs automatically refresh every 5 minutes. To refresh them manually, click the refresh button on the upper-right corner of the page.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Summary

- Summarized view of member health and utilization




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

The **SD-WAN Summary** page on FortiView provides a summarized view of your SD-WAN deployment. Like the secure SD-WAN monitor page, it provides SD-WAN health and utilization information, except that it can aggregate the data from multiple devices in the network.

The example on this slide shows the **SD-WAN Health Overview** and **Top SD-WAN SLA Issues** widgets. The former indicates how many devices are in critical, major, and healthy states. You can also click the graph sectors to get the list of devices in each of those states. The **Top SD-WAN SLA Issues** widget displays the best performance interfaces based on jitter, latency, or packet loss. You can select the interface to display and the performance parameter from the fields on the upper-right corner of the page.

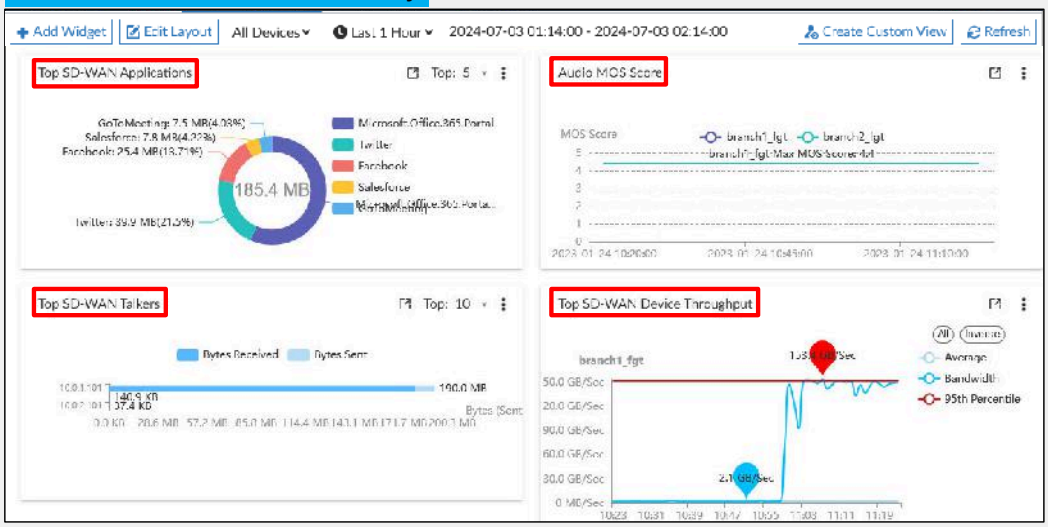

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Summary (Contd)

- Other widgets:

**FortiView > SD-WAN > SD-WAN Summary**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

This slide shows additional widgets available on the **SD-WAN Summary** page.

The **Top SD-WAN Applications** and **Top SD-WAN Talkers** widgets display the applications and endpoints that generated the most traffic in SD-WAN, respectively.

The **Audio MOS Score** widget graphs MOS for each codec and each FortiGate.

The **Top SD-WAN Device Throughput** widget graphs the bandwidth utilization for SD-WAN traffic.

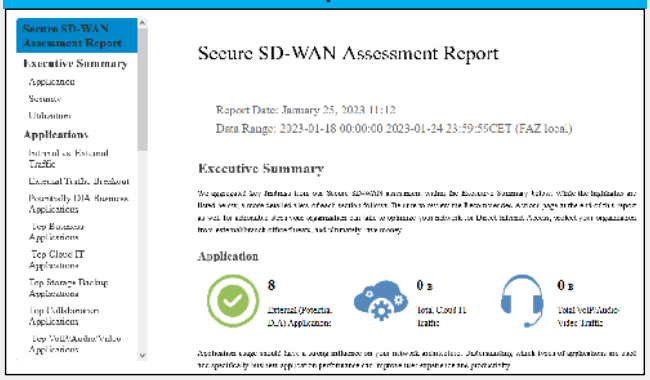

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

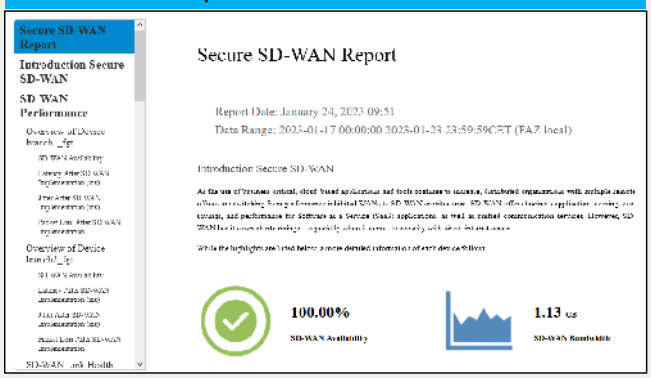
## Built-In SD-WAN Reports

- Secure SD-WAN Assessment
  - For pre-SD-WAN deployments
  - Describes traffic patterns and how SD-WAN can help improve application performance
- Secure SD-WAN
  - For post-SD-WAN deployments
  - Lists applications and indicates status of devices and members

**Reports > Reports Definitions > All Reports > Network Reports > Secure SD-WAN Assessment Report**




**Reports > Reports Definitions > All Reports > Network Reports > Secure SD-WAN Report**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

FortiAnalyzer comes with two preconfigured SD-WAN reports: the **Secure SD-WAN Assessment Report** and **Secure SD-WAN Report**.

The **Secure SD-WAN Assessment Report** is intended to be run before you deploy SD-WAN on the network. The report describes how much traffic is considered external or internal, the top applications in the network, and their category (business, cloud IT, social media, and so on). The report also indicates the top sources and destinations based on traffic volume. The goal of the report is for administrators and management to understand the current traffic pattern and then identify areas where SD-WAN can help improve application performance and availability.

The **Secure SD-WAN Report** is meant to be run after you deploy SD-WAN. The report lists the applications steered by SD-WAN, and the health and performance information for devices and members. Administrators and management can use the report to check the status of SD-WAN during a given period and identify past issues.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Understand zero-touch provisioning for SD-WAN branches
- ✓ Describe device blueprints
- ✓ Understand how to import model devices with CSV files
- ✓ Identify FortiManager monitoring features for SD-WAN
- ✓ Describe the speed test feature
- ✓ Understand FortiAnalyzer basics
- ✓ Identify SD-WAN logs
- ✓ Describe SD-WAN analytics and reports

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

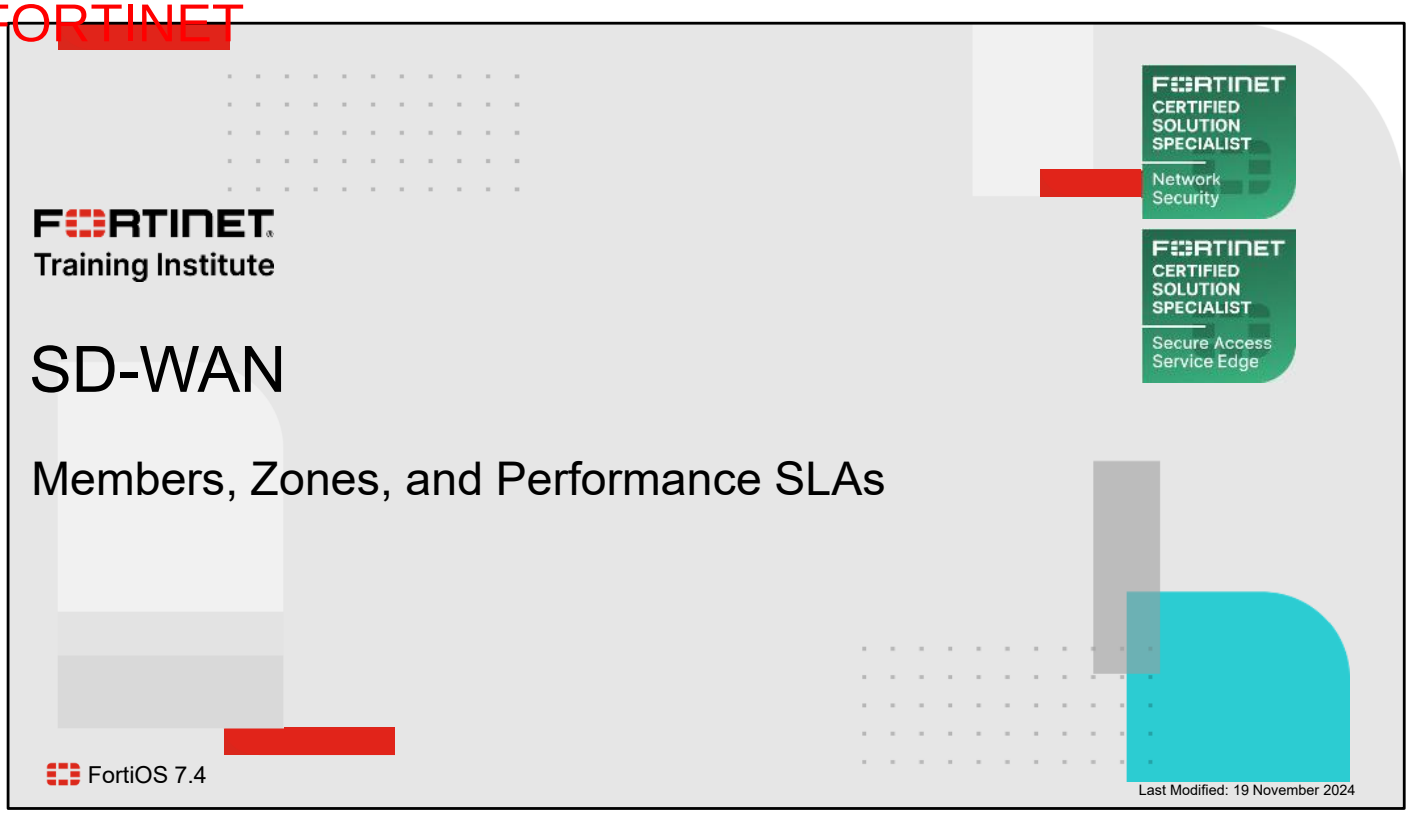
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned the most useful features available on FortiManager for deploying SD-WAN in large networks.



Vouchers & Dumps are Available | WhatsApp +201224560923

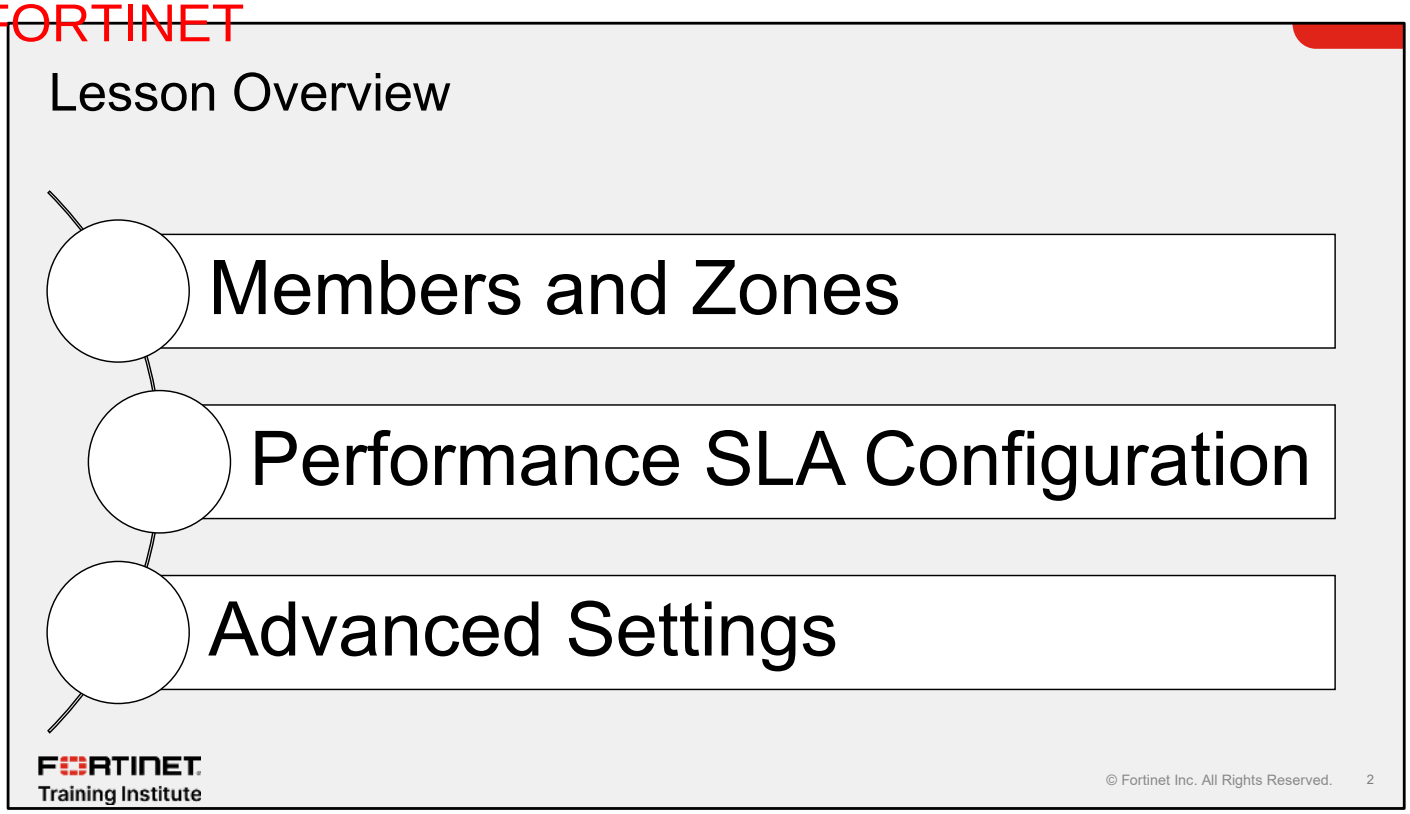
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about members, zones, and performance SLAs in detail.


Vouchers & Dumps are Available | WhatsApp +201224560923

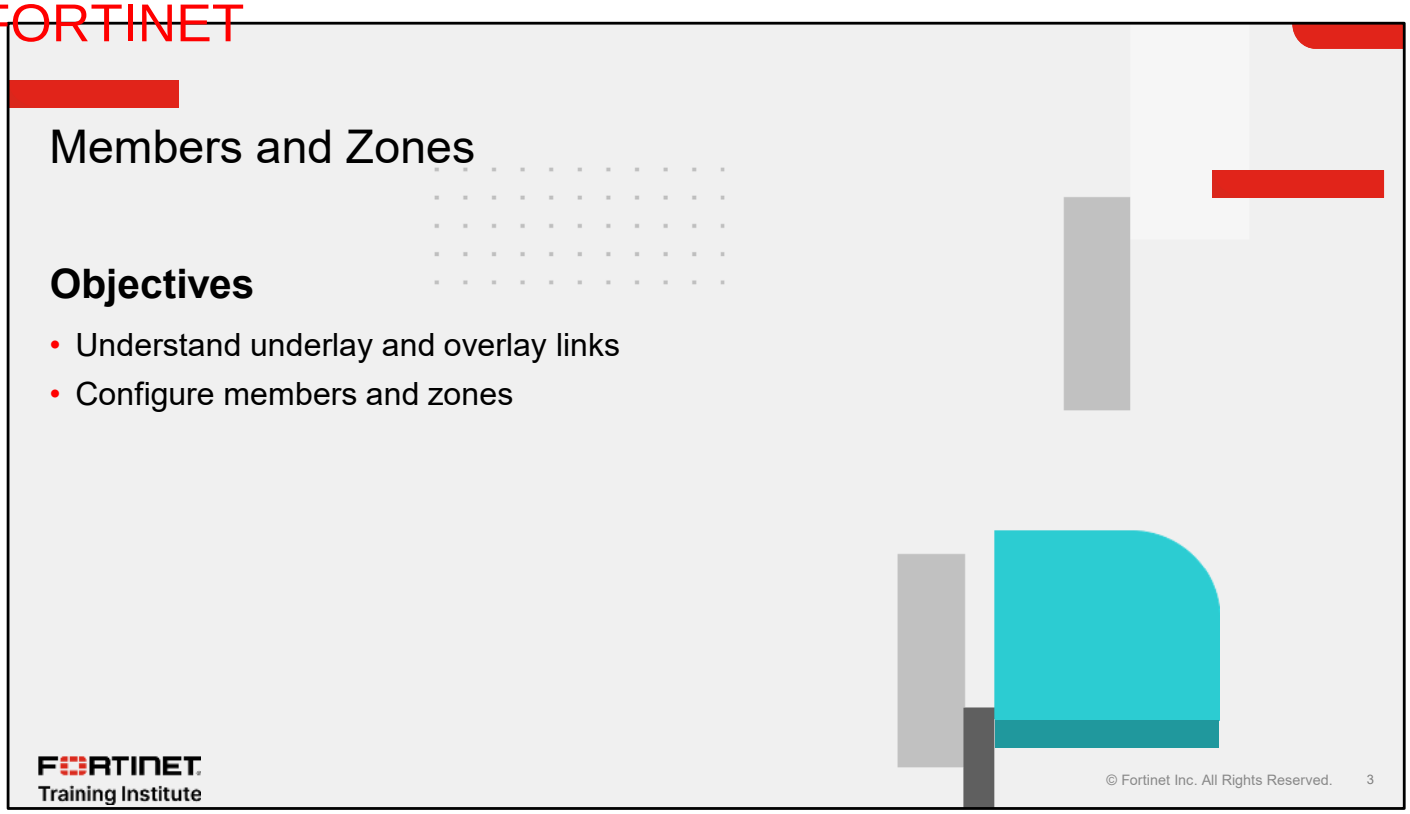
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of SD-WAN members and zones, you will be able to select and organize your underlay and overlay links for effective WAN usage.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Members—Underlay and Overlay Links

- Underlay:
  - Physical links provided by ISP
    - Cable, DSL, fiber, MPLS, 3G/4G/5G/LTE, ATM
  - Restricted routing
  - No added security
- Overlay:
  - Virtual links built on top of underlay links
    - IPsec, GRE, IP-in-IP
  - Flexible routing
  - Enhanced security

| Supported SD-WAN Members | |
|---|---|
| **Interface** | **Type** |
| Physical | Underlay |
| VLAN | |
| LAG | |
| 3G/4G/5G/LTE USB modems | |
| FortiExtender | |
| IPsec (including ADVPN) | Overlay |
| GRE | |
| IP-in-IP | |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

You discovered this slide in the introduction lesson. Let's review it as you will use the concept of underlay and overlay links in this lesson.

The terms *underlay* and *overlay* are used to describe the link type of an SD-WAN member.

Underlays refer to the physical links that you can rent or buy from an ISP, such as cable, DSL, fiber, MPLS, 3G/4G/5G/LTE, and ATM links. These links are part of the ISP physical infrastructure that is responsible for delivering packets across networks. The traffic that travels through underlays is restricted to the routing policies deployed by the ISP, and therefore, the packet source and destination IP addresses must be routable within the ISP network. This restriction leaves you with limited options to define your network addressing plan. In addition, traffic transmitted through underlays is usually not encrypted by the ISP network, which means that sensitive data can be accessed by unauthorized parties if the data is not encrypted by the sender.

Overlays are virtual links that you build on top of underlays. A common example of an overlay is an IPsec tunnel. Because original packets are often encapsulated in Encapsulating Security Payload (ESP) packets, the networks that communicate through the IPsec tunnel are no longer restricted to the routing policies of the ISP. In addition, the privacy and authentication features provided by IPsec protect your traffic from unauthorized access.

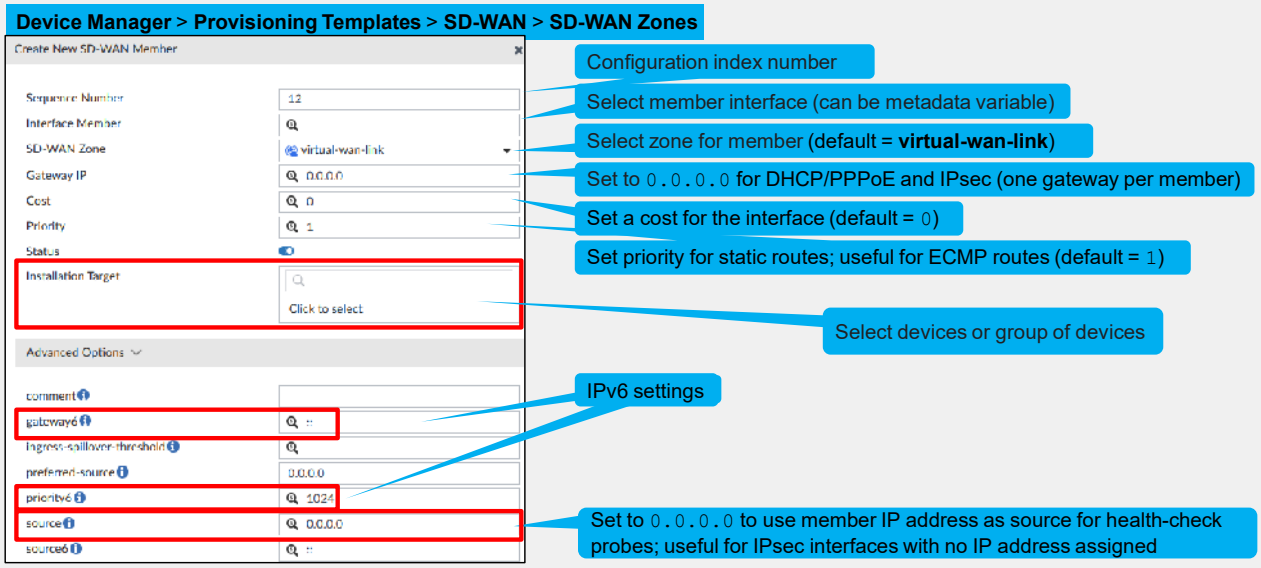
This slide shows the different underlay and overlay links supported by FortiGate as SD-WAN members.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Members—Configuration

- FortiManager GUI:




When you configure an SD-WAN member using the Device Manager or the SD-WAN provisioning template on FortiManager, you can configure the following settings:

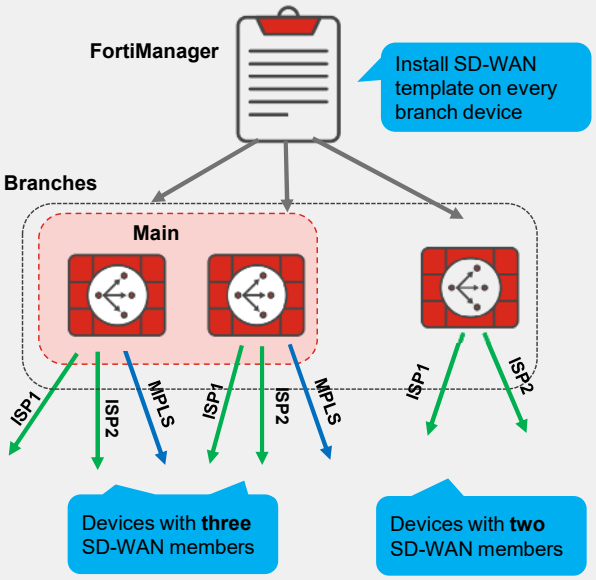
- **Sequence Number**: Sets the configuration index number of the member. It's automatically assigned by FortiManager in sequential order, but can be changed by the administrator.
- **Interface Member**: Type the name of the interface on the device to use as the SD-WAN member, or a metadata variable.
- **SD-WAN Zone**: Select the zone to place the member in. A member can be assigned to one zone only.
- **Gateway IP**: Indicates the IPv4 gateway address to use by the member. Set the address to `0.0.0.0` if the interface is DHCP, Point-to-Point Protocol over Ethernet (PPPoE), or IPsec. This instructs FortiGate to automatically use the gateway assigned by the ISP. The gateway is then used for static routes and health-check probes. Note that you can assign one gateway only per member.
- **Cost**: Set the cost of the member. The cost serves as a tiebreaker in SD-WAN rules using the lowest cost traffic-steering strategy.
- **Priority**: Assigns the priority of static routes created by SD-WAN. The priority setting is useful for prioritizing one equal-cost multipath (ECMP) route over other ECMP routes. The default priority is 1 for static routes associated with SD-WAN members.
- **Status**: Enable or disable a member. When disabled, the member is not used in SD-WAN.
- **Installation Target**: Define a subset of devices on which the SD-WAN member is installed. Leave empty to install the member on every device on which this SD-WAN templated applies.
- **Source**: Indicates the member source IP address for health-check probes. If set to `0.0.0.0`, FortiGate uses the primary IP address of the member interface as source. This setting is useful for IPsec interfaces with no IP address assigned.
- **Gateway6**, **priority6**, **source6**: Settings for IPv6.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Member—Installation Target

- Flexible SD-member definitions
- Accommodates a range of requirements
  - Hardware
  - Type of site
- Common use cases
  - Branches with more WAN links than others
  - Only some branches have 4G/5G backup links
- Installation targets
  - Device groups or subgroups
  - Individual devices
  - Leave empty to install on all devices




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

When defining an SD-WAN template, you might encounter situations where most devices share the SD-WAN configuration, except for certain interfaces. For example, you might have some branch devices with a 4G/5G link, and some without. You might have an MPLS link for your main branches only. For such situations, you can define installation targets for your SD-WAN members.

To define an installation target, you can select device groups or individual devices. Leave the **Installation Target** field empty to install the member on every device.

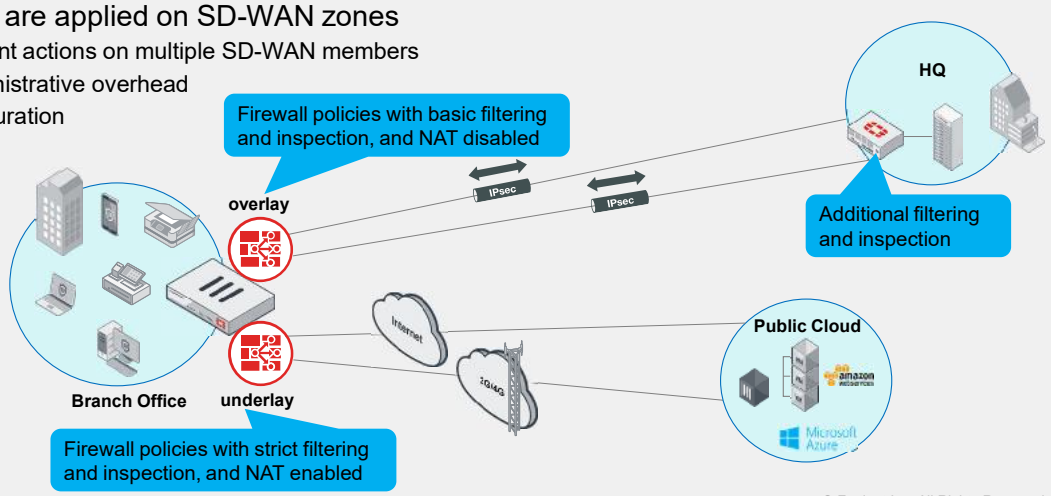
In the example shown on this slide, the template defines three SD-WAN members. The members, port1 (ISP1) and port2 (ISP2), apply on every branch device. However, when you install the configuration, FortiManager will define port4 (MPLS) as an SD-WAN member only on devices that are part of the main group.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Zones

- Divides SD-WAN members in groups
  - Default zone: virtual-wan-link
    - Can't be deleted
  - An interface can belong to one zone only
- Firewall policies are applied on SD-WAN zones
  - Perform different actions on multiple SD-WAN members
  - Reduces administrative overhead
  - Cleaner configuration
- Usually, underlay and overlay links are grouped into different SD-WAN zones




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Typically, you would apply a different set of policies, based on the link type of your SD-WAN members. For example, you may want to enable NAT and apply strict security policies to internet traffic sent through underlay links, because the traffic directly leaves the site boundaries. Conversely, you typically disable NAT and apply basic filtering and inspection to traffic sent through overlay links, because the remote site is fully routable and performs additional filtering and inspection on the traffic.

SD-WAN zones allow administrators to group together members that require a similar set of firewall policies. Usually, this means grouping underlays and overlays into different SD-WAN zones. Firewall policies defined for your SD-WAN traffic must reference the SD-WAN zones and cannot reference individual SD-WAN members.

The virtual-wan-link SD-WAN zone is created by default and can't be deleted. It contains any SD-WAN member not explicitly assigned to a user-defined SD-WAN zone.

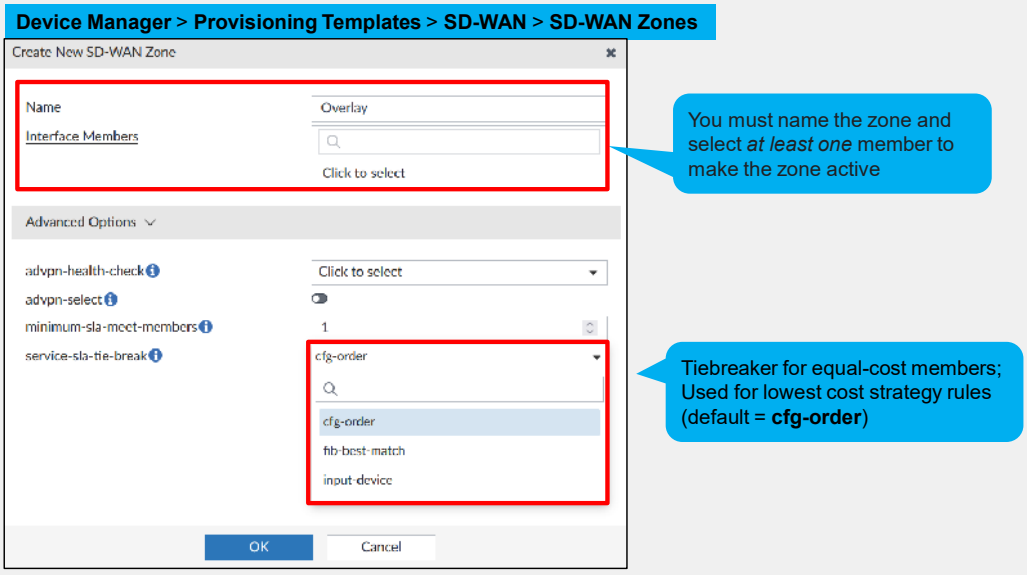
The topology shown on this slide shows a branch office with two SD-WAN zones configured: overlay and underlay. The overlay SD-WAN zone is composed of IPsec tunnels and the underlay SD-WAN zone is composed of an internet link and a 4G/5G link. The branch office uses the overlays to access the headquarter networks, and the underlays to access services in the public cloud. By dividing SD-WAN members into zones, you can apply the same set of firewall policies to a zone instead of having to apply them to individual members, reducing the administrative overhead and building a cleaner configuration.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Zones—Configuration

- FortiManager GUI:




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

When you configure an SD-WAN zone using Device Manager or the SD-WAN provisioning template, you must configure the following settings:

- **Name**: Type in a name for the zone.
- **Interface Members**: Select one or more members to be included in the zone. You can use a zone to steer the traffic, it must contain at least one member.

Optionally, you can configure **service-sla-tie-break.** This setting is applicable to all SD-WAN rule strategies except in conjunction with the load balancing option. You would usually use this setting when you select the lowest cost strategy for the SD-WAN rule.

- **cfg-order** instructs FortiGate to use the member configuration order as the tiebreaker for the selected member. That is, members that meet the SLA are selected in the order they are configured (default).
- **fib-best-match** uses as tiebreaker the most specific route. That is, the member with the most specific route—longest prefix match—to the destination becomes the selected member.
- **input-device** is used for overlay stickiness. Traffic received on one overlay should egress on same overlay, when possible. It instructs FortiGate to send the reply through the overlay link that received the incoming flow, provided it matches the SLA criteria. You can associate this setting with an option in the SD-WAN service rule to ensure that traffic received in a zone stays in that zone. The CLI commands for the service definition are: `set input-zone` and `set tie-break input-device`.

Note that when you create a zone with the FortiManager SD-WAN template, FortiManager automatically creates a corresponding normalized interface.

You will learn more about SD-WAN rules and the available strategies in another lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# SD-WAN Members and Zones—CLI Configuration

- FortiGate CLI configuration:

```
config system sdwan
    config zone
        edit underlay
            set service-sla-tie-break cfg-order
        next
    end
    config members
        edit 1
            set interface port1
            set zone underlay
            set gateway 0.0.0.0
            set preferred-source 0.0.0.0
            set source 0.0.0.0
            set gateway6 ::
            set source6 ::
            set cost 0
            set priority 1
            set priority6 1024
            set status enable
        next
```

Setting hidden for IPsec interfaces

service-sla-tie-break options

```
fgt1 (underlay) # set service-sla-tie-break ?
   cfg-order
      Members that meet the SLA are selected in the
      order they are configured.
   fib-best-match
      Members that meet the SLA are selected
      that match the longest prefix in the routing
      table.
   input-device
      Members that meet the SLA are selected by
      matching the input device.
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

This slide shows the equivalent CLI configuration for the SD-WAN member and zone created on FortiManager on the previous slides. Although this course is focused on SD-WAN deployment from FortiManager, it is useful to know the corresponding SD-WAN FortiGate CLI settings, in case you want to apply the configuration using FortiManager CLI templates and scripts.

Note that the `gateway` and `gateway6` settings are not available if `interface` is set to an IPsec interface. This is because FortiOS automatically uses the tunnel ID as the gateway for IPsec interfaces. FortiGate uses tunnel IDs to determine the next hop for IPsec traffic. The tunnel ID can be found in the output of `diagnose vpn tunnel list`. Usually, FortiOS uses the IP address configured as `remote-gw` in the phase 1 settings as the tunnel ID.

Also note that the output shown on this slide has been modified to include a mix of settings with default and non-default values. On the FortiGate CLI, you can run `show full-configuration system sdwan` to display the SD-WAN settings with default values.

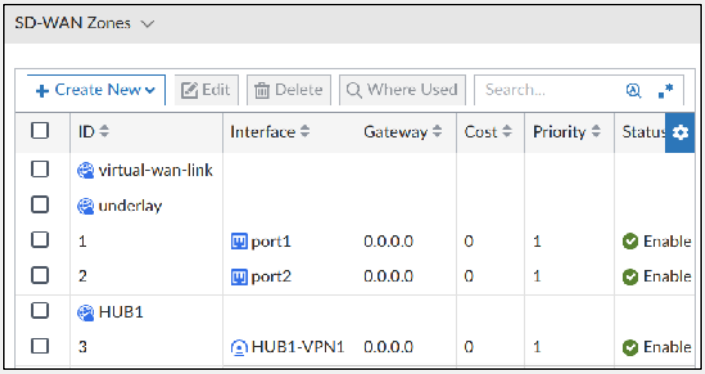


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Members and Zones—CLI Configuration (Contd)

- Sample FortiManager configuration




- Equivalent FortiOS CLI configuration

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "underlay"
        next
        edit "HUB1"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
        next
        edit 2
            set interface "port2"
            set zone "underlay"
        next
        edit 3
            set interface "HUB1-VPN1"
            set zone "HUB1"
        next
    end
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

This slide shows a more elaborate member and zone configuration and its corresponding FortiOS CLI configuration. Note that, by default, the CLI configuration shows only settings with non-default values.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Members and Zones—CLI Verification

- FortiOS CLI verification:

```
# diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, source 192.2.0.1, priority: 1 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, source 192.2.0.9, priority: 1 1024, weight: 0
Member(3): interface: HUB1-VPN1, flags=0xc , gateway: 100.64.1.1, source 192.168.1.2, priority: 1 1024
weight: 0

# diagnose sys sdwan zone
Zone HUB1 index=3
         members(1): 20(HUB1-VPN1)
Zone underlay index=2
         members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
         members(0):

# diagnose netlink interface list | grep index=20
if=HUB1-VPN1 family=00 type=768 index=20 mtu=1420 link=0 master=0
```

Configuration index number

Automatic gateway detection—tunnel ID for IPsec tunnels (`diagnose vpn tunnel list`)

For volume-based load balancing

Kernel interface index number

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

In addition to checking the FortiOS CLI configuration for SD-WAN, you can also run the commands shown on this slide to verify the SD-WAN settings in place.

The `diagnose sys sdwan member` command displays the settings of each member. Some of the settings shown in the output are the configuration index number, the gateway, and the weight. The configuration index number should match the member index under `config member` in `config system sdwan`.

If the member is configured with automatic gateway detection—that is, the gateway is set to `0.0.0.0`—or if the member is an IPsec interface, the output displays the gateway detected by FortiGate. If the member is an IPsec interface, FortiGate uses as gateway its tunnel ID. The tunnel ID can be found in the output of `diagnose vpn tunnel list`. Usually, FortiOS uses as tunnel ID the IP address configured as `remote-gw` in the phase 1 settings.

The source corresponds to the source IP address used for traffic initiated from this member, such as health-check probes. By default, it uses the interface IP address. For IPsec tunnels, by default, FortiGate uses the address of the interface with the lowest index number (port1). The administrator can define another value. You will learn how in this course.

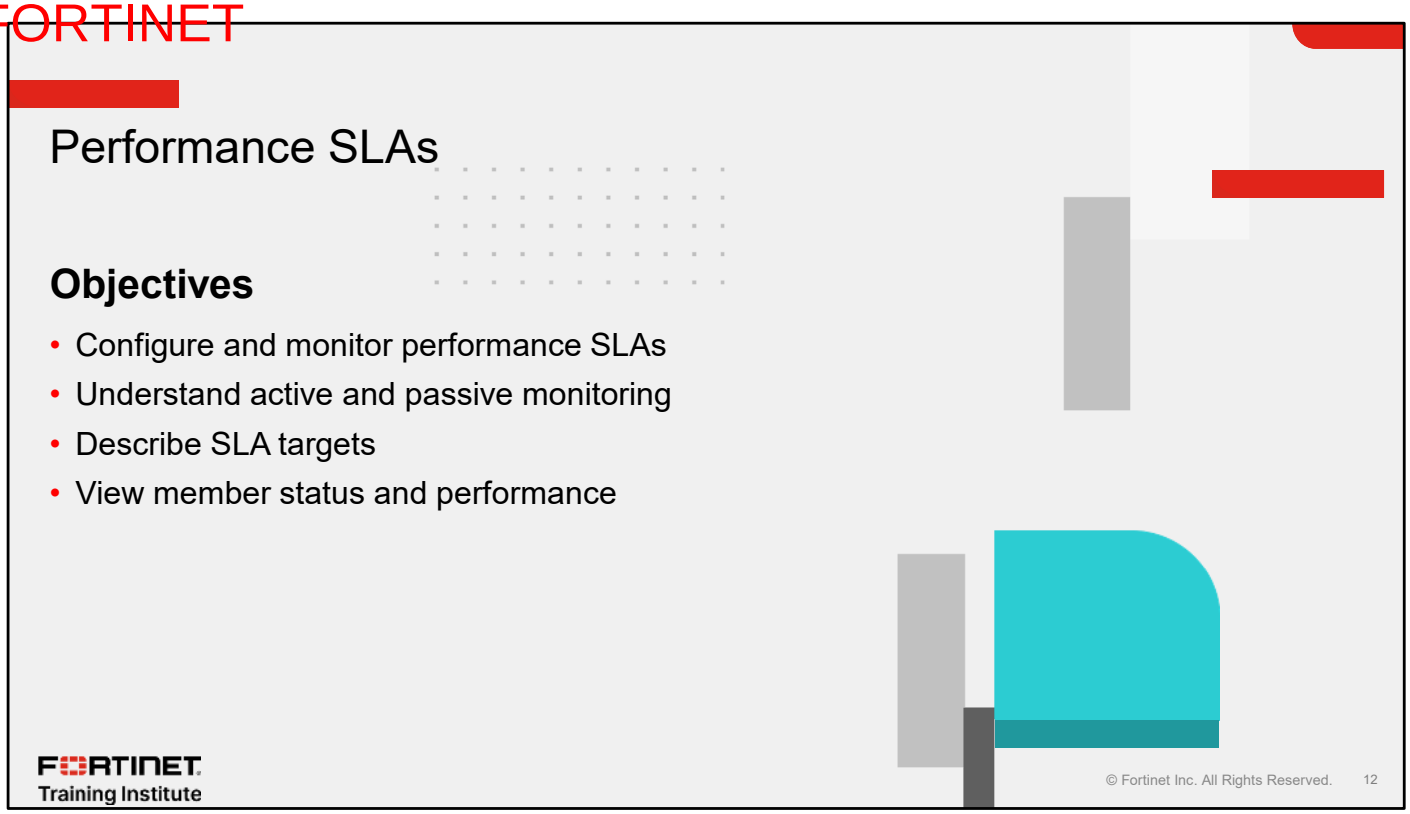
The weight setting applies to the volume-based load balancing algorithm only, which can be configured for the implicit SD-WAN rule. You will learn more about load balancing algorithms available for traffic that matches the implicit SD-WAN rule in another lesson.

The `diagnose sys sdwan zone` command displays the configured zones and their members. Note that the output indicates the kernel interface index number of a member, which should match the index displayed by `diagnose netlink interface list`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of performance SLAs, you should be able to configure appropriate health check and performance monitoring for your SD-WAN members. Member health check and performance are key components in an effective SD-WAN deployment.

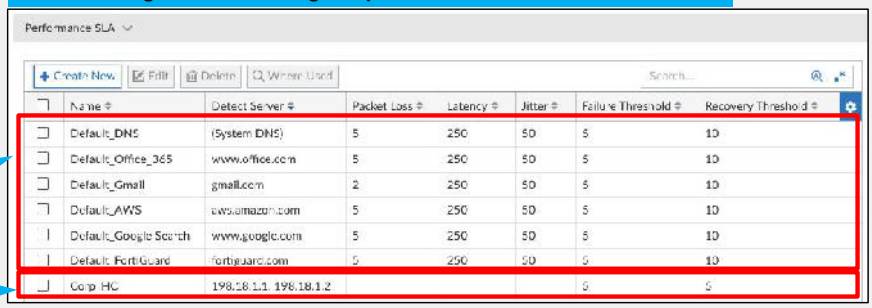

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Performance SLAs

- Monitor member health:
  - State
    - Alive or dead
  - Performance
    - Packet loss, latency, and jitter
    - Mean Opinion Score (MOS)
    - SLA targets
      - Minimum performance requirements
- Health can be measured:
  - Actively
    - Based on periodic probes sent to configured servers
  - Passively
    - Based on member traffic

**Device Manager > Provisioning Templates > SD-WAN > Performance SLA**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

You can use performance SLAs to monitor the health and performance of members. Although configuring performance SLAs is optional, you should configure them to ensure members meet the health and performance requirements for steering traffic, which is critical for effective WAN usage with SD-WAN.

When you configure performance SLAs, you configure health checks, and optionally you can define SLA targets. Active health checks determine the state of members—alive or dead—and monitor their performance in terms of packet loss, latency, and jitter. You can also decide to combine the three criteria and determine what is called the mean opinion score or MOS. SLA targets define the minimum performance requirements for members to be eligible for steering traffic. SD-WAN then uses this information to make traffic steering decisions based on the SD-WAN rules configured. For example, you can instruct FortiGate to steer internet traffic to an alive member whose latency doesn't exceed a given threshold.

There are several performance SLAs created by default that you can use for your setup. The default performance SLAs measure the health of members against well-known internet services, such as FortiGuard, Google Search, and Amazon AWS. Alternatively, you can create your own entry and choose whether you want to monitor the member actively or passively. In active monitoring, the health of the member is checked by periodically sending probes from the member to one or two servers that act as beacons. In passive monitoring, the health of a member is determined based on the traffic passing through the member.

The example on this slide shows a user-defined performance SLA named **Corp_HC**, which monitors the health and performance of members by sending pings to corporate devices located in the hub location **198.18.1.1** and **198.18.1.2** DNS servers.

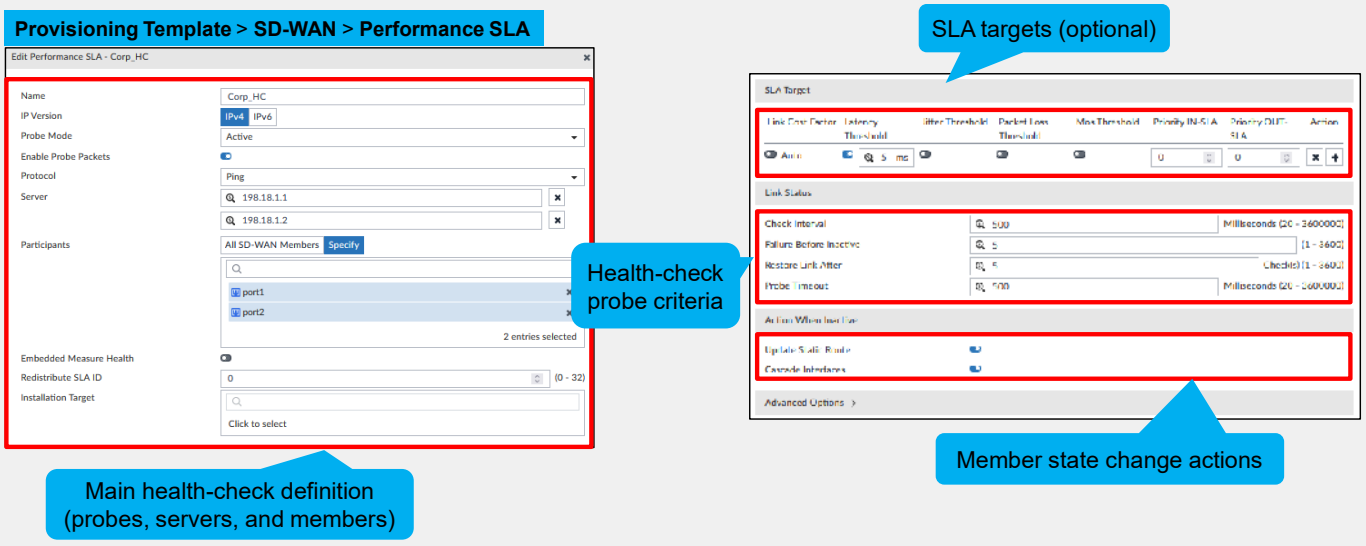


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Performance SLAs Configuration Overview

- Multiple sections for each performance SLA




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

The FortiManager Performance SLA configuration page can be divided into the following sections:

- Health check: Divided into two parts. In the performance SLA header, you configure how the member health check is performed and which members it applies to. In the **Link Status** section, you configure the criteria for alive and dead members, probe interface, and the acceptable failure rate.
- **SLA Target**: Define the performance requirements of alive members so they can be eligible for traffic steering. SLA targets can be used with the *lowest cost* traffic-steering strategy, with or without traffic load-balancing.
- **Action When Inactive**: When there is a change in the state of a member (alive or dead), you can instruct FortiGate to update the static routes that match the gateway used by the member. You can also instruct FortiGate to bring down or bring up one or more alert interfaces based on the state of all members. You will learn more about these features later in this lesson.
- **Advanced Options**: This is where you configure additional performance SLA settings.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# CLI Configuration for Performance SLAs

- Named `health-check` on the FortiGate CLI

Health check (probes and servers)

Health check (member state criteria)

Member state change actions

Health check (members)

SLA targets

```
config health-check
    edit "Corp HC"
        set probe-packets enable
        set addr-mode ipv4
        set server "198.18.1.1" "198.18.1.2"
        set detect-mode active
        set protocol ping
        set interval 500
        set probe-timeout 500
        set failtime 5
        set recoverytime 5
        set update-cascade-interface enable
        set update-static-route enable
        set members 1 2
        config sla
            edit 1
                set link-cost-factor latency
                set latency-threshold 5
            next
        end
    next
end
```

Configuration index number

FORTINET Training Institute

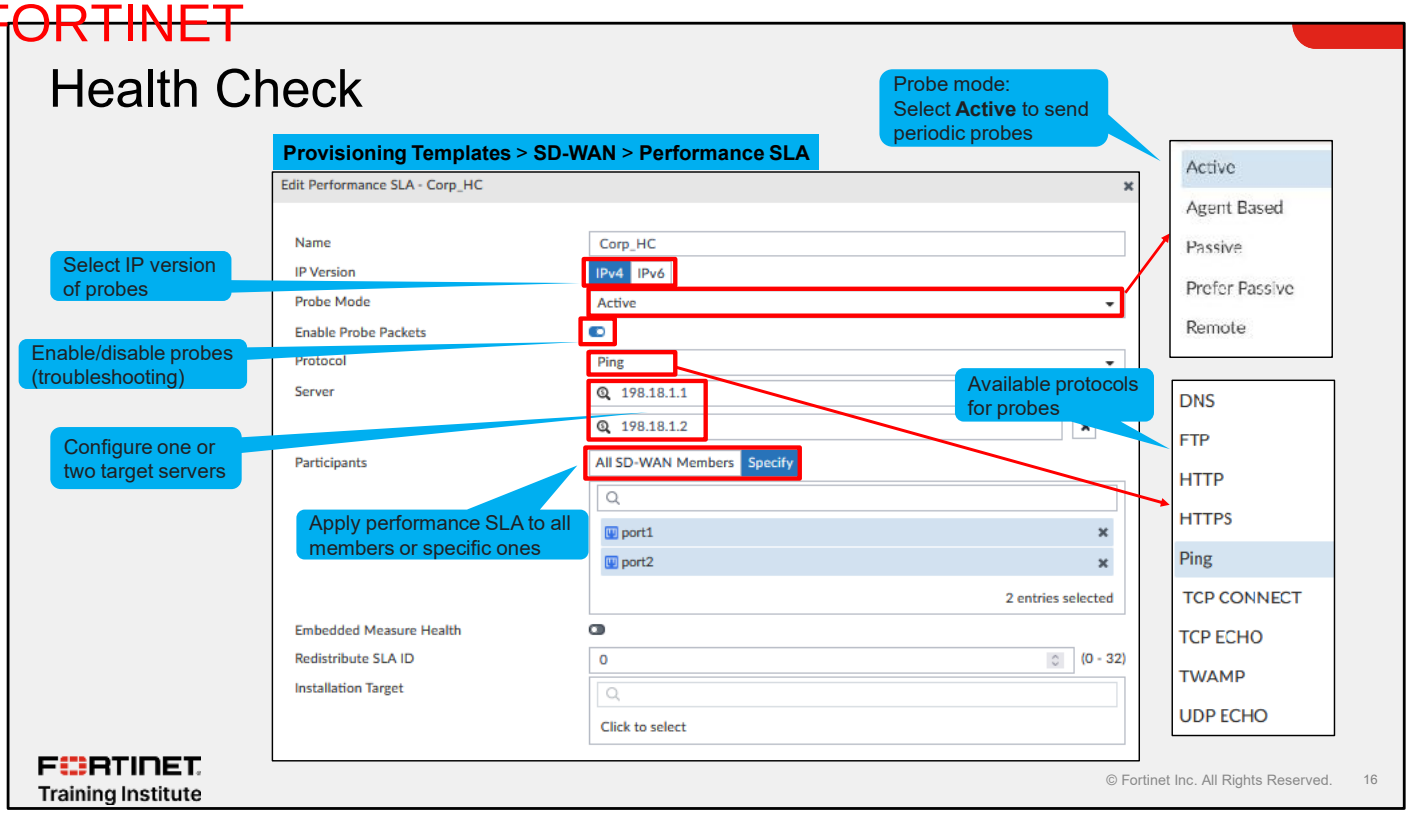
© Fortinet Inc. All Rights Reserved. 15

This slide shows the FortiOS CLI configuration that is equivalent to the FortiManager example configuration shown on the previous slide. Note that performance SLA is called `health-check` on CLI configurations.

Note also that the members are referenced using their configuration index number, and not their names. The same is done for most SD-WAN settings and diagnostics. For this reason, it's very useful to identify the configuration index numbers of your members for troubleshooting purposes.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

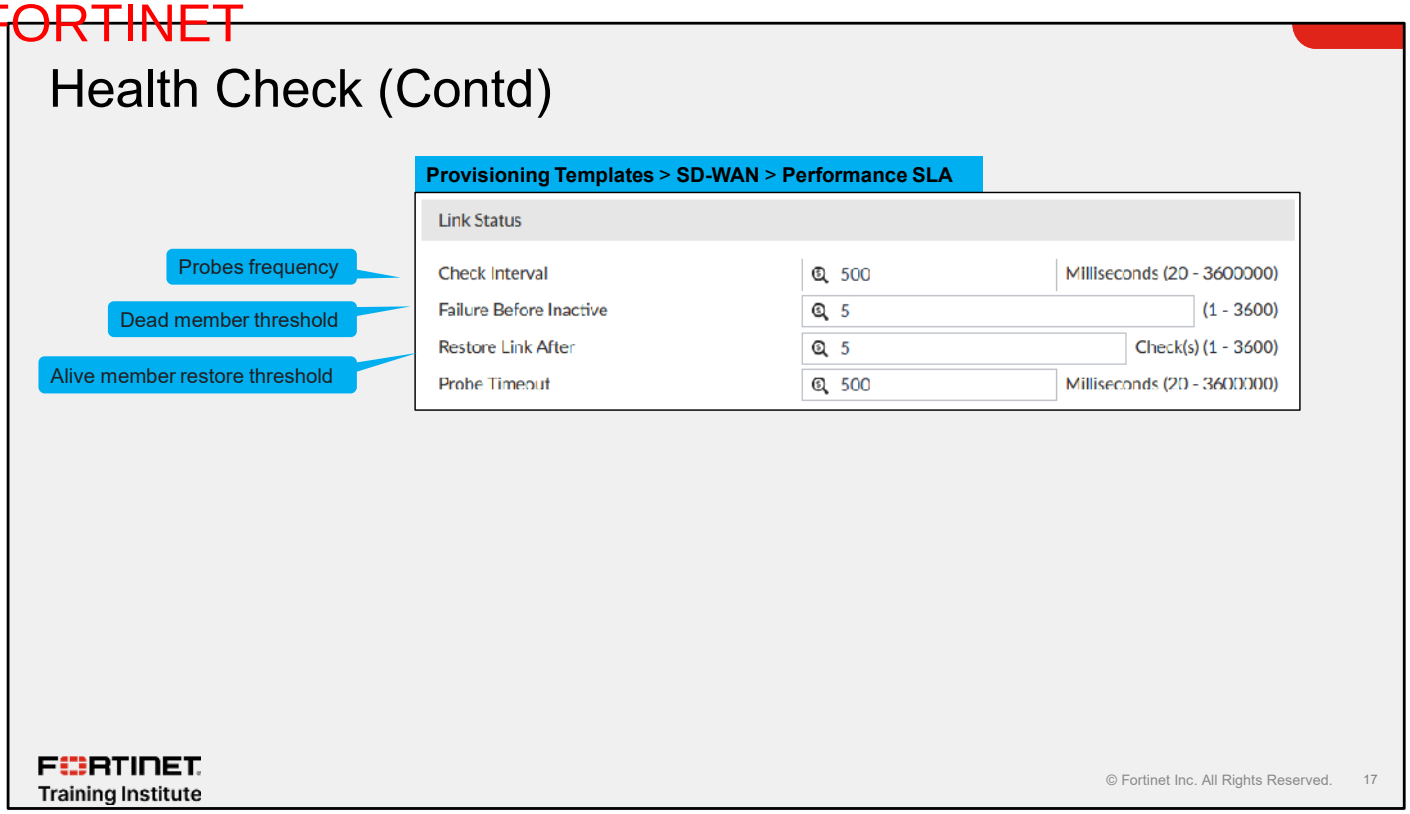



The first part of the health check configuration provides the following settings:

- **IP Version**: Select the IP version to use for probes. Both IPv4 and IPv6 are supported.
- **Probe Mode**: FortiGate can monitor members actively, passively, using a mix of both (**Prefer Passive**) or using information received from other devices. In **Active** mode, FortiGate sends periodic probes through the member to monitor its health and performance. In **Passive** mode, FortiGate monitors the actual network traffic flowing through the member to determine its performance. In **Prefer Passive** mode, FortiGate uses passive mode first, and then switches to active mode if there was no TCP traffic across the member for three minutes. With **Remote** mode, FortiGate uses SLA information received from the remote device. Use **Agent Based** if the FortiGate collaborates with FortiMonitor agents to collect application-level performance statistics per link. You will learn more about detection modes in this lesson.
- **Protocol**: Select the protocol to use for probes.
- **Server**: If using **Active** or **Prefer Passive** modes, configure up to two servers to send the probes to. It is the best practice to configure two servers to guard against false positives caused by the server being at fault, and not the link.
- **Participants**: Select if you want to use the health check to monitor all SD-WAN members or specific ones.
- **Enable Probe Packets**: If using **Active** or **Prefer Passive** modes, disable or enable the use of probes. When you disable probes, FortiGate continues processing SD-WAN traffic using the last known measured metrics for members but stops monitoring them, which means that FortiGate won't detect new changes in the quality of links. For this reason, you should disable probes for troubleshooting purposes only.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




The second part of the health-check configuration provides the following settings:

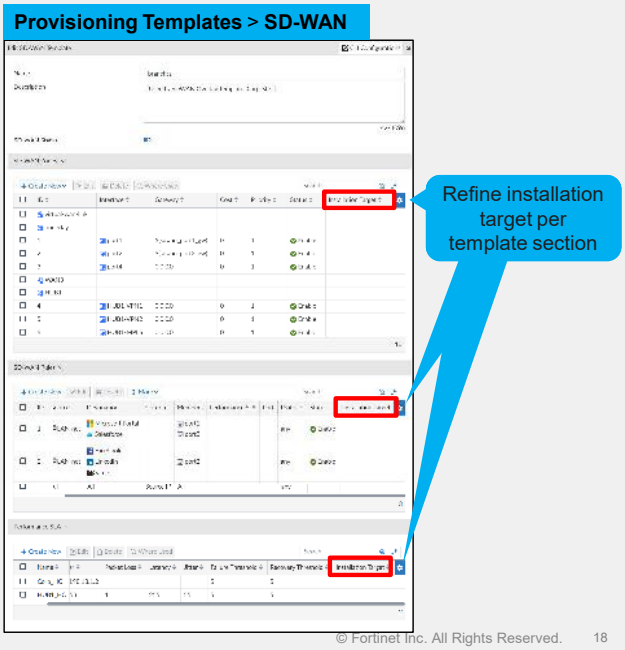
- **Check Interval**: Defines how often the probes are sent to the configured target servers. By default, probes are sent every 500 milliseconds.
- **Failure Before Inactive**: Defines the number of consecutive failed probes to detect before a member is determined dead. By default, a member is considered dead after five consecutive failed probes. While a heath-check member is declared dead, it is not used to steer traffic.
- **Restore Link After**: Defines the number of consecutive successful probes to detect before a member changes from the dead state to the alive state. Initially, all members are considered alive. If the member is later detected dead, by default, it becomes alive again after five consecutive successful probes.
- **Probe Timeout**: Defines the delay to wait for probe responses.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Template for Heterogeneous WAN Links

- You can apply a single SD-WAN template differently based on device type or site requirements
- Define installation targets for:
  - SD-WAN members
  - SD-WAN service
  - SD-WAN performance SLAs
  - SD-WAN BGP neighbor
- Define targets for each:
  - Branch device
  - Device subgroups (recommended)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

Earlier in this lesson, you discovered how you can specify the installation target for each SD-WAN member. Similarly, you can define installation targets in your SD-WAN template for the services, performance SLAs, and BGP neighbor.

For SD-WAN topologies with heterogeneous WAN links, it's a best practice to group the devices in subgroups and use those groups to define the installation target per SD-WAN elements. Later, when the network expands, you can add the devices to the correct subgroups. FortiManager automatically adjusts the SD-WAN configuration to install it on the devices.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Active Monitoring

- Periodic probes sent to target servers to determine a member:
  - State: alive or dead
    - Initial state for members: alive
  - Performance: packet loss, latency, and jitter
    - Used by SD-WAN rules
- Probes:
  - Supported IPv4 protocols:
    - General-purpose
      - Ping, UDP echo, TWAMP, TCP connect, and TCP echo
    - Application-specific:
      - DNS, FTP, HTTP, and HTTPS
  - Supported IPv6 protocols:
    - General-purpose
      - Ping, UDP echo, TCP connect
    - Application-specific:
      - DNS, FTP
  - Default interval: 500 ms
  - Default failure and restore thresholds: 5 probes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

When you configure a performance SLA to use active monitoring, FortiGate sends probes to determine the state of the member—whether it is alive or dead—and its performance in terms of latency, packet loss, and jitter.

The protocols supported for probes can be divided into two groups: general-purpose and application-specific. The protocols in the former group can be used to measure the quality of a link regardless of which type of application the target server is running. The application-specific protocols enable you to get more accurate performance results for applications and services. For example, you may want to prefer HTTP over ping to measure the performance of a member that is used to steer web traffic. In this case, an HTTP probe would provide more accurate results instead of ping, which could be blocked or rate-limited along the path.

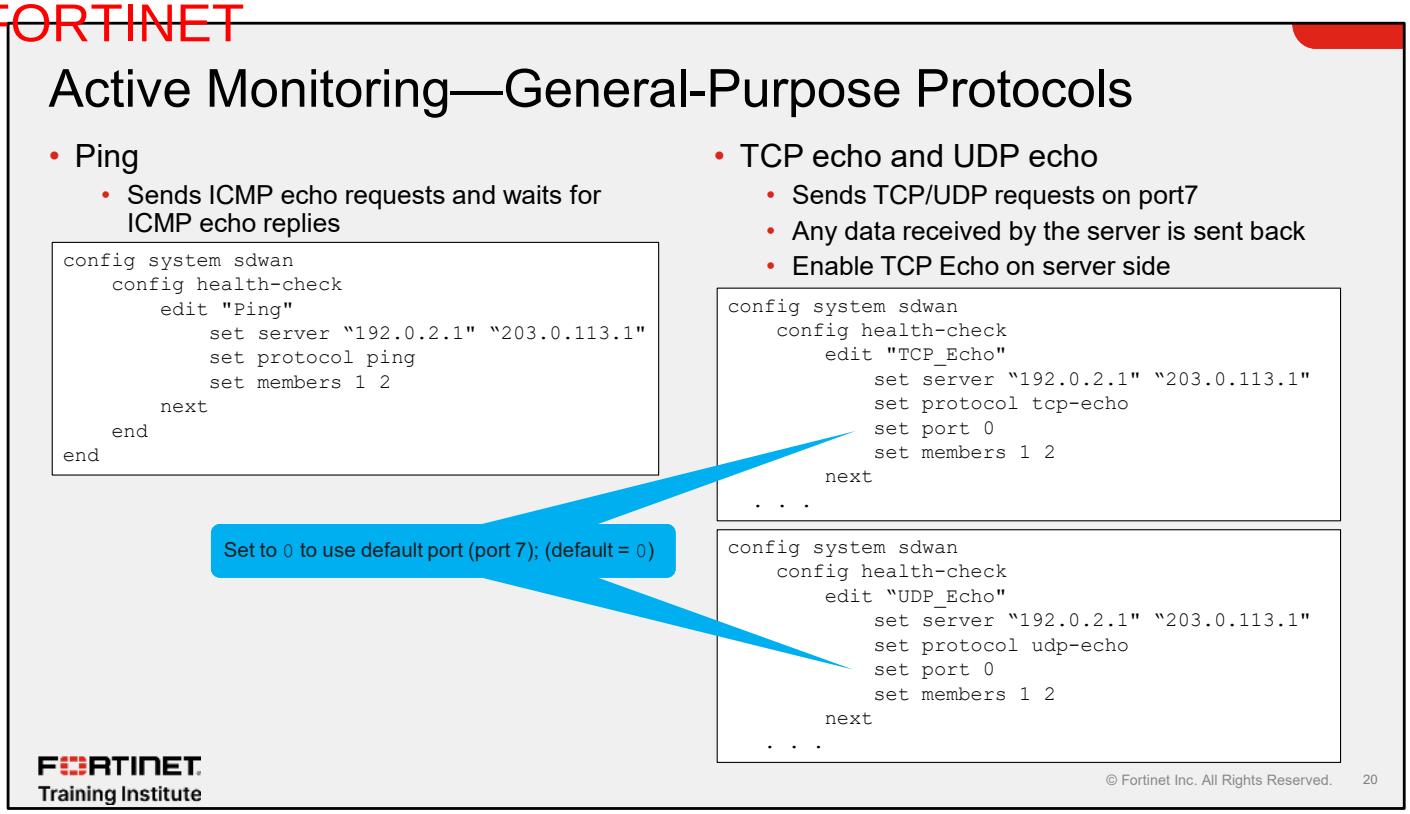
For IPv4 probes, FortiGate supports the protocols listed on this slide. For IPv6 probes, FortiGate supports the same protocols as in IPv4 except TCP echo, HTTP, and Two-Way Active Measurement Protocol (TWAMP). You will learn more about these protocols in this lesson.

Initially, all configured members are assigned the alive state, and then FortiGate starts sending probes at the configured interval—500 ms by default. After that, FortiGate marks a member as dead if the number of consecutive failed probes reach the failure threshold—five probes by default. A dead member is determined alive again if the number of consecutive successful probes reach the restore threshold—also five probes by default.

The probes are also used to measure the member performance. FortiGate measures the packet loss, latency, and jitter based on requests and replies sent and received for probes. The measured performance can then be used in SD-WAN rules to identify members that meet the required performance of applications and services.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




This slide describes the general-purpose protocols supported by SD-WAN when using active monitoring.

Ping is the most used network monitoring protocol because it is supported by virtually all network devices. When you use ping, FortiGate sends ICMP echo requests to the configured target servers and waits for the respective ICMP echo replies. Because some ISPs and content providers block or limit ICMP traffic on their network, you may want to switch to TCP echo, UDP echo, or TWAMP.

When you use TCP echo and UDP echo, FortiGate sends periodic packets to the configured target servers, which are listening for connections on port7 for both TCP and UDP. Upon reception of the packets, the server sends back an identical copy of the data it received from FortiGate.

This slide shows a FortiOS CLI configuration example of performance SLAs using ping, TCP echo, and UDP echo protocols. Note that you can configure a custom port for TCP echo and UDP echo, in case you don't want to use the default port—port7.

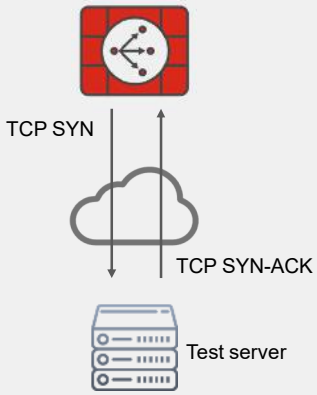


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Active Monitoring—TCP Connect

- TCP connect
  - Use a full TCP connection to test the link with the server
  - TCP connections using a custom port
    - Check connectivity of any TCP application
    - Methods to measure the quality of the TCP connection:
      - `half-open`: FortiGate sends SYN and gets SYN-ACK
        The latency is based on the round trip between SYN and SYN-ACK (default)
      - `half-close`: FortiGate sends FIN and gets FIN-ACK
        The latency is based on the round trip between FIN and FIN-ACK




```
config system sdwan
    config health-check
        edit "TCP_Connect"
            set server "100.64.1.1"
            set protocol tcp-connect
            set port 22
            set quality-measured-method half-open | half-close
        next
    end
end
```

Measure latency based on connection setup

Measure latency based on connection teardown

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

Active monitoring with TCP connect works by initiating TCP connections to the target servers using a custom port. TCP connect enables you to test the connectivity of any TCP application running on the target servers, by monitoring packets exchanged for TCP connection setup and teardown. That is, when you set `quality-measured-method` to `half-open`, FortiGate determines the latency based on the round-trip time (RTT) between the TCP SYN it sends and the TCP SYN-ACK that it receives. If you set `quality-measured-method` to `half-close`, FortiGate determines the latency based on the RTT between the TCP FIN it sends and the TCP FIN-ACK that it receives.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Active Monitoring—TWAMP

- TWAMP
  - Client-side implementation
    - On SD-WAN FortiGate
  - Most accurate protocol
  - Two sessions:
    - Control: TCP 862 by default
      - Not seen if authentication is disabled (default=disabled)
    - Test: UDP 862 by default

```
config system sdwan
    config health-check
        edit "TWAMP"
            set server "100.64.1.1"
            set protocol twamp
            set port 0
            set security-mode authentication
            set password fortinet
        next
    end
end
```

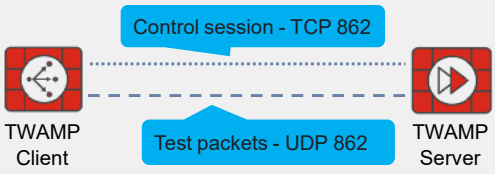
Set to 0 to use default port (port 862); (default = 0)

- FortiGate as TWAMP server
  - Configure the server side for TWAMP

```
config system probe-response
    set port 862
    set mode twamp
    set security-mode authentication
    set password fortinet
end
config system interface
    edit "port1"
        append allowaccess probe-response
...
```

Default port: 8008

Enable probe-response access




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

Two-Way Active Management Protocol (TWAMP)—described in RFC 5357—is the most accurate protocol among the five monitoring protocols that FortiGate supports.

SD-WAN uses the client-side implementation of TWAMP. There are two sessions used in TWAMP: control and test. The former is used to authenticate the endpoints, and the latter to exchange packets used to measure the performance. Note that if authentication is disabled—it is disabled by default—FortiGate generates the test session only. SD-WAN uses port 862 as default port for both control and test sessions, but you can configure a different port, as shown on this slide.

The TWAMP server can be any compatible device, such as a Linux or a Windows server. You can also configure FortiGate as a TWAMP server in your network. For example, you can use the FortiGate device that acts as hub in the SD-WAN topology. You can then configure the performance SLAs that use TWAMP to point to the FortiGate device acting as TWAMP server.

This slide shows a CLI configuration examples of a FortiGate TWAP client and a FortiGate TWAMP server, both have authentication enabled.

To configure a TWAMP server on FortiGate, you configure a probe response service. Note that, unlike the client-side implementation used in performance SLAs, the server-side implementation uses a different default port for TWAMP—port 8008. Also, make sure to enable `probe-response` access on the interface that listens for TWAMP requests.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Passive Monitoring

- Probe-free performance monitoring
  - Performance based on member traffic
- Benefits
  - More accurate measuring
  - Simplified configuration
  - Reduced network traffic
- Limitations:
  - Only TCP traffic is measured
    - Latency is based on RTT during TCP setup and teardown
    - Jitter and packet loss are based on TCP headers
  - No member state detection
    - Members are always alive
  - Hardware acceleration is disabled

- CLI configuration
  - Performance SLA:

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end
```

  - Firewall policy:

```
config firewall policy
    edit 5
        set passive-wan-health-measurement enable
    next
end
```

```
# show full firewall policy 5 | grep auto
        set auto-asic-offload disable
```

Hardware acceleration is automatically disabled

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

Active monitoring requires you to configure target servers and protocols for each probe, which can sometimes result in complex SD-WAN configurations. In addition, the more active health checks and members you configure, the more monitoring traffic is generated in the network.

Passive monitoring simplifies configuration and reduces network traffic by using a probe-free approach for measuring the performance of members. FortiGate measures packet loss, latency, and jitter based on TCP traffic sent and received through a member. Passive monitoring is a more accurate approach than active monitoring because you measure the member performance based on the actual traffic passing through the member, instead of measuring it based on probes that may be unrelated to the application you want to effectively steer using SD-WAN. For example, configuring a ping probe to monitor the health of a member that is used to steer web traffic won't provide more accurate performance metrics than the ones obtained by monitoring the web traffic itself.

In passive monitoring, latency is calculated based on the round-trip time (RTT) of TCP connection setup and teardown, while jitter and packet loss are calculated based on TCP header information.

Note that passive monitoring doesn't detect dead members. That is, members are always assumed alive. Also, note that hardware acceleration is disabled on traffic subject to passive monitoring.

This slide shows a CLI configuration example for passive monitoring. Note that, in addition to configuring the health check in passive mode (`set detect-mode passive`), you must also enable `passive-wan-health-measurement` on the firewall policies that accept traffic for the monitoring member. When you enable `passive-wan-health-measurement` on a policy, `auto-asic-offload` is automatically disabled.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Per-Application Passive Monitoring

- Differentiate and collect metrics for apps defined in rules
  - If multiple apps are defined, an average is calculated
- Benefits
  - Most accurate monitoring method
- CLI configuration:

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end
config firewall policy
    edit 5
        set passive-wan-health-measurement enable
    next
end
```

- CLI configuration (contd):

```
config system sdwan
    config service
        edit 1
            set name "GoToMeeting-Salesforce"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 16354 16920
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end
```

Application IDs:
16354: GoToMeeting
16920: Salesforce

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

When you use passive monitoring, you get more accurate member metrics because the metrics are calculated based on the actual traffic passing through the members. However, if multiple applications use the same member, then the member metrics are a result of measuring the traffic for multiple applications, including irrelevant applications. This lack of granularity may affect the steering decisions made by FortiGate for SD-WAN rules configured for specific applications.

Per-application passive monitoring instructs FortiGate to measure the member quality based on the performance of applications selected in SD-WAN rules. For SD-WAN rules, you select applications by choosing the respective internet service or application name. FortiGate then differentiates and collects the metrics for each internet service and application. If you define multiple applications in a rule, then FortiGate determines the member quality by averaging the metrics of all configured internet services and applications in the rule.

The configuration required for per-application passive monitoring is the same as regular passive monitoring, except that you must enable `passive-measurement` in one ore more SD-WAN rules that match traffic based on the detected application. These type of rules enable you to perform application steering, and you will learn more about it in another lesson.

This slide shows a CLI configuration example for per-application passive monitoring. The configuration instructs FortiGate to passively measure the quality of members 3 and 4 by averaging the metrics measured for GoToMeeting and Salesforce traffic passing through members 3 and 4.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Prefer Passive Monitoring

- Mix of passive and active monitoring
  - Passive when there is TCP traffic
  - Active when no TCP traffic has been detected for 3 minutes (hard-coded)
- Dead members detected during active monitoring

- CLI Configuration
  - Performance SLA:

```
config system sdwan
    config health-check
        edit "T_INET_0_Passive"
            set server "10.1.0.7"
            set protocol ping
            set detect-mode prefer-passive
            set members 3
        next
    end
end
```

  - Firewall policy:

```
config firewall policy
    edit 5
        set passive-wan-health-measurement enable
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

An alternative to active and passive monitoring is prefer passive monitoring.

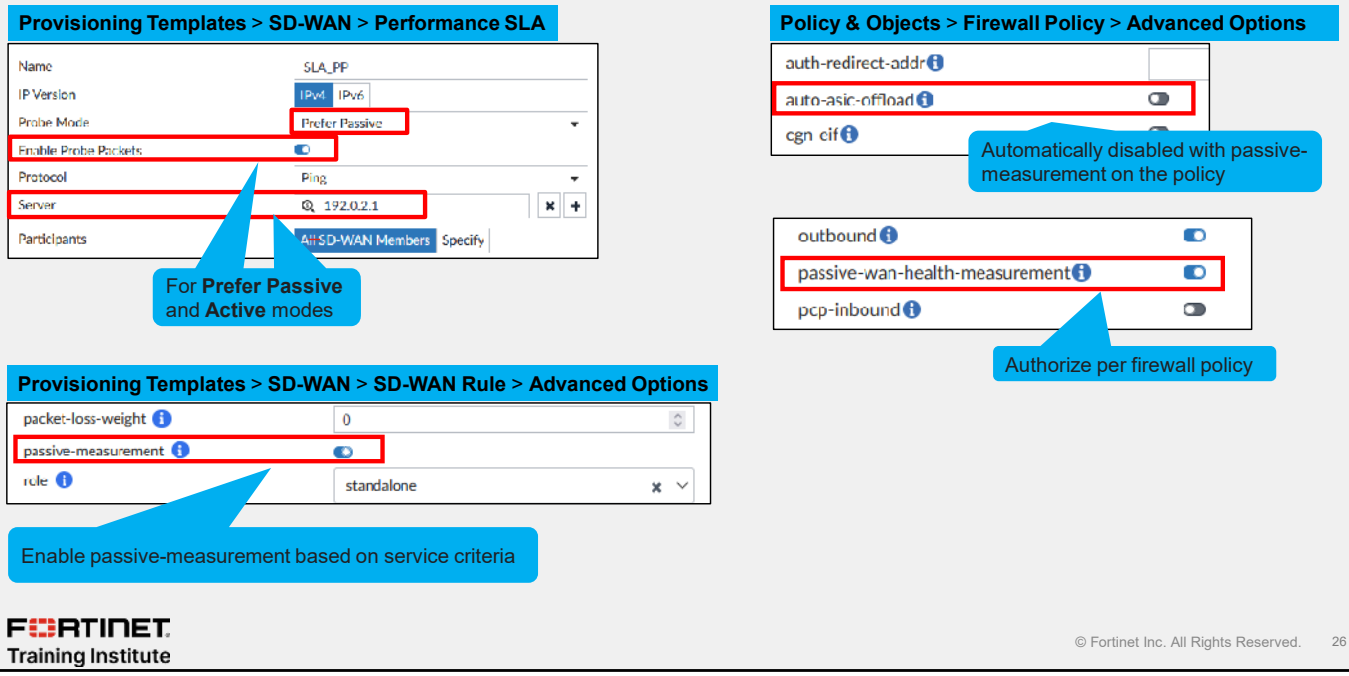
In prefer passive monitoring, FortiGate uses passive monitoring if there is TCP traffic through the member. If no TCP traffic is detected for three minutes, then FortiGate starts using the configured probe to actively monitor the state and performance of the member. If FortiGate later detects TCP traffic through the member, it switches immediately back to passive monitoring. Note that changes in member state are detected only when FortiGate is doing active monitoring. Also note that the 3-minute TCP traffic idle timer is hard-coded and can't be changed.

This slide shows a CLI configuration example for prefer passive monitoring. FortiGate starts pinging `10.1.0.7` only after no TCP traffic has been seen through the member for three minutes. Like in passive monitoring, you must enable `passive-wan-health-measurement` on the firewall policies that accept traffic for the monitoring member. Consequently, this also results in `auto-asic-offload` being automatically disabled on the respective policies.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Passive Monitoring—GUI Configuration




This slide shows the GUI menus used for the configuration of passive performance SLA monitoring.

After you select **Passive** or **Prefer Passive** for a performance SLA, you must activate **passive-wan-health-measurement** for at least one policy with SD-WAN zone as the source or destination interface. This option will automatically disable **auto-asic-offload** for the policy.

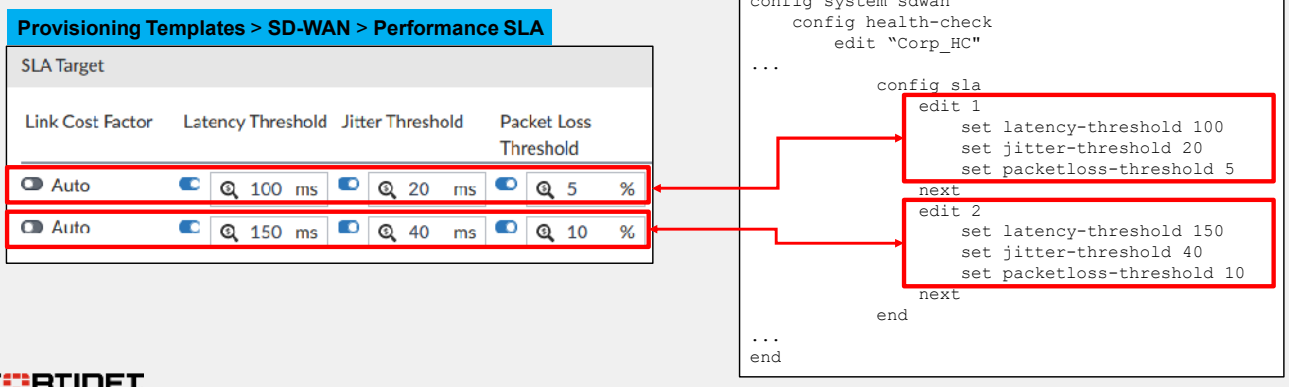
If you want to specify the service used for passive measurement, you must activate **passive-measurement** on the corresponding SD-WAN rule.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SLA Targets

- Define member performance requirements
- Used by lowest cost (SLA) rule—with or without load balancing
- Members that meet one or more SLA targets are preferred for steering the traffic
- Configure one or more SLA targets per performance SLA
  - Use same health check for multiple applications




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

When you configure a performance SLA, you can optionally configure SLA targets. SLA targets define the performance requirements that alive members must meet for being a preferred member for traffic steering. SLA targets are required by SD-WAN rules that use lowest cost (SLA) as a strategy. In addition to verifying that members are alive, these strategies also check the quality of the members.

Using SLA targets enable you to fine-tune SD-WAN rules for specific applications. For example, you may want to configure an SD-WAN rule that steers voice traffic through members whose latency and jitter don't exceed 300 msec and 30 msec, respectively. Otherwise, the quality of voice during calls will likely be poor.

You can configure one or more SLA targets per performance SLA. This enables you to have different performance requirements for the same monitoring mode, and then configure the SD-WAN rule to use the best suited SLA target for a given application. For example, you can monitor the performance of a member using a particular mode—active, passive, or prefer passive—and then define two SLA targets, one with stricter performance requirements than the other. You can then configure an SD-WAN rule that steers sensitive traffic to use the stricter SLA target, and another SD-WAN rule that steers non-sensitive traffic to use the more lenient SLA target.

This slide shows a configuration example using SD-WAN templates on FortiManager, and the corresponding CLI settings on FortiGate.

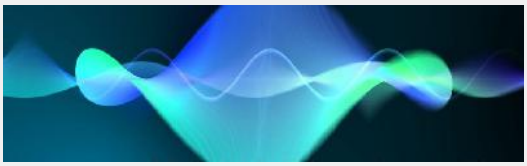

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

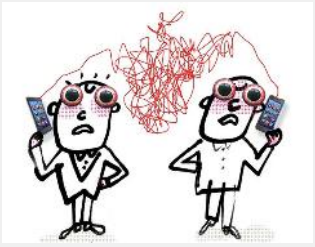
## MOS—Mean Opinion Score

- MOS measures the perceived quality of VoIP traffic
  - Scale from one to five
  - Five is the best theorical possible score
- Link quality for voice traffic
  - Combines latency, jitter, and packet loss
  - Formula per codec: G.711, G.729, G.722
  - Provides a score from one to five
- Benefits
  - Optimize link selection for voice traffic
  - Better user experience
- Limitation
  - SD-WAN rule mode lowest cost (SLA) only

MOS 4.9: perceived voice quality is very good



MOS 1.2: perceived voice quality is poor



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

The perceived voice quality is sensitive to multiple factors, including latency, jitter, and packet loss, and the interactions between them. The MOS is a method of measuring link quality using a formula that takes into account latency, jitter, packet loss, and the codec to produce a score from one to five. You can use this score to steer voice traffic to the most appropriate link for optimal perceived voice quality.

Available codecs are G.711, G.729, and G.722 (default G.711).

Note that on FortiGate, you can associate MOS performance SLAs only with rules defined with the lowest cost (SLA) strategy.

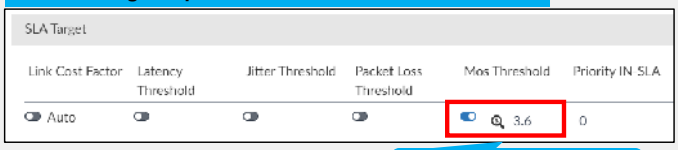

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Performance Settings for VoIP

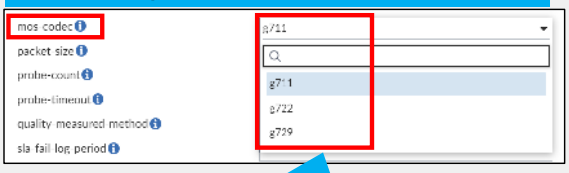
- FortiManager GUI

**Provisioning Templates > SD-WAN > Performance SLA**




Enable MOS calculation and define the threshold

**Provisioning Templates > SD-WAN > Performance SLA > Advanced Options**




Select the MOS codec, used to define the calculation formula

- FortiGate CLI

```
config system sdwan
    config health-check
        edit "Voice_health"
           set server "10.200.99.1"
           set mos-codec g711
           set members 3 4
           config sla
              edit 1
                 set link-cost-factor mos
                 set mos-threshold "3.6"
              next
     . . .
    config service
        edit 1
           set name "MOS_traffic_steering"
           set mode sla
           config sla
              edit "Voice_health"
                 set id 1
              next
           end
           set priority-members 3 4
        next
```

Forward VoIP traffic to the member with MOS 3.6 or above

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

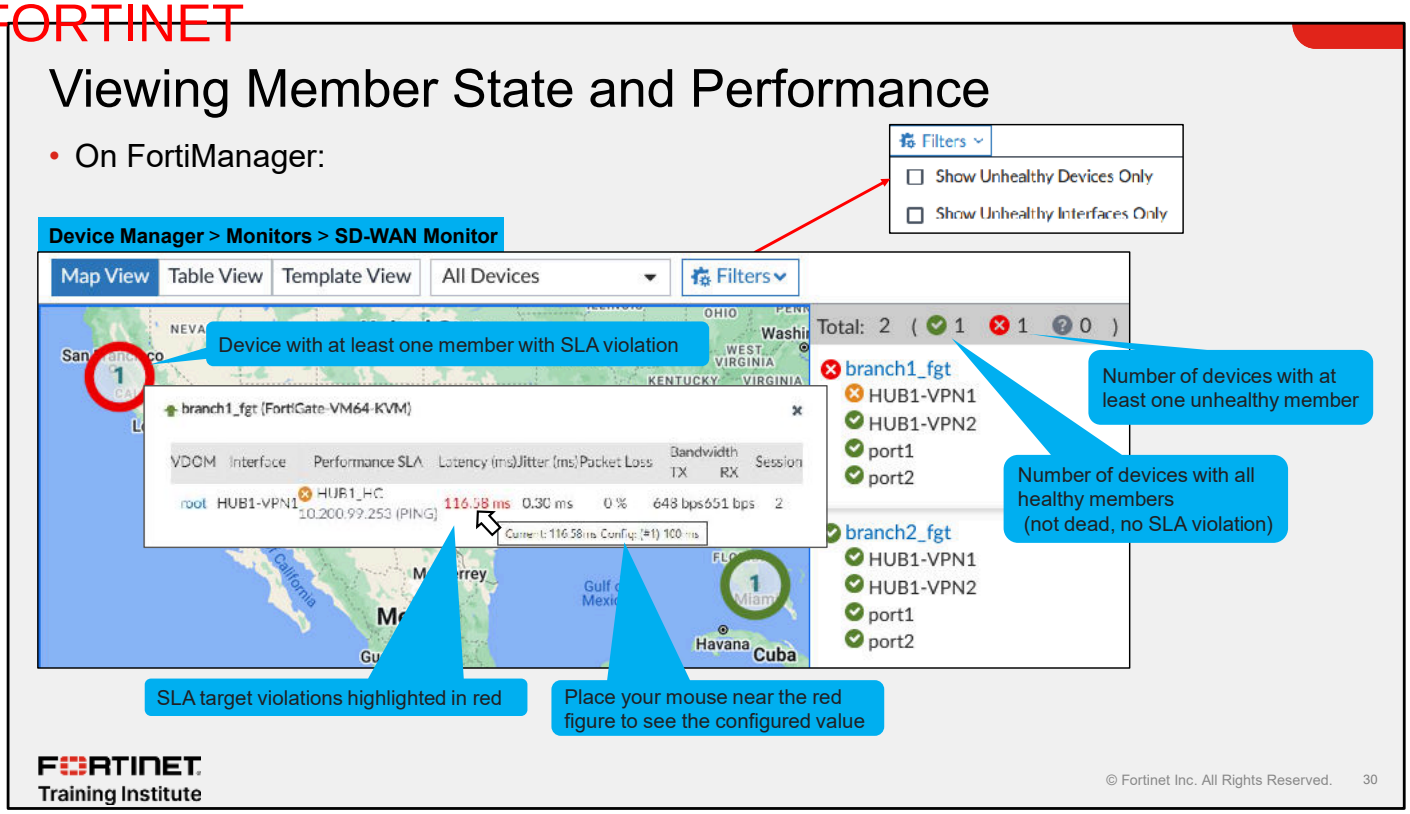
You can define performance SLA with MOS criteria using GUI or CLI commands, as this slide shows. The MOS codec you use for the calculation should match the codec you use for the voice traffic on your network.

Remember that you can use MOS only when service is lowest cost (SLA). It is not supported with manual or best quality service mode.

The MOS threshold indicates the minimum MOS score for the SLA to pass. It is defined as a one-digit decimal value between 1.0 and 5.0, with a default of 3.6.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




You can use FortiManager and the FortiGate GUI to view the state and performance of members.

Both FortiManager and the FortiGate GUI indicate whether the member is alive or dead. In FortiManager, alive members are shown with a green icon, and members that miss at least one SLA target are shown with an orange icon, dead members with a read icon.

When you hover your mouse over a member, you can view the measured performance of members that are up. Then, place you mouse on missed SLA target—red figures—to see the SLA value configured. If you configure SLA targets, both FortiManager and FortiGate highlight the members that don't meet the configured SLA targets.

In the example shown on this slide, the **HUB1_HC** performance SLA reports that **HUB1-VPN1** doesn't meet the configured SLA target for latency criteria. The administrator placed the mouse near the red figures, 116.58 ms, to check the SLA configuration—100 ms.

From the map view, you can use filters to see only healthy or only unhealthy devices.

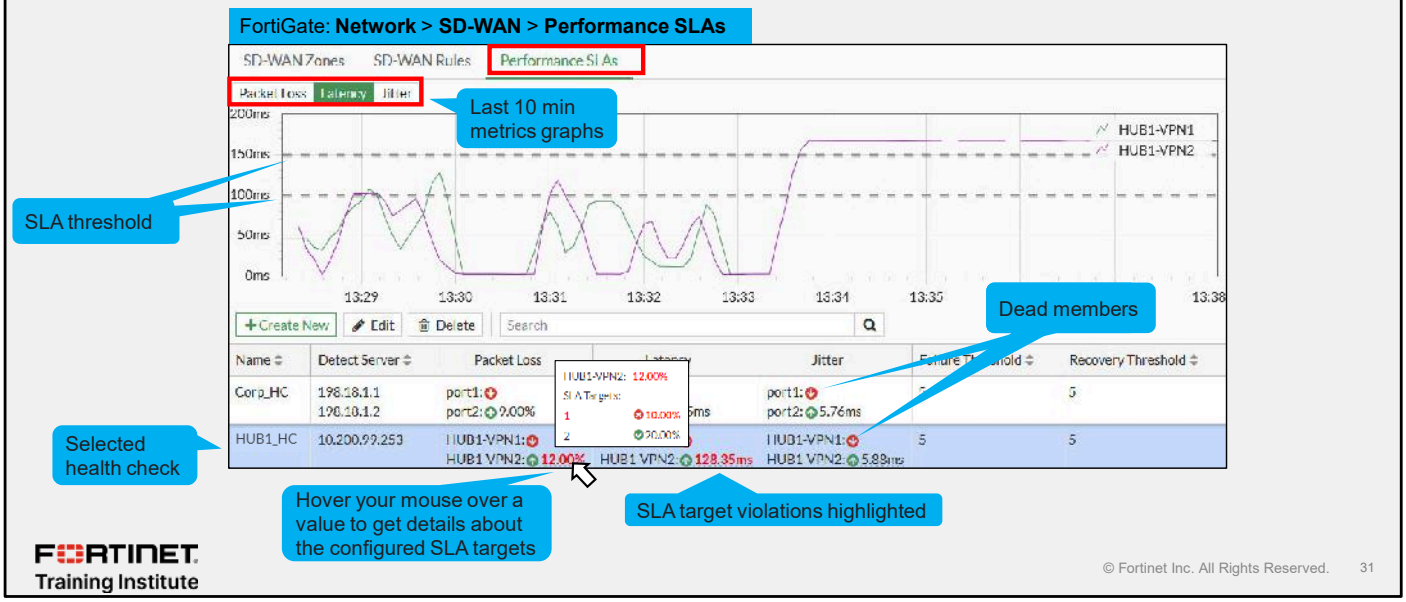


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Viewing Member State and Performance (Contd)

- On the FortiGate GUI:




The FortiGate GUI shows the state and performance of members, with some additional details.

Like FortiManager, the FortiGate GUI allows you to easily see alive and dead members. The FortiGate GUI shows alive members with a green up arrow icon, and dead members with a red down arrow icon. For a missed SLA target, the FortiGate GUI highlights the impacted metric in red.

FortiOS stores the last 10 minutes of SLA metrics for each monitoring member. The FortiGate GUI displays the graph for the selected performance SLA and criteria.

In the example shown on this slide, the **HUB1_HC** performance SLA is selected and reports that **HUB1-VPN2** is alive and **HUB1-VPN1** is dead. The administrator placed the mouse near the packet loss value for **HUB1-VPN2** and can see two SLA targets configured: The first to 10%, that the link missed, and the second to 20%, that it passed.

The graph shows latency for both monitored interfaces over the past 10 minutes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Viewing Member State and Performance on the FortiGate CLI

- Performance SLA:

```
# diagnose sys sdwan health-check status
Health Check(Corp_HC):
Seq(1 port1): state(alive), packet-loss(9.000%) latency(42.351), jitter(0.270), mos(4.377), bandwidth-up(10217),
bandwidth-dw(10016), bandwidth-bi(20233) sla_map=0x1
Seq(2 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Health Check(HQ):
Seq(3 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(0.000), jitter(0.000), mos(4.404), bandwidth-
up(10240), bandwidth-dw(10240), bandwidth-bi(20480) sla_map=0x0
```

Configuration index number

- Link monitor status:

```
# diagnose sys link-monitor interface port1
Interface(port1): state(up, since Fri Jul 05 08:22:49 2024), bandwidth(up:79743bps, down:1094502bps), session
count(IPv4:412, IPv6:0), tx(39720018 bytes), rx(2184681 bytes), latency(21.96), jitter(0.17), packet-loss(0.00).
```

- Link monitor passive status:

```
# diagnose sys link-monitor-passive admin list
  HUB1-VPN1( 19) | service=0x00000000 | latency=70.0  14:21:35 | jitter=0.0  14:21:47 | pktloss=0.0 %  14:21:47
```

Last time for criteria check

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

You can also display the state and performance of members on the FortiGate CLI, which is often more convenient for troubleshooting purposes.

The `diagnose sys sdwan health-check status` command displays the member status information per performance SLA. The output includes both the member state and the measured performance.

The performance SLAs rely on the FortiOS link monitor process (`lnkmtd`) to monitor the state and performance of members. For this reason, you can run the `diagnose sys link-monitor interface` command to display member status information that is similar to what is displayed by the `diagnose sys sdwan health-check status` command.

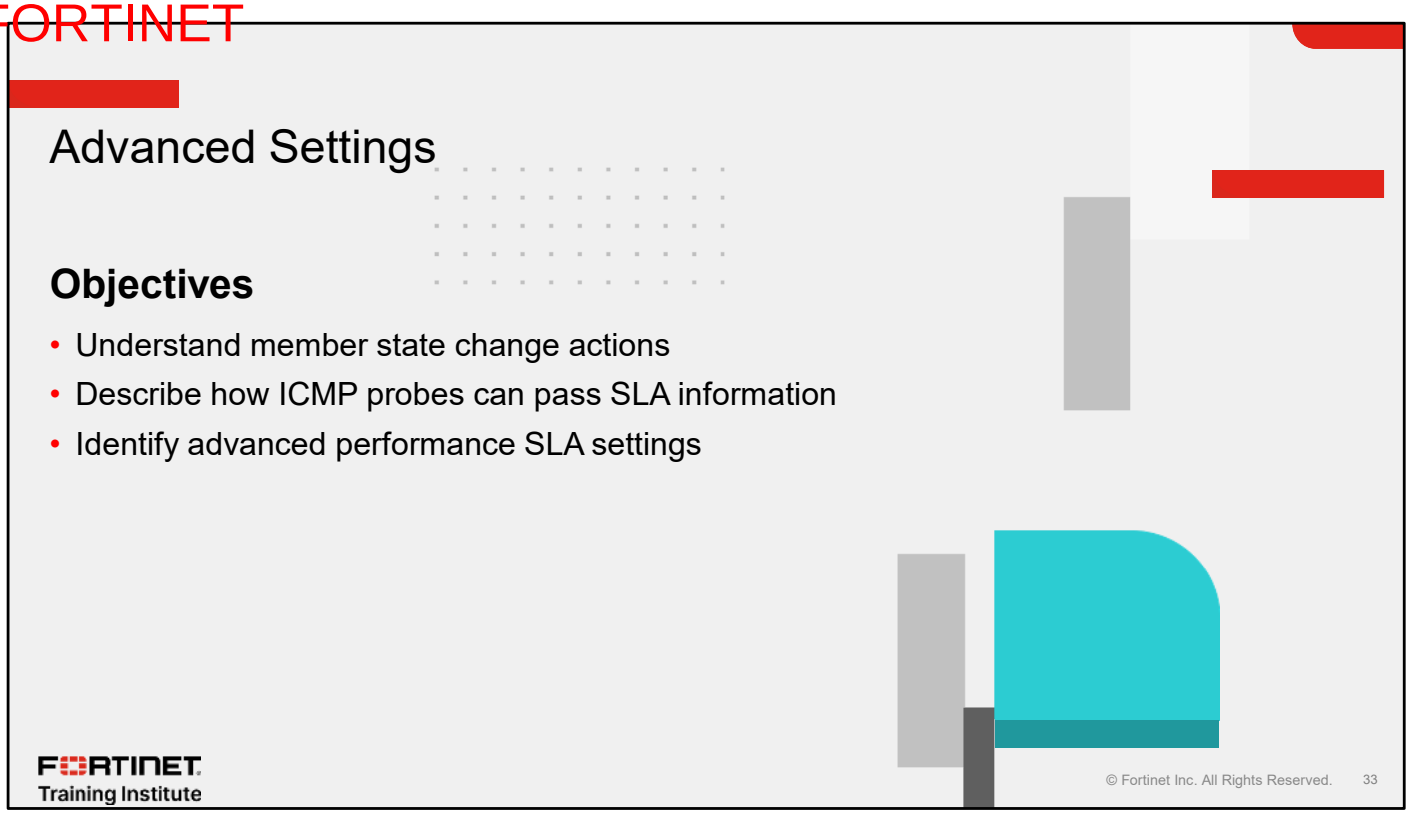
In passive or prefer passive mode, the link monitor passive process (`lnkmt_passive`) is responsible for gathering the data and preparing the reports used by the link monitor process to calculate packet loss, latency, and jitter. For this reason, you can run the `diagnose sys link-monitor-passive admin list` command to display the passive data collected.

This slide shows sample outputs for the three commands discussed on this slide. Note that the `Corp_HC` performance SLA monitors `port1` and `port2` actively, while `HQ` monitors `HUB1-VPN1` passively. Also note that `port2` is dead.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

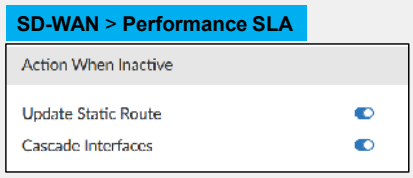
By demonstrating a competent understanding of advanced SLA performance settings, you will be able to use them effectively in your network.


Vouchers & Dumps are Available | WhatsApp +201224560923

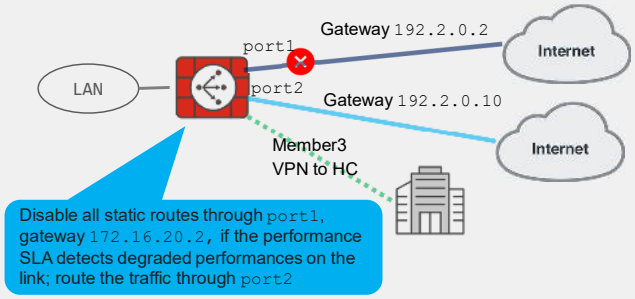
DO NOT REPRINT Brave-dumps.com
© FORTINET

## Performance SLA—Member State Change Actions

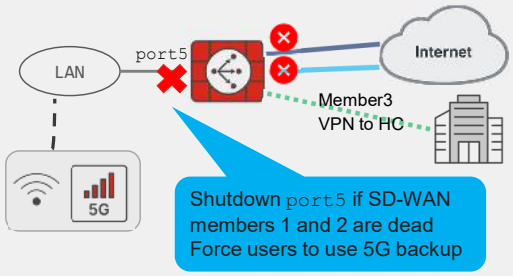
- Define actions when members are inactive
  - **Update Static Route**
  - **Cascade Interfaces**
  - Default for both options: enabled
  - Define the behavior of interfaces or static routes when the SD-WAN members do not meet SLAs or are down




- Use case for **Update Static Route**:




- Use case for **Cascade Interfaces**:




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

For each performance SLA that you configure, you can select the actions that FortiGate takes when the link performances degrades. The possible actions that FortiGate can take when it declares SD-WAN link members down are: **Update Static Route** and **Cascade Interfaces**. Note that both actions are enabled by default, for each performance SLA.

When **Update Static Route** is enabled, FortiGate disables the static routes for inactive interfaces. In the example shown on this slide, FortiGate disables all static routes that go through the interface `port1` and are configured with the gateway `192.2.0.2`. The objective of this action is to route the traffic through the alternative link—through `port2`—and to apply this change to every flow, whether it is steered by SD-WAN or not. When you enable **Update Static Route**, you must carefully consider the consequence on overlay tunnels. In this example, the tunnel to the headquarters, which is defined as the SD-WAN member3, is impacted if it is established over `port1` and it uses a static route to connect to its IPsec peer. FortiGate needs to establish a new tunnel through `port2`—if this option is configured.

The **Cascade Interface** feature is enabled by default, but is active only after the administrator defines at least one cascade interface. In the example shown on this slide, the administrator defined `port5` as cascade interface for the performance SLA that monitors the ISP links, `port1` and `port2`. Therefore, when the performance SLA finds both links are invalid, FortiGate shuts down the interface `port5`. You usually use these settings to force a flow, in this example the LAN traffic, to use an alternative path when the connections through the FortiGate are dead. In this example, the administrator instructed the LAN device to use WIFI and a 5G connection, when the wired connection is not longer valid. You can use a similar configuration, if you have a Virtual Router Redundancy Protocol (VRRP) router that directs traffic to FortiGate or to a backup device.

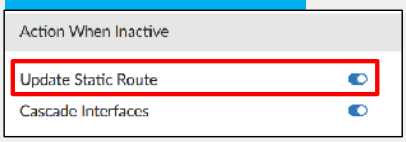


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Member State Change Actions—Update Static Route

SD-WAN > Performance SLA




- Update status of static routes matching the gateway of members that change their state
- Static routes of alive members are installed in the routing table

```
# diagnose sys sdwan member
Member(1): […] interface: port1, flags=0x0 , gateway: 192.2.0.2, source 192.2.0.1, priority: 1 1024, weight: 0
Member(2): […] interface: port2, flags=0x0 , gateway: 192.2.0.10, source 192.2.0.10, priority: 1 1024, weight: 0
Member(3): […] interface: HUB1-VPN1, flags=0xc , gateway: 100.64.1.1, source 192.168.1.2, priority: 1 1024, weight: 0

# diagnose sys sdwan health-check status
Health Check(Corp_HC):
Seq(1 port1): state(alive), packet-loss(2.000%) latency(22.300), jitter(0.218) ...
Seq(2 port2): state(alive), packet-loss(0.000%) latency(52.406), jitter(0.253) ...
Health Check(HQ):
Seq(3 HUB1-VPN1): state(alive), packet-loss(3.000%) latency(1.891), jitter(0.319)...

# get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
...
S       10.0.0.0/8 [10/0] via HUB1-VPN1 tunnel 100.64.1.1, [1/0]
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

When **Update Static Route** is enabled, FortiGate updates the status of static routes that match the gateway used by a member that changes its state—from alive to dead, and vice versa. This setting is enabled by default. The goal is to prevent traffic from being routed through a dead member.

When the member is alive, the static routes become active, and therefore, are installed in the routing table if they are determined the best routes, or other active routes, to the destination. Note that static routes of members configured with automatic gateway detection are also automatically identified by FortiGate.

The example on this slide shows the status of three members: `port1`, `port2`, and `HUB1-VPN1`. The three members are alive, and therefore, the static routes that match the member gateway is assigned an active status. The result is that the static routes are installed in the routing table.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Member State Change Actions—Update Static Route (Contd)

- Static routes of dead members become inactive
  - Inactive routes are removed from the routing table
  - You can view the inactive routes in the routing table database

```
# diagnose sys sdwan health-check status
Health Check(Corp_HC):
Seq(1 port1): state(alive), packet-loss(4.000%) latency(1.634), jitter(0.894),..., sla_map=0x1
Seq(2 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Health Check(HQ):
Seq(3 HUB1-VPN1): state(dead), packet-loss(100.000%) sla_map=0x0

# get router info routing-table database
...
S     *> 0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
       >           [1/0] via 192.2.0.10, port2 inactive, [1/0]
...
S       10.0.0.0/8 [10/0] via HUB1-VPN1 tunnel 100.64.1.1 inactive, [1/0]
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

If a member is determined dead, the static routes that match the member gateway become inactive. The result is that the routes are not installed in the routing table.

The example on this slide shows `port2` and `HUB1-VPN1` as dead. As a result, the static routes that match the gateways used by `port2` and `HUB1-VPN1` become inactive. For this reason, you can view the impacted static routes in the routing table database only.

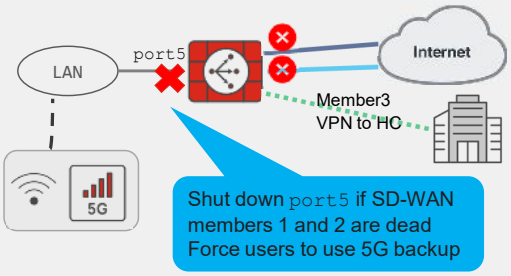


Vouchers & Dumps are Available | WhatsApp +201224560923

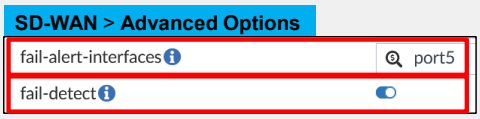
DO NOT REPRINT Brave-dumps.com
© FORTINET

## Member State Change Actions—Cascade Interfaces

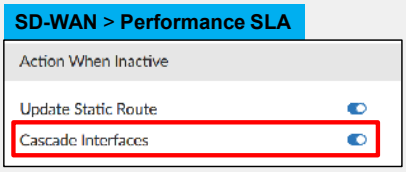
- Shut down alert interfaces, if all members are dead
- Bring up alert interfaces, if at least one member is alive
- Use case: Force the LAN to use an alternative path




- For each SD-WAN instance




- For each performance SLA




Configure one or more alert interfaces

```
config system sdwan
    set fail-detect enable
    set fail-alert-interfaces "port5"
    config health-check
        edit "Corp_HC"
            set update-cascade-interface enable
            set members 1 2
        next
        edit "HQ"
            set update-cascade-interface enable
            set members 3
        next
    ...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

When you enable **Cascade Interfaces** and configure one or more alert interfaces, one of the following events occurs:

- FortiGate shuts down the alert interfaces, if all members are dead, for example, because of degraded performances.
- FortiGate brings up the alert interfaces, if at least one member is alive.

**Cascade Interfaces** is useful to force the traffic from networks behind the alert interfaces to be routed through a different device, if all SD-WAN members are dead, which could mean that FortiGate is unable to forward traffic to the WAN.

You define the cascade interfaces globally for the SD-WAN instance, and then you activate the detection and action for each performance SLA. For example, you might decide to cascade, if the underlay links fail to meet the health check, but not set the trigger for overlay links.

Usually, you should configure alert interfaces for critical interfaces, such as LAN interfaces, which provide users with WAN access, and for which you want WAN traffic to be rerouted through a different device if all SD-WAN members are dead. For example, if you are using dynamic routing VRRP on your LAN interface, then shutting down the interface can trigger a routing failover to a backup gateway. In the example shown on this slide, the company provides backup for LAN users with a 5G device not connected to FortiGate.

This slide shows an example of the **Cascade Interfaces** option enabled and the interface to shut down—port5—configured on FortiManager; and the equivalent configuration on the FortiGate CLI.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Member State Change Actions—Cascade Interfaces (Contd)

- Alert interface (port5) is up if there is at least one alive member:

```
# diagnose sys sdwan health-check status
Health Check(Corp_HC):
Seq(1 port1): state(alive), packet-loss(73.000%) latency(1.546), jitter(2.071), ..., sla_map=0x1
Seq(2 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Health Check(HQ):
Seq(3 HUB1-VPN2): state(dead), packet-loss(99.000%) sla_map=0x0

# diagnose hardware deviceinfo nic port5 | grep "Link|State"
State:              up
Link:               up
```

port5 interface status

- Alert interface is down if all members are dead:

```
# diagnose sys sdwan health-check status
Health Check(Level3_DNS):
Seq(1 port1): state(dead), packet-loss(11.000%) sla_map=0x0
Seq(2 port2): state(dead), packet-loss(97.000%) sla_map=0x0
Health Check(HQ):
Seq(3 HUB1-VPN2): state(dead), packet-loss(100.000%) sla_map=0x0

# diagnose hardware deviceinfo nic port5 | grep "Link\|State"
State:              down
Link:               down
```

port5 interface status

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

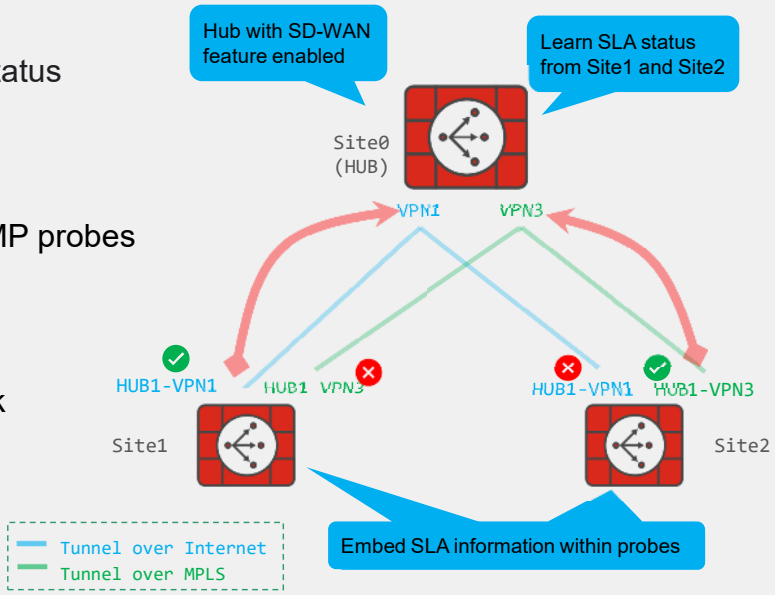
This slide shows the effect of **Cascade Interfaces** based on the configuration shown in the previous slide. If there is at least one alive member—port1 in the example—the alert interface (port5) is up. However, if all members are dead, port5 is brought down.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Embedded SD-WAN SLA Information in ICMP Probes

- Objectives
  - Inform remote device about link status
  - Allow symmetric link selection
- Principle
  - Spoke provides SLA status to hub
  - SLA information embedded in ICMP probes
  - Hub learns from remote devices
- Benefits
  - Compatible with static routing
  - Compatible with BGP on loopback topologies
- Limitations
  - Active probe mode
  - Protocol ping




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

In a hub-and-spoke design, if the hub is unaware of the spoke decision-making process, it might route traffic over a link that is different from the preferred spoke link. This can cause asymmetric traffic flow and selection of a poor performing link. To avoid this, the spoke SD-WAN device can pass SLA information to the hub with SLA information embedded into ICMP probes.

With embedded SD-WAN SLA information in ICMP probes, the spoke communicates the SLA status to the hub for each overlay, directly through ICMP probes. The hub can use the received SLA status information to apply priorities to the IKE routes, giving routes over overlays that are inside SLAs a lower priority value than routes over overlays that are outside of SLAs.

This method is particularly useful in combination with BGP and loopback topologies or with static routing. With BGP routing, when not on lookback topologies, it is a common practice to use the SD-WAN neighbor feature `route-map-out-preferable` setting to signal the health of each overlay to the hub. You will learn about this in another lesson.

Note that you need to use active probes and protocol ping to inform remote devices about SLA status.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Remote Health Check Configuration—CLI

- Spoke side
  - Embed SLA measure in health check

```
config system sdwan
    config health-check
        edit "to_hub"
            set server "4.2.2.1" "4.2.2.2"
            set detect-mode active
            set protocol ping
            set embed-measured-health enable
            set members 3 4
            config sla
               edit 1
                set link-cost-factor latency
                set latency-threshold 100
            end
        next
    end
end
```

- Hub side
  - Use SLA result provided by remote device

```
config system sdwan
    config health-check
        edit "from_spoke"
            set detect-mode remote
            set sla-id-redistribute 1
            set members 1 2
            config sla
               edit 1
                set link-cost-factor latency
                set latency-threshold 100
                set priority-in-sla 10
                set priority-out-sla 20
            end
        next
    end
end
```

Matching SLA criteria on hub and spoke

Lower value for higher priority route

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

This slide shows example CLI configurations.

On the spoke, you activate transmission of SLA information in the ICMP probe using the command `set embed-measured-health enable`. On the hub, you use the command `set detect-mode remote` to instruct the device to get SLA information from received SLA probes. On the hub, you must also define the priority to assign to IKE routes depending on whether the corresponding overlay is in SLA or out of SLA. You do this with the commands `set priority-in-sla` and `set priority-out-sla`. The lower the priority of an interface is, the more preferrable it becomes when considered with static routing. Optionally, you can define the SLA entry that is applied to the IKE routes using the parameter `sla-id-redistribute`.

For consistency, when using the remote detect mode, you must specify the same link cost factor and metric on the spoke and the hub. In the example shown on this slide, the SLA measure latency with a threshold set to 100.

You can use the embedded SLA mechanism with static routing or BGP for each overlay topology. However, note that to use embedded SLA with BGP, you must use static IP addressing for tunnels. It is commonly used with BGP on loopback. It is not compatible with the IKE option `mode-cfg`.

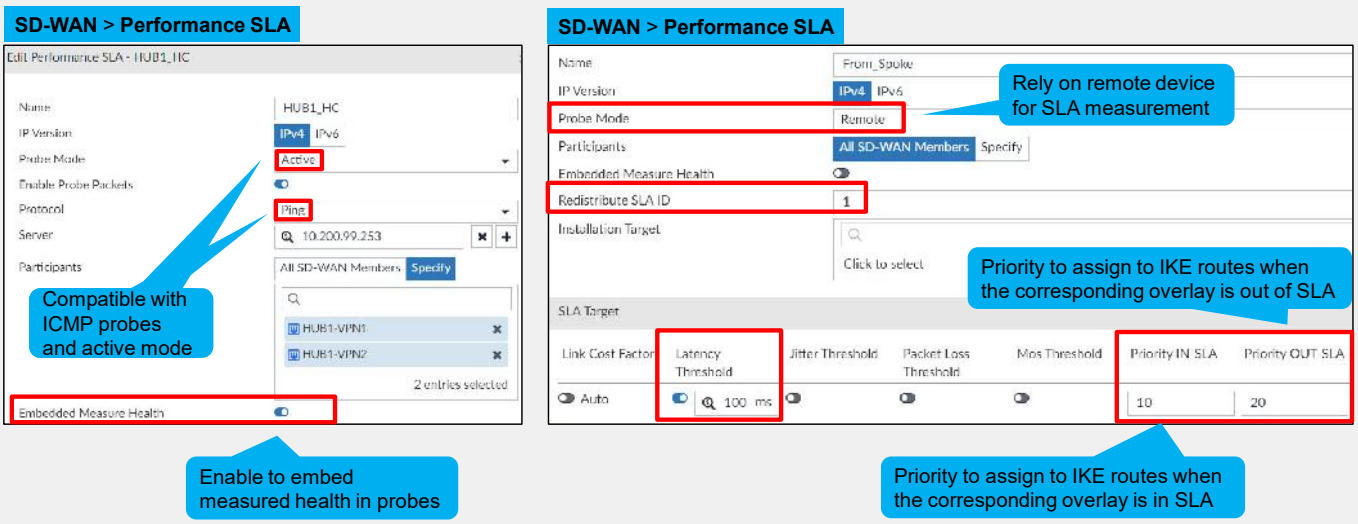


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Remote Health-Check Configuration—GUI

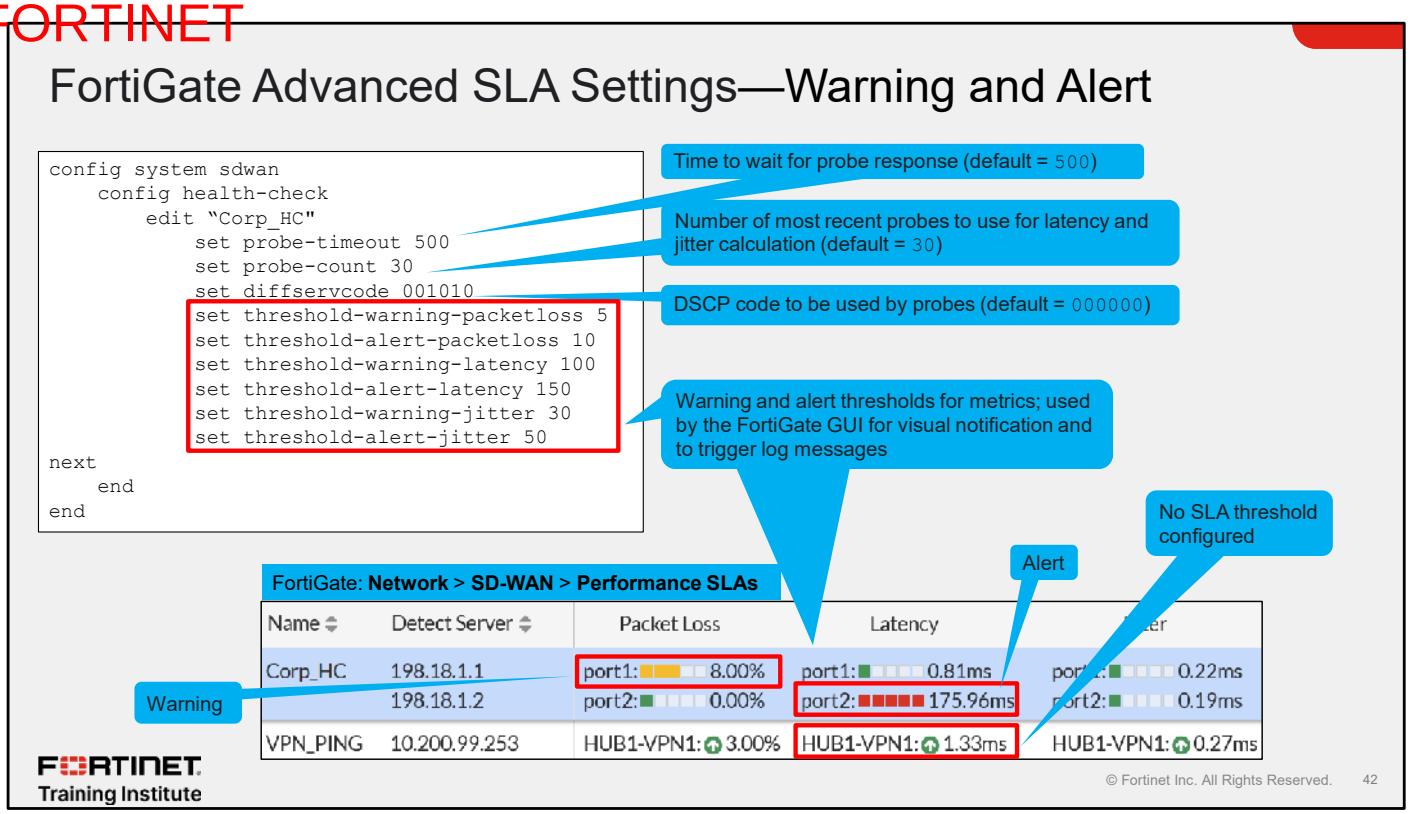
- Spoke side
  - Embed SLA measure in health check
- Hub side
  - Use SLA result provided by remote device




This slide shows the GUI configuration that corresponds to the CLI configuration shown on the previous slide. On the spoke side, for at least one performance SLA definition, you enable the parameter **Embedded Measure Health**. On the hub side, you configure the **Remote** probe mode and define the priority to set to IKE routes when the corresponding overlay is in or out of SLA with the parameters **Priority IN-SLA** and **Priority OUT-SLA**, respectively.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




This slide shows some advanced settings that you may want to configure for performance SLAs:

- `probe-timeout`: Defines the time, in milliseconds, to wait for probe responses before the response is considered lost. The default value is `500`.
- `probe-count`: Defines the number of the most recent probes to use to calculate latency and jitter. By default, FortiGate uses the last 30 probes. Note that this setting doesn't apply to packet loss calculation. Packet loss calculation always uses the last 100 probes.
- `diffservcode`: Sets the 6-bit differentiated services code point (DSCP) marking for probes. This is useful when a member is connected to a link that uses DSCP markings to classify and prioritize traffic. For example, some MPLS links prioritize packets with DSCP markings assigned for voice services. In this scenario, setting a DSCP probe enables you get more accurate member performance results for voice traffic. The default value is `000000`, which means no marking is used.
- `threshold-warning` and `threshold-alert`: These settings define the warning and alert thresholds for packet loss, latency, and jitter.
  - These settings are used by the FortiGate GUI. If a metric exceeds its configured threshold, the FortiGate GUI displays a visual notification. In the example shown on this slide, the measured packet loss has reached 8% for **port1** and is reported as a warning. The measured latency for **port2** exceeds its configured alert threshold (150 msec), which is why a critical notification is shown on the FortiGate GUI. The default value is `0`, which means no threshold is used. The FortiGate GUI displays no progress bar when warning or alert threshold remain at the default value. On the example, you can see that the administrator didn't define alert or warning thresholds for the VPN_PING health check.
  - FortiGate also uses these settings to trigger log messages. You can use FortiAnalyzer to collect and analyze these log messages, or use them to trigger automation stitches.



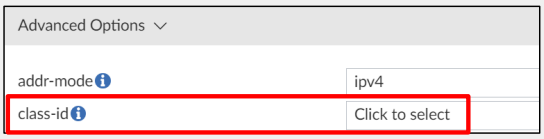
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Prioritize SLA Probes

- For networks using QoS
- Set **class-id** for SLA probes
- Advantages
  - Prioritize probes in times of congestion
  - Limit SD-WAN link flapping
  - Align the class IDs of probes and traffic steered through the link

- FortiManager GUI configuration




- CLI configuration

```
config system sdwan
   config health-check
      edit Corp_HC
         set class-id 4
      next
   end
end
```

Select the QoS class ID to assign to health-check probes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

If you use QoS on your network, you may want to define the QoS class ID for your SD-WAN health-check probes. If you set high-priority traffic classification on SLA probes, you ensure they are prioritized in times of congestion. This prevents SD-WAN link flapping and unexpected routing behaviors. It helps stabilize your SD-WAN traffic steering. Alternatively, you might decide to align the probe class ID with the class ID assigned to the traffic steered through the SD-WAN link.

When you configure a class ID for SLA probes, make sure to check periodically that the behavior is in line with your expectations. For example, you should avoid over prioritized probes, which means a link that remains active while the user traffic traveling through this link is degraded.

You can assign a class ID to each health-check probe using either the advanced option on the GUI or the `class-id` command on the CLI.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe underlay and overlay links and identify supported interfaces
- ✓ Identify and verify member and zone configuration
- ✓ Describe the benefits of using zones
- ✓ Identify performance SLA configuration sections
- ✓ Understand active, passive, and remote member monitoring
- ✓ Describe SLA targets and use cases
- ✓ Monitor member state and performance using FortiManager and the FortiGate CLI
- ✓ Identify relevant advanced performance SLA settings

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

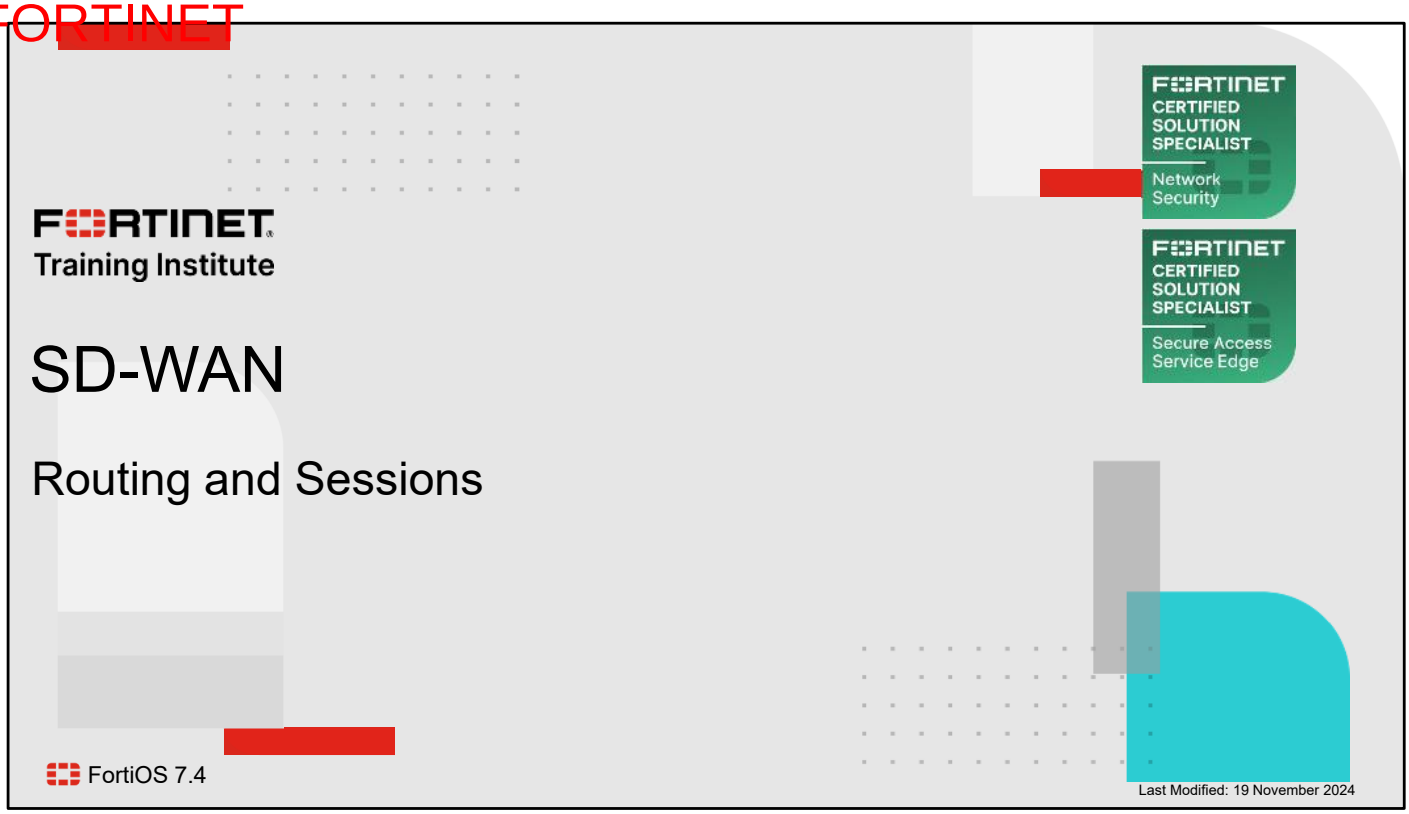
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the supported interfaces for SD-WAN, the benefits of placing members in zones, and the options available to monitor the state and performance of members.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

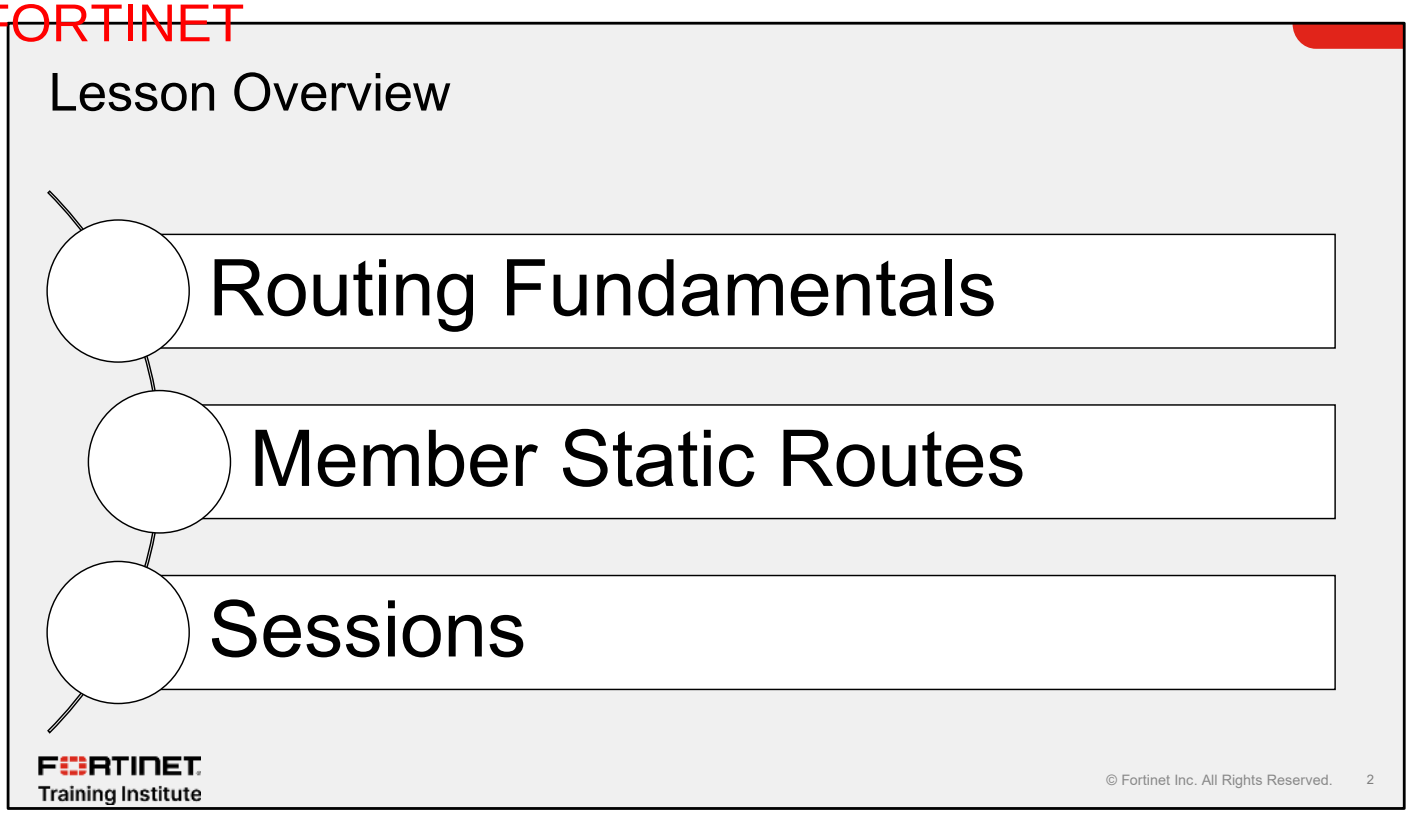



In this lesson, you will learn how FortiGate performs routing and handles sessions for SD-WAN traffic.



Vouchers & Dumps are Available | WhatsApp +201224560923

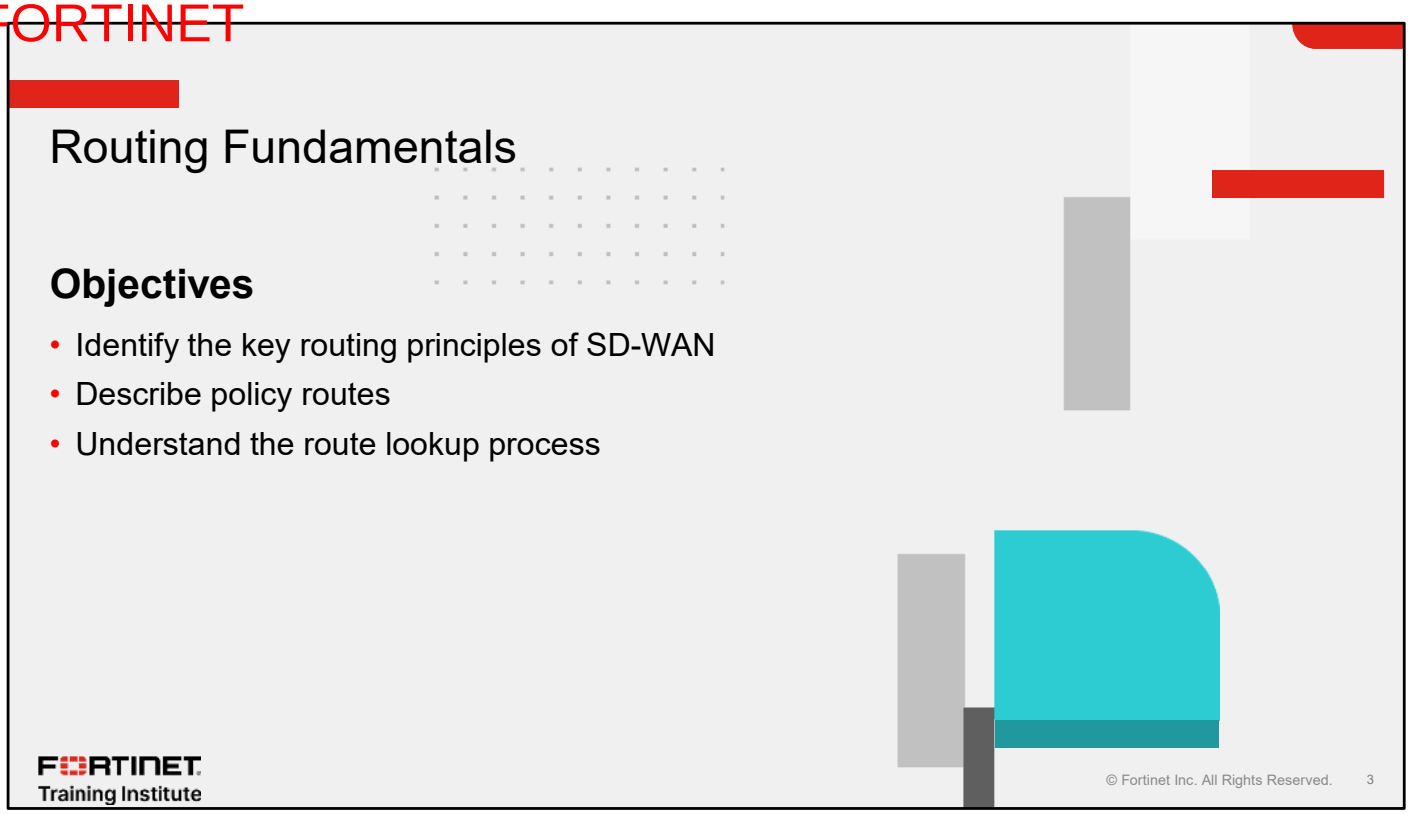
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding SD-WAN routing fundamentals, you will be able to understand how FortiGate performs routing when SD-WAN is involved.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Key Routing Principles

1. SD-WAN rules are policy routes
2. Regular policy routes have precedence over SD-WAN rules
3. Route lookup is done for new and dirty sessions
   - For original and reply traffic
   - Includes policy route lookup
4. SD-WAN rules are skipped if:
   - Best route to destination isn't an SD-WAN member
   - None of the members have a valid route to destination
     - If the preferred member doesn't have a valid route to destination, the next member in the rule is checked
5. Implicit SD-WAN rule equals standard forwarding information base (FIB) lookup
   - If lookup matches ECMP routes, traffic is load balanced using the configured algorithm

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

Routing is a core component of SD-WAN. Understanding how routing works in SD-WAN is essential for design and troubleshooting. The following are the SD-WAN key routing principles:

1. SD-WAN rules are policy routes. Like regular policy routes, SD-WAN rules route traffic based on multiple criteria. That is, when you configure an SD-WAN rule, the kernel installs a corresponding policy route that reflects the source, destination, service, and outgoing interfaces configured in the SD-WAN rule.

2. Regular policy routes have precedence over SD-WAN rules. Therefore, if you configure regular policy routes, you should ensure that their matching criteria is as narrow as possible. Otherwise, traffic that is intended to be handled by SD-WAN could end up being handled by regular policy routes instead.

3. FortiGate performs route lookup on both new and dirty sessions. A dirty session is a session that must be re-evaluated by the kernel after it is impacted by a change, such as routing, firewall policy, or interface change. FortiGate performs route lookups for both original and reply traffic. During route lookup, FortiGate checks policy routes before it looks for regular routes from the FIB.

4. FortiGate skips SD-WAN rules if the best route to the destination isn't an SD-WAN member. If the best route matches an SD-WAN member, then the selected member in the rule must have a valid route to the destination, otherwise FortiGate skips the member, and checks the next best member. If none of the members have a valid route to the destination, then FortiGate skips the rule.

5. The implicit SD-WAN rule equals standard FIB lookup. That is, if the traffic doesn't match any of the SD-WAN rules, then FortiGate routes the traffic using the regular routing process, which consists of looking for the best route in the FIB. If the best route matches equal cost multipath (ECMP) routes—usually the case—then FortiGate load balances the traffic using the configured load balancing algorithm.

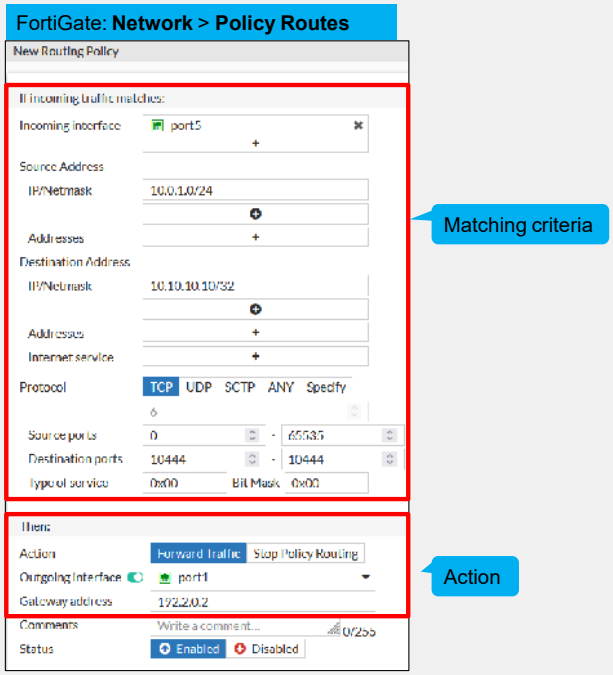


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Policy Routes

- SD-WAN rules are essentially policy routes
- Policy routes:
  - Provide more granular matching than static or dynamic routes:
    - Protocol
    - Source address
    - Source ports
    - Destination ports
    - ToS marking
    - Destination internet service
  - Have precedence over SD-WAN rules and entries in the FIB
  - Best practice: Narrow down matching criteria




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

When you configure an SD-WAN rule, FortiGate essentially applies a policy route in FortiOS. For this reason, before learning how routing in SD-WAN works, it is important that you first understand policy routes.

Static routes are simple and are often used in small networks. Policy routes, however, are more flexible because they can match more than just the destination IP address. For example, you can configure as matching criteria the incoming interface, the source and destination subnets, protocol, and port number. Because regular policy routes have precedence over any other routes, it is a best practice to narrow down the matching criteria as much as possible. Otherwise, traffic that is expected to be routed by SD-WAN rules or other routes in the FIB could be handled by regular policy routes instead.

This slide shows an example of a policy route configured using the FortiGate GUI. The policy route instructs FortiGate to match traffic received at **port5**, sourced from `10.0.1.0/24` and destined to the host `10.10.10.10`. The traffic must also be destined to TCP port `10444` for the policy route to match. FortiGate then forwards the traffic—**Forward Traffic** action—to **port1** through the gateway `192.2.0.2`.

On the FortiManager GUI, to configure a policy route, you must first enable the visibility of the corresponding menu. In the **Device & Groups** menu, select the device that you want to configure and then enable **Policy Routes** in the **Feature Visibility** list.

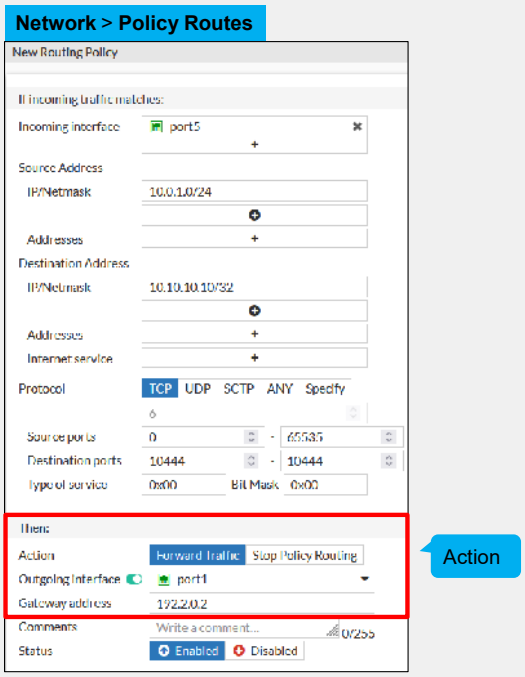


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Policy Routes—Actions

- **Stop Policy Routing**
  - Skips all policy routes, uses the FIB
- **Forward Traffic**
  - Forwards traffic using the set outgoing interface and gateway
  - FIB must have a matching route; otherwise, policy route is considered invalid and skipped




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

When a packet matches a policy route, FortiGate takes one of two actions. Either it routes the packet to the configured outgoing interface and gateway—**Forward Traffic** action—or it stops checking the policy routes—**Stop Policy Routing** action—so the packet is routed based on the FIB.

Note that when you configure **Forward Traffic** as the action, the **Destination Address**, **Outgoing interface**, and the **Gateway address** settings must match a route in the FIB. Otherwise, the policy route is considered invalid and, as a result, skipped.

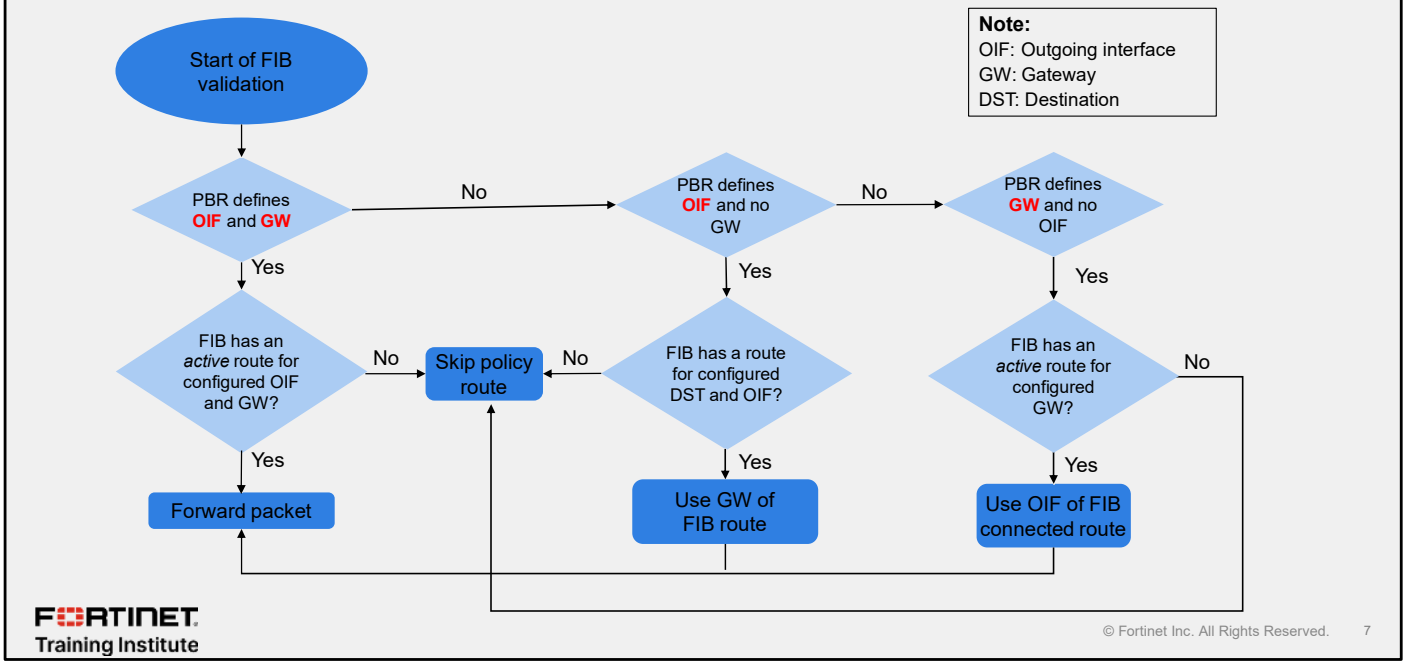
Also note that policy routes have precedence over SD-WAN rules, and over any routes in the FIB. That is, if a packet matches a policy route and the policy route has a matching route in the FIB, then FortiGate doesn't check any of the configured SD-WAN rules or the routes in the FIB.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Policy Routes—FIB Validation




A policy route with the **Forward Traffic** action is subject to a validation against the FIB before the packet is forwarded. The goal is for FortiGate to check the configured **Destination Address**, **Outgoing interface**, and the **Gateway address** settings against the routes in the FIB, or to identify the outgoing interface or gateway to use if one of them is not specified in the policy route configuration.

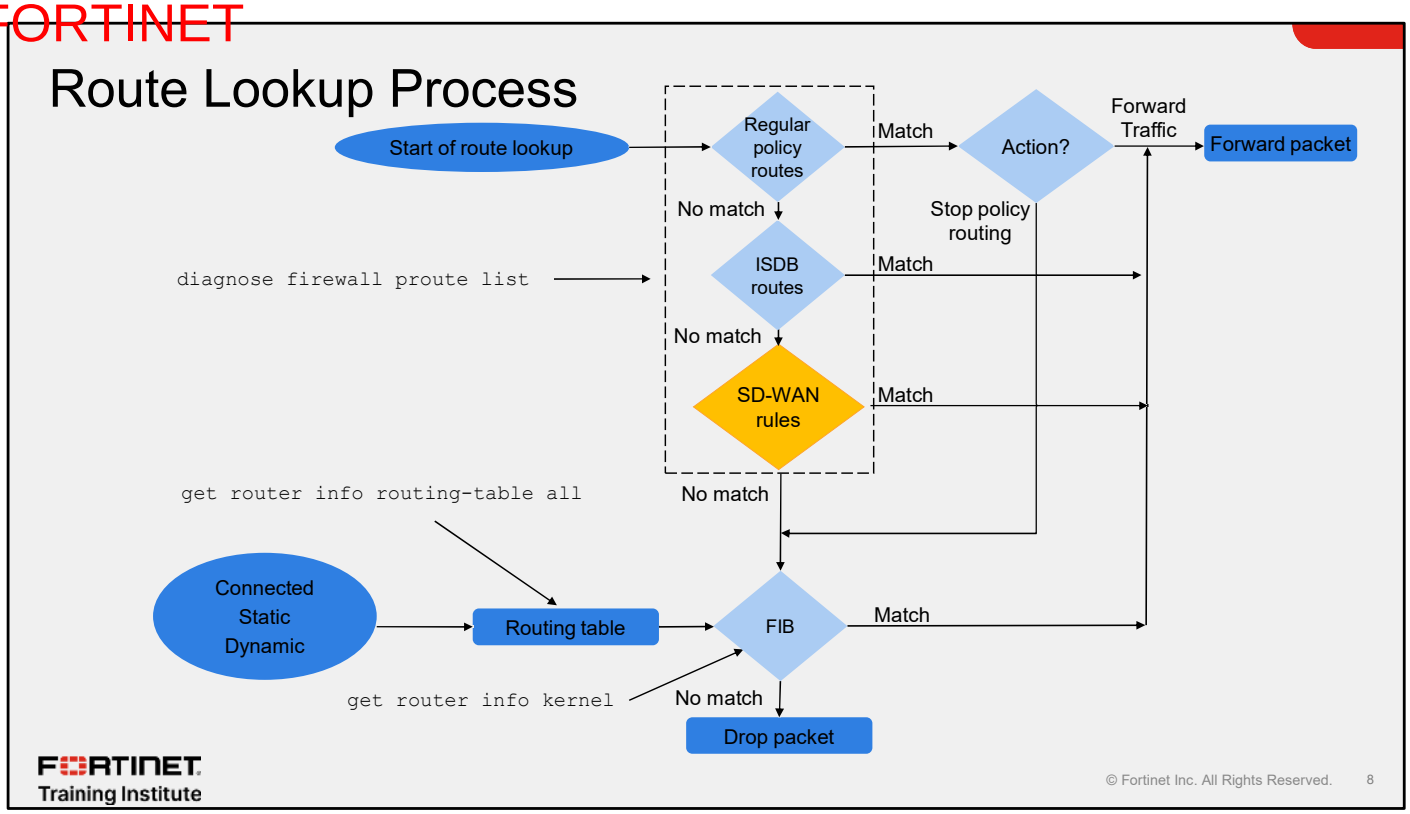
The validation is as follows:

- If you configure the outgoing interface and the gateway, FortiGate uses the policy route if the FIB contains an active route that matches the configured gateway and outgoing interface. If so, FortiGate routes the packet using the configured outgoing interface and gateway. Otherwise, FortiGate skips the policy route.
- If you configure the outgoing interface only—that is, the gateway is set to `0.0.0.0`—FortiGate uses the policy route if the FIB contains a route—any type of route—that matches the configured destination and outgoing interface. If so, FortiGate routes the packet using the outgoing interface of the policy route and the gateway of the matching route in the FIB. Otherwise, FortiGate skips the policy route.
- If you configure the gateway only, FortiGate uses the policy route if the FIB contains an active route for the configured gateway. If so, FortiGate routes the packet using the interface of the route and the configured gateway. Otherwise, FortiGate skips the policy route.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




The flowchart on this slide describes the route lookup process that FortiGate performs when it uses policy routes. Note that policy routes can be regular policy routes, internet-service database (ISDB) routes, or SD-WAN rules.

First, FortiGate checks the policy routes. The first type of policy routes to check is the regular policy routes. If there is a match, and the action is **Forward Traffic**, FortiGate routes the packet accordingly provided the policy route passes the FIB validation process. If the action is **Stop Policy Routing**, FortiGate moves on to check its FIB.

If the packet doesn't match any of the regular policy routes, FortiGate moves on to check the ISDB routes first, and then the SD-WAN rules. If the packet doesn't match any of the SD-WAN rules, FortiGate checks its FIB. You will learn more about the SD-WAN rule matching process in another lesson.

Next, FortiGate checks the FIB, which is the table used for performing standard routing. The FIB can be described as the routing table from the kernel point of view, and is built mostly out of routes in the routing table, but also from system-specific entries required by FortiOS. If the packet doesn't match any of the routes in the FIB, FortiGate drops the packet and sends an ICMP destination network unreachable message to the sender.

This slide also shows the FortiOS CLI commands you can use to display the policy routes, the routing table entries, and the FIB entries.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Policy Route Table

```
# diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=7 dport=0-65535
path(1) oif=21(HUB1-VPN3)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=18 last_used=2024-09-12 05:47:21

id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0
iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2024-09-12 06:39:07

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2) oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2024-09-12 05:46:43
```

This is a regular policy route (ID ≤ 65535)

This is an ISDB route (ID > 65535 and no `vwl_service` field)

This is an SD-WAN rule (ID > 65535 and the `vwl_service` field is present)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

FortiOS maintains a policy route table that you can view by running the `diagnose firewall proute list` command.

There are three types of policy routes displayed in the policy route table: regular policy routes, ISDB routes, and SD-WAN rules. Follow these rules to identify each type of policy route in the table:

- Regular policy routes are assigned an ID no higher than 65535. In the output shown on this slide, the first entry is assigned ID 1, which makes it a regular policy route.
- ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the `vwl_service` field, and ISDB route entries don't. The `vwl_service` field indicates the ID and the name of the rule from the SD-WAN configuration perspective. In the output shown on this slide, the second entry is an ISDB route and the third entry an SD-WAN rule.

Note that although IDs for regular policy routes are in the 1 to 65535 range, the maximum number of regular policy routes that you can configure are much lower and varies among models. For example, you can configure up to 512 regular policy routes in a FortiGate 100F device. For more information about the maximum supported values per model, refer to the `FortiOS Maximum Values Table` on `docs.fortinet.com`. Alternatively, you can run the `print tablesize` command on the FortiGate CLI to get the maximum values for your device.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Matching Policy Route in Debug Flow

- The debug flow output indicates the ID of the matching policy route:

```
branch1_fgt # id=65308 trace_id=145 func=print_pkt_detail line=5892 msg="vd-root:0 received a
packet(proto=1, 10.0.1.101:2124->10.0.2.101:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2124,
seq=1."
id=65308 trace_id=145 func=init_ip_session_common line=6073 msg="allocate a new session-00050a89,
tun_id=0.0.0.0"
id=65308 trace_id=145 func=rpdb_srv_match_input line=1043 msg="Match policy routing id=2130903043: to
10.0.2.101 via ifindex-3"
...
```

Matching policy route ID (ID based on the policy route table)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

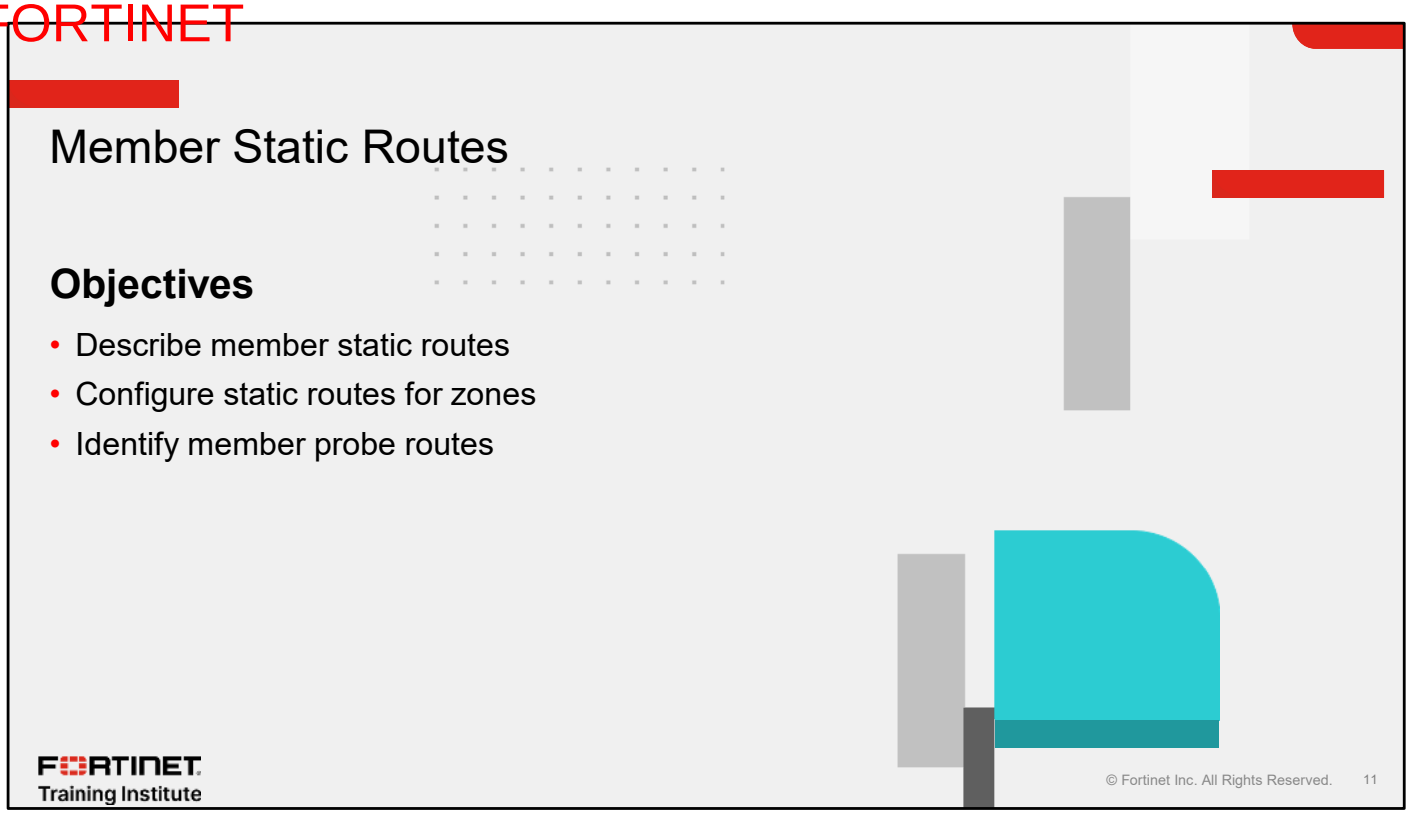
The debug flow tool indicates the ID of the matching policy route, which is useful for troubleshooting purposes. Note that the displayed ID corresponds to the entry ID in the policy route table.

You can collect the debug flow on the CLI, using the `diagnose debug flow` commands or from the FortiGate GUI menu: **Network** > **Diagnostics** > **Debug Flow**.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding static routes for SD-WAN members, you will be able to configure static routes for members based on SD-WAN requirements and limitations.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Member Routes

- FortiGate requires a valid route to steer traffic to a member
  - Best practice: Ensure that sites learn all possible routes to all possible destinations
- Static routes
  - Reference an SD-WAN zone
    - Common case, simplified configuration
    - Individual ECMP routes installed for each member in the zone
    - Gateway obtained from member configuration
  - Reference a member
    - More granular control

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

One of the key routing principles is that SD-WAN requires a valid route in the FIB so the member can be used to steer traffic. Because the goal is to have SD-WAN pick the best member to forward the traffic to, based on the SD-WAN rule criteria, it's a best practice to configure your routing setup so your SD-WAN sites know all possible routes to all possible destinations that are intended for handling by SD-WAN. Otherwise, SD-WAN may fail to choose the best member, not because it doesn't meet the application requirements, but because FortiGate doesn't have a route for the destination and member.

You can use static and dynamic routing in SD-WAN. This section focuses on static routing. When you configure static routes for SD-WAN, you usually reference an SD-WAN zone to simplify the configuration. However, you can also reference individual members instead, so you can have more granular control over traffic. When you reference a zone in a static route, FortiGate installs individual routes for each member in the zone. FortiGate then displays the individual routes in the routing table as ECMP routes.

Note that when you configure a static route that references an SD-WAN zone, you don't have to specify a gateway address because FortiGate retrieves it from the member configuration.

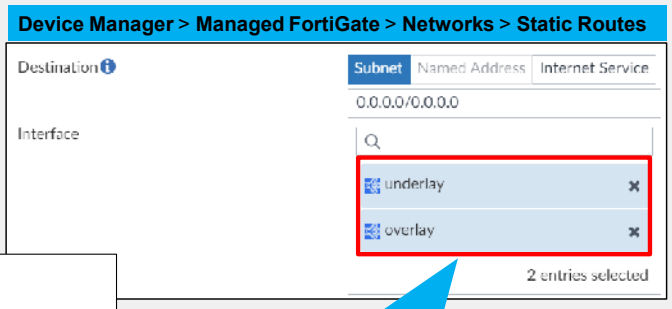


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Static Routes for SD-WAN Zones

- Reference one or more zones
- ECMP routes for each zone member
- Default distance assigned: 1
  - Higher preference over other routes
  - Can be changed




```
# diagnose sys sdwan zone
...
Zone overlay index=4
         members(1): 25(HUB1-VPN1)
Zone underlay index=3
         members(2): 3(port1) 4(port2)
...

# get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via HUB1-VPN1 tunnel 100.64.1.1, [1/0]
                  [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
...
```

Default distance: 1

Individual ECMP routes for each member in the zone

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

You can reference one or more zones when you configure a static route. As a result, FortiOS installs a static route for every member configured in the zone in the routing table. Because the static routes share the same admin distance and priority, they become ECMP routes.

When you create a static route for a zone, FortiOS assigns the routes with a distance of `1` by default. FortiOS assigns such a low distance by default because administrators usually want their SD-WAN routes to have preference over other routes in the FIB. However, you can change the distance to a different value if required.

In the example shown on this slide, `port1` and `port2` are members of the `underlay` zone, and the IPsec tunnel `HUB1-VPN1` is a member of the `overlay` zone. The administrator created a default static route that references both zones. The result is that the routing table displays ECMP routes for each of the three members.

FortiGate automatically create a default static route for each DHCP or PPoE interfaces with an admin distance of 5. With an admin distance of 1, default static routes created for DHCP or PPoE SD-WAN members takes precedence over those automatic routes.

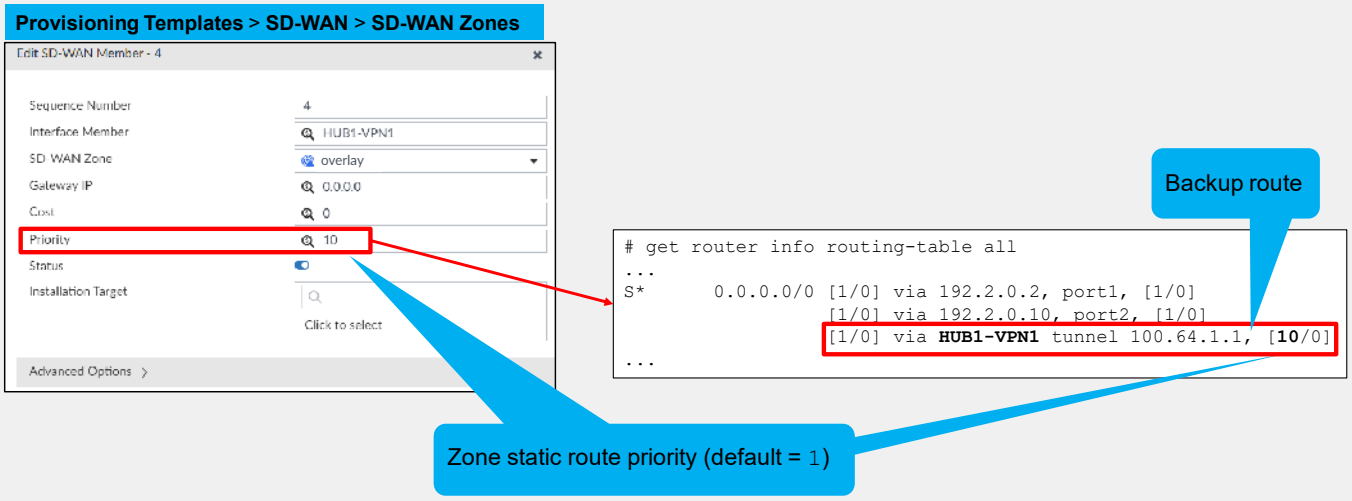


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Member Priority

- Control member preference in static routes for SD-WAN zone
- Used as tie-breaker for ECMP routes in zone (implicit SD-WAN rule)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

Traffic that doesn't match an SD-WAN rule is handled by the implicit SD-WAN rule, which means that traffic is routed based on the FIB contents. If you configure a static route for a zone, which results in ECMP routes, FortiGate load balances the connections that don't match an SD-WAN rule but match the destination of the ECMP routes, across all zone members.

In the same setup as the previous slide, internet traffic that matches the implicit rule is load balanced across underlay and overlay links. But what if, in that setup, you want FortiGate to prefer the underlay links for internet traffic to leverage the lower latency of direct internet access (DIA)? And then use the overlays only if the underlays are dead? You can achieve this behavior by increasing the priority of overlay interfaces.

By default, the member priority is set to `1`. The higher the priority number, the lower the member preference. In the example shown on this slide, the overlay `HUB1-VPN1` is assigned `10` as priority. The result is that internet traffic that doesn't match the SD-WAN rules is load balanced across `port1` and `port2`. FortiGate uses `HUB1-VPN1` to route internet traffic only if both `port1` and `port2` are dead.

Note that the member priority setting available in the SD-WAN configuration applies only to *zone static routes*. The priority of per-member static routes is controlled by the priority setting available in the static route configuration.



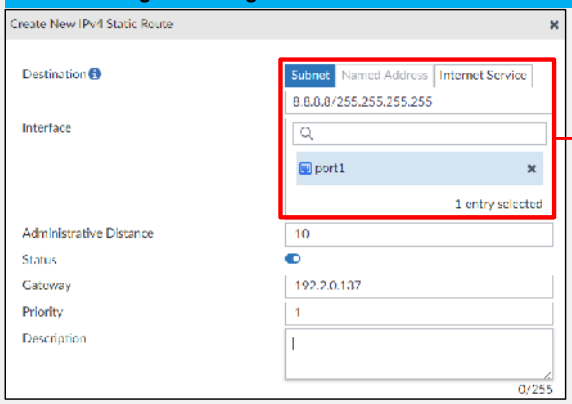
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Static Routes for Members

- Configure per-member static routes
  - More granularity
- Gateway setting may be required
  - Gateway is not retrieved from member settings

**Device Manager > Managed FortiGate > Network > Static Routes**




```
# get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
                  [1/0] via HUB1-VPN1 tunnel 100.64.1.1, [10/0]
S       8.8.8.8/32 [10/0] via 192.2.0.137, port1, [1/0]
...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

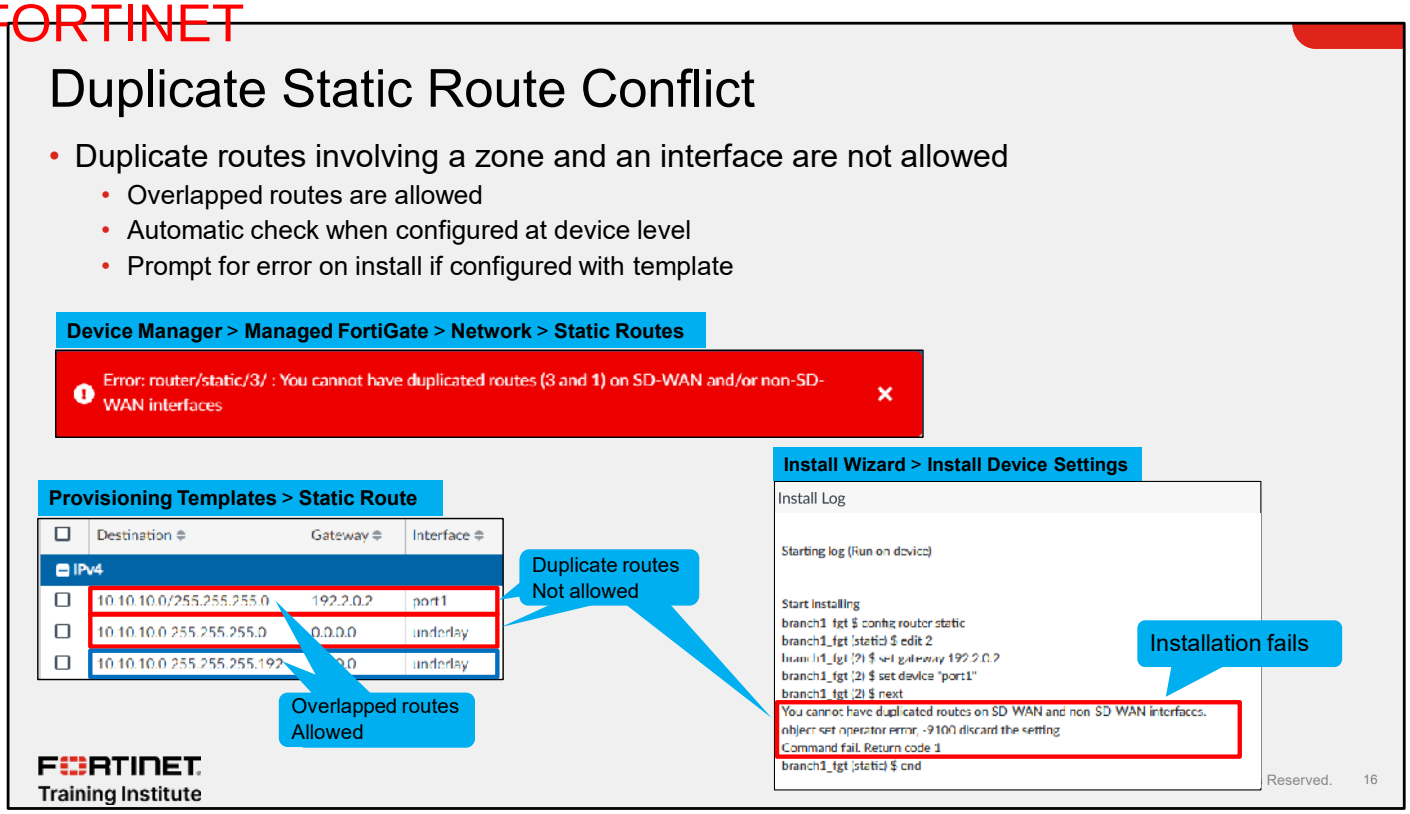
Alternatively, you can configure per-member static routes for more granular control over traffic. However, unlike static routes for zones, which retrieve the member gateway from the member configuration, with per-member static routes, you must specify a gateway if the interface type requires it.

In the example shown on this slide, the administrator configured a per-member static route for `8.8.8.8` through **port1**. The route can then be used by SD-WAN rules to route traffic, or by the FIB to route traffic when no rule is matched.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



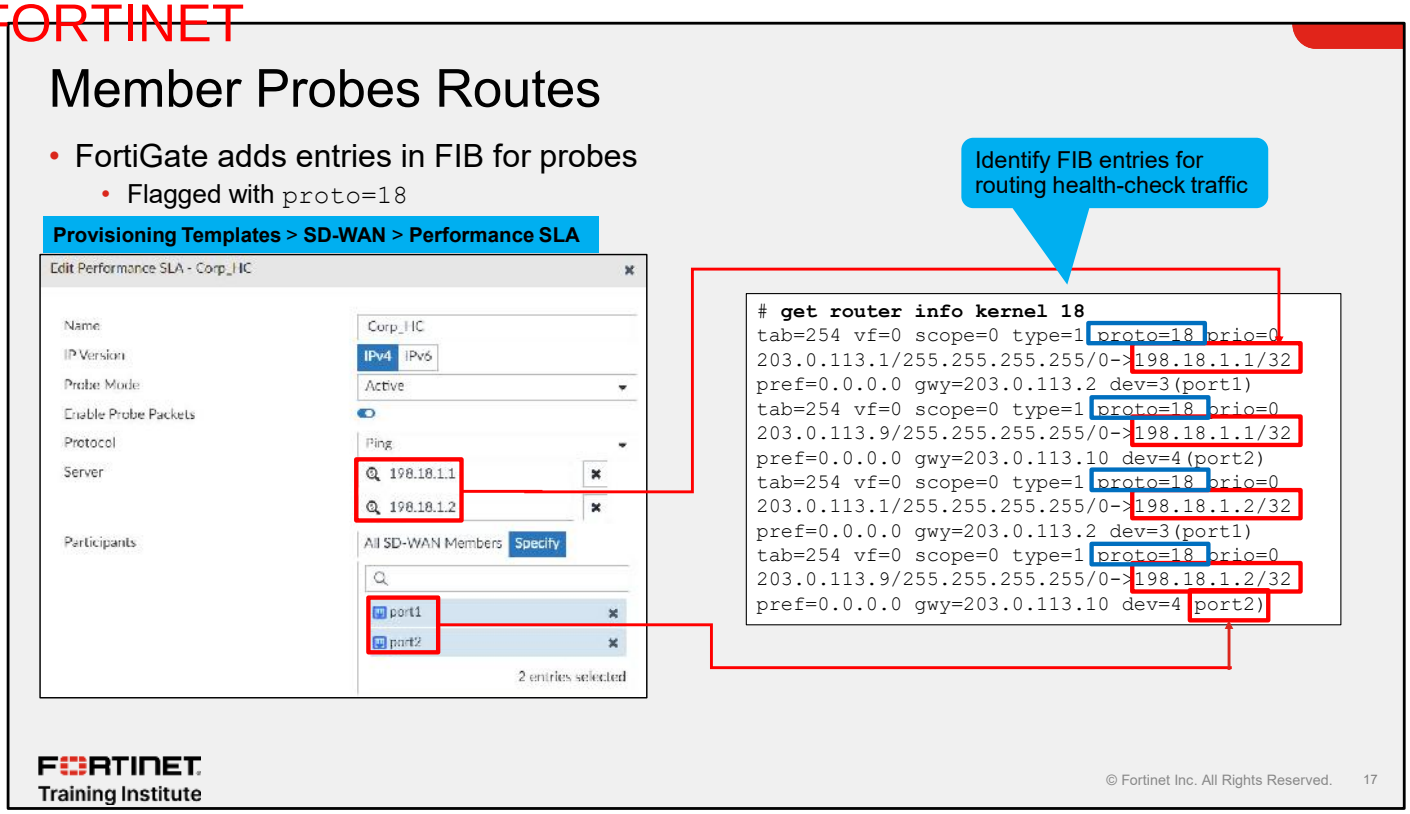

If you configure a static route for a destination that references a zone, FortiOS doesn't allow you to configure a static route for the same destination that references an interface. In SD-WAN, these routes are known as duplicate routes. You can, however, configure overlapping routes for zones and interfaces. For example, you can configure a route `10.10.10.0/24` through port1 and the overlap route `10.10.10.0/26` through the SD-WAN zone underlay.

In the example shown on this slide, the administrator tries to configure a default static route for **port1** on FortiManager at the device level. However, because there is already a default static route configured for the **underlay** and **overlay** zones, FortiManager rejects the second route configuration and displays an error message. If a similar configuration is done at the template level, FortiManager detects the conflict during device settings installation, and the install log reports an error indicating that such configuration is not allowed. As a result, the installation fails.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




When you use active monitoring for measuring the performance of members, FortiGate doesn't use the entries in the routing table to route the probes. Instead, FortiGate adds a FIB route entry for the configured target servers through each monitoring member and its gateway. These kernel routes are flagged as `proto=18`, as shown on this slide.

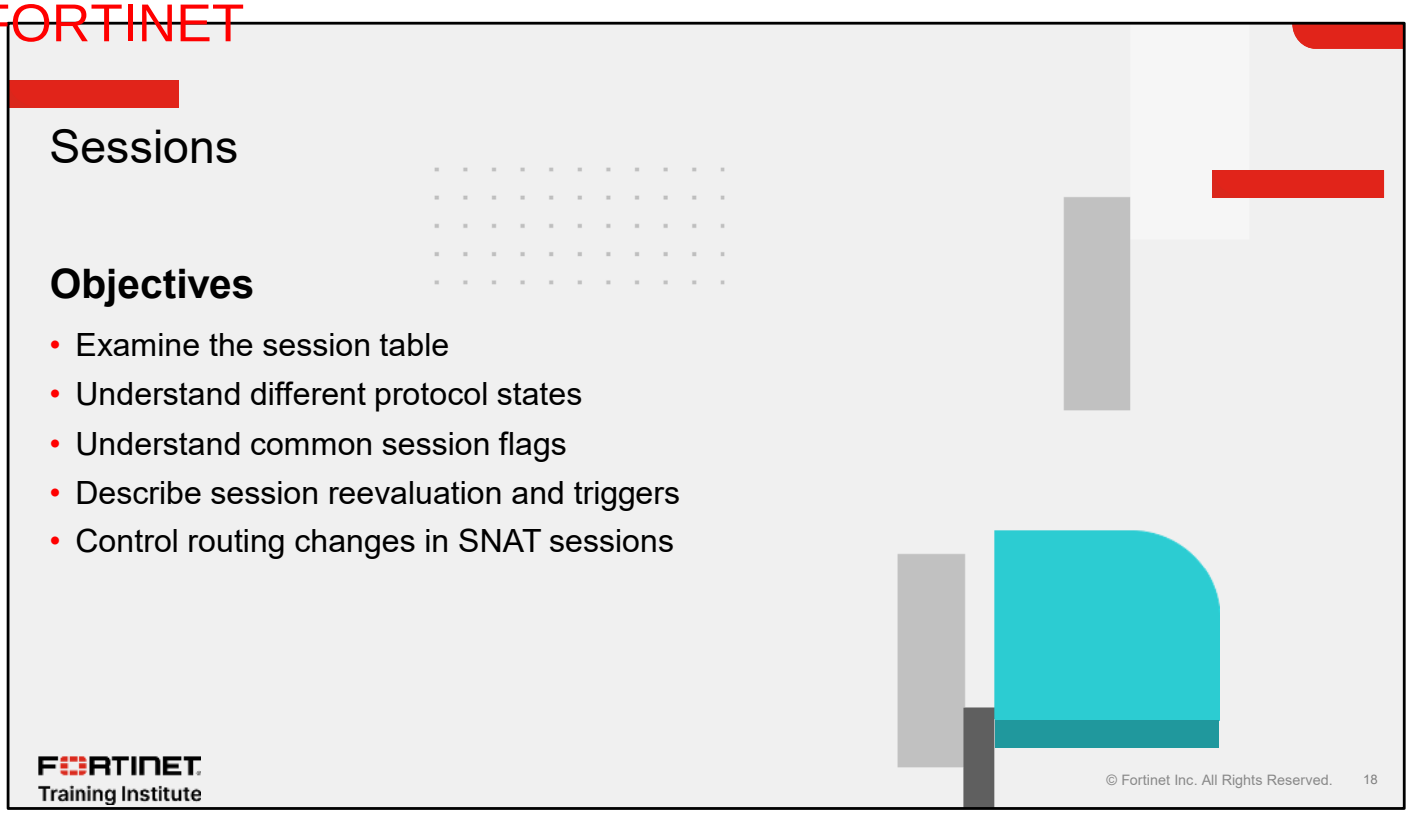
Note that `proto=18` has nothing to do with assigned internet protocol numbers. It is an arbitrary protocol number assigned by Fortinet to identify entries in the FIB used for routing health-check traffic.

You can use the command `get router info kernel 18` to filter the kernel table route and display only the proto 18 routes. It is equivalent to the command `get router info kernel | grep proto=18`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding FortiOS sessions, you will be able to identify relevant SD-WAN fields in a session, factors that trigger a session reevaluation, and settings that enable you to change the default behavior.

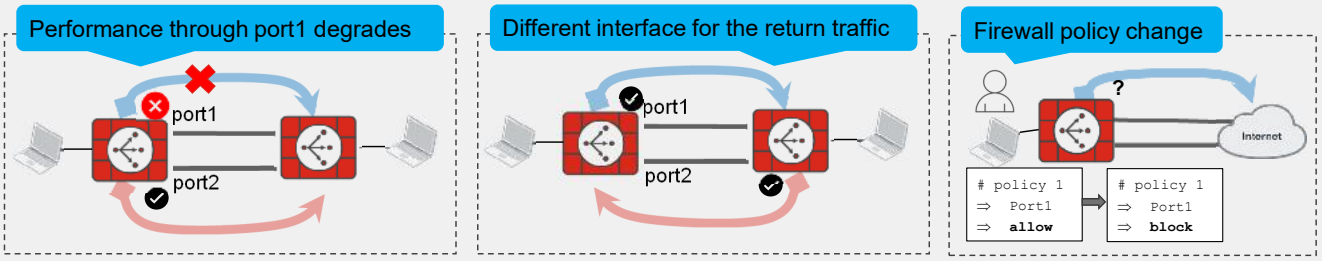


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN and Sessions on FortiGate

- By default, FortiGate steers each packet of a traffic flow—a session—through the same interface
- How does FortiGate handle the following situations:
  - Due to link performance degradation, the preferred member for an SD-WAN rule changes
  - FortiGate receives the return traffic for a session through an interface that is different from the one used to steer the outgoing packets
  - The administrator adjusts the firewall policy configuration while traffic flows through the device
- FortiGate session behavior applies
- Administrators can use FortiGate tools to refine the session behavior




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

FortiGate is a stateful firewall and handles traffic per session. This behavior remains true when FortiGate use SD-WAN to steer the traffic. Consequently, by default, FortiGate steers each packet of a traffic flow—a session—through the same interface.

The general rule is that a single interface is used for a traffic flow. But, how does FortiGate handle situations such as the following:

- The performance of the link used to steer the traffic degrades and the preferred member for the SD-WAN rule changes.
- FortiGate receives the return traffic for a session through an interface that is different from the one used to steer the outgoing packets.
- The administrator adjusts the firewall policy configuration while traffic flows through the device and the flow is no longer allowed by the updated policy.

For all of these situations, FortiGate reevaluates the session to reflect the changes. The administrator can refine the configuration to define precisely how FortiGate acts. In this lesson, you will learn about some of the tools used to refine the configuration. Note that you can use these tools any time you need to refine how FortiGate handles changes that impact sessions. Though not exclusively, you will use them frequently with SD-WAN, because the dynamic nature of SD-WAN triggers more frequent routing changes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Sessions—Table Summary

```
# get system session status
The total number of IPv4 sessions for the current VDOM: 11

# get system session list
PROTO    EXPIRE SOURCE           SOURCE-NAT       DESTINATION      DESTINATION-NAT
tcp      3522   10.1.10.1:41418  100.64.1.1:41418 172.217.0.106:443        -
udp      151    10.1.0.1:4387    100.64.1.1:64803 208.91.112.220:53        -
udp      28     10.1.0.1:1687    100.64.1.1:62103 208.91.112.52:53         -
udp      61     100.64.1.1:3075  -                208.91.112.53:53-
udp      55     100.64.1.1:3075  -                208.91.112.52:53         -
udp      172    10.1.10.1:123    100.64.1.1:60539 209.121.129.48:123       -
udp      152    10.1.0.1:4387    100.64.1.1:64803 173.243.138.221:53       -
udp      152    10.1.0.1:4387    100.64.1.1:64803 45.75.200.89:53          -
udp      171    10.1.10.1:123    100.64.1.1:60539 208.81.1.197:123         -
udp      104    10.1.0.1:1420    -                10.1.0.254:53            -
tcp      3600   10.1.10.1:34433  -                10.1.0.254:22            -
udp      176    10.1.0.1:1900    -                10.1.0.254:53            -
tcp      3524   10.1.10.1:59972  100.64.1.1:59972 172.217.0.110:80         -
tcp      119    10.1.10.1:42824  100.64.1.1:42824 72.21.91.29:80           -
tcp      3517   10.1.10.1:42816  100.64.1.1:42816 72.21.91.29:80           -
udp      171    10.1.10.1:123    100.64.1.1:60539 144.217.65.184:123       -
udp      175    10.1.10.1:123    100.64.1.1:60539 144.217.65.182:123       -
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

The FortiGate session table contains detailed information about every IP connection that crosses, terminates, or is initiated by FortiGate. The command `get system session status` displays the total number of sessions in the current VDOM. The command `get system session list` provides a brief summary of each session. This command lists one session per line, and includes information such as protocol, source IP address, destination IP address, and port. You can use the `grep` utility to filter the output.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Sessions—TCP Example

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=1 expire=3599 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 app valid
statistic(bytes/packets/allow_err): org=1720/9/1 reply=10804/13/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->31/31->7 gwy=10.1.0.254/10.9.31.117
hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)
hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)
hook=post dir=reply act=noop 200.8.57.5:443->10.9.31.117:45388(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88,
vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

Session flags

SD-WAN session information

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

This slide shows an example output detailing information particular to a single session table entry. The command `diagnose sys session list` which provides this output is extensively used for troubleshooting purposes. It provides detailed information about SD-WAN sessions and much more.

From left to right, and from top to bottom, the following information is highlighted:

- The IP protocol number and the protocol state
- The length of time until the session expires (if no more traffic matches the session)
- Session flags
- Received and transmitted packet and byte counters
- The original and reply direction of the traffic. If the device is doing network address translation (NAT), this portion shows the type of NAT (source or destination) for each traffic direction, and the NAT IP address.
- The ID of the matching policy
- The SD-WAN specific session information. `sdwan_mbr_seq` and `sdwan_service_id` indicate the SD-WAN member ID and the SD-WAN rule ID in use, respectively. If the session matched the SD-WAN implicit rule, and therefore was handled using standard FIB routing, these SD-WAN fields do not appear.

Use the CLI command `diagnose sys session list` for IPv4 traffic, and the command `diagnose sys session6 list` for IPv6 traffic.
The output for both commands is similar (it displays the same fields, in the same order).



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## May_Dirty Sessions

- New firewall sessions created after matching a firewall policy with `accept` action
  - A firewall policy lookup is done (top-down)
  - Flagged as `may_dirty`
- Lookup process
  - First original packet (route and firewall policy lookup)
  - First reply packet (route lookup only)
  - No additional lookups unless session is flagged as `dirty`

```
# diagnose sys session list
session info: proto=17 proto_state=01 duration=6 expire=173 timeout=0 […]
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/0
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=124/2/1 reply=226/2/1 tuples=3
tx speed(Bps/kbps): 18/0 rx speed(Bps/kbps): 33/0
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

When working with FortiGate, especially with SD-WAN setups, it's important to understand the concept of may_dirty and dirty sessions.

May_dirty sessions are firewall sessions that were created after matching a firewall policy with `accept` as action. For FortiGate to identify the matching policy, it performs a firewall policy lookup, selecting the first matching policy in the configuration from the top down. Most firewall sessions contain the `may_dirty` flag. However, some sessions such as expectation sessions, do not contain the `may_dirty` flag because they are not created as a result of matching a firewall policy.

For new sessions, FortiGate performs route and firewall policy lookups upon receiving the first packet (in the original direction). FortiGate also performs a route lookup—but not a firewall policy lookup—for the first reply packet. FortiGate then saves the information that results from the route lookup—the outgoing interface and gateway to use—and the firewall policy lookup—policy ID, address translation, inspection, authentication, logging, and so on—to the session.

FortiGate doesn't perform additional lookups for the session unless the session is flagged as `dirty`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Dirty Sessions

- A session is flagged as `dirty` after a routing, firewall policy, or interface change
  - Each direction of a dirty session must be reevaluated
  - Routing changes are common in SD-WAN
  - Session routing information is flushed (routing change)
- Default reevaluation process after a routing change (*no SNAT*):
  - Next packet in each direction goes to the CPU (applies only to NPU-offloaded sessions)
  - Original direction: Route and firewall policy lookups for first packet
  - Reply direction: Only route lookup for first packet
  - FortiGate updates the session with new routing and firewall policy information, and removes the `dirty` flag
  - If the action is still `accept`, FortiGate forwards the packet
  - If the new action of the matching firewall is `deny`, then:
    - FortiGate flags the session as `block`, and drops the packet
    - The session remains in the session table until it expires
    - FortiGate drops further packets matching the session
  - FortiGate eventually offloads sessions again to hardware

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

By default, FortiGate flags all `may_dirty` sessions as `dirty` if there is a routing, firewall policy, interface, or recognized application change. The FortiGate must reevaluate every dirty session. During reevaluation, it checks both directions of the dirty session.

Dirty sessions are common in SD-WAN because of its dynamic nature. Members that are down or performing poorly may change the entries in the FIB and policy route table, respectively. In either case, the result is a routing change that may affect multiple SD-WAN sessions.

After a routing change, the routing information of `may_dirty` sessions is flushed. The default reevaluation process following a routing change for sessions *without* source NAT (SNAT) is as follows:

- If the impacted session is offloaded to the NPU, FortiGate instructs the NPU to send the next packet from each direction of the session to the CPU. This ensures that the session is handled by the CPU, and thus reevaluated. If the session is not offloaded to the NPU, then the packets are always handled by the CPU, and this step is not required.
- In the original direction, FortiGate performs route and firewall policy lookups for the first packet.
- In the reply direction, FortiGate performs only a route lookup for the first packet.
- FortiGate updates the session with the new routing and firewall policy information, and removes the `dirty` flag.
- If the matching firewall policy action is still `accept`, FortiGate forwards the packet.
- If the matching firewall policy action is `deny`, FortiGate flags the session as `block`, drops the packet, and retains the session in the session table until it expires. FortiGate also drops any additional packets that match the session.
- FortiGate eventually offloads allowed sessions again to the NPU, if they still meet the NPU offloading requirements.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Dirty Sessions (Contd)

- Before the route change (`may_dirty` flag)

```
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
state=log may dirty npu f00
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101
misc=0 policy id=3 auth_info=0 chk_client_info=0 vd=0
sdwan_mbr_seq=3 sdwan_service_id=2
```

- After the route change (`dirty` flag; gateway is flushed)

```
session info: proto=1 proto_state=00 duration=30 expire=29 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
state=log dirty may_dirty npu f00
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=0.0.0.0/0.0.0.0
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
sdwan_mbr_seq=3 sdwan_service_id=2
```

- After reevaluation (no `dirty` flag; outgoing interface, gateway, and SD-WAN member updated)

```
session info: proto=1 proto_state=00 duration=53 expire=56 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
state=log may_dirty npu f00
orgin->sink: org pre->post, reply pre->post dev=7->20/20->7 gwy=100.64.1.9/10.0.1.101
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
sdwan_mbr_seq=4 sdwan_service_id=2
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

This slide shows the transition of an ICMP session from `may_dirty` to `dirty`, and then back to `may_dirty`, following a route change. Note that only relevant lines of the session are displayed.

Before the route change, the session is flagged as `may_dirty`. The session output shows the index number of the outgoing interface in use (`19`), the gateway information (`gwy`), and the configuration index number of the SD-WAN member in use (`3`).

After the route change, the session is flagged as `dirty`. Note that the `may_dirty` flag is still there, and the `dirty` flag is just added. The gateway information is also flushed.

After reevaluation, the `dirty` flag is removed, and the index number of the outgoing interface and the gateway information are updated based on the new route. Because the outgoing interface changed, the configuration index number of the SD-WAN member also changed.

Note that the firewall policy (`policy_id`) didn't change. This is because the firewall policy lookup during reevaluation resulted in the same firewall policy, but this is not always the case.

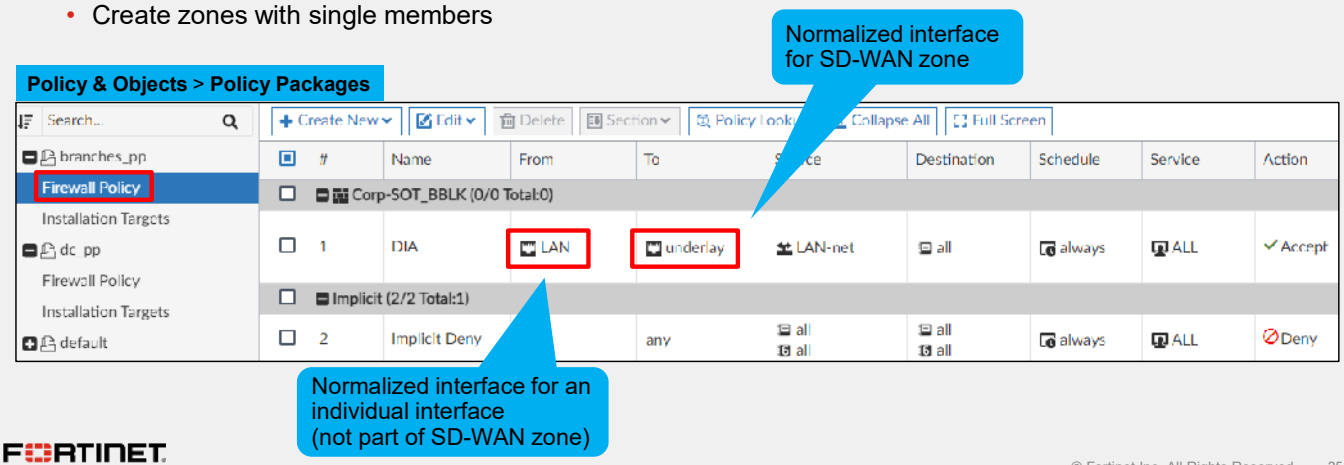


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Firewall Policies

- Steered traffic must be allowed by a firewall policy
- Reference normalized interface for SD-WAN zones only
  - Simplified configuration
- Can't reference a member directly
  - Create zones with single members




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

You configure SD-WAN firewall policies in the same way as regular firewall policies, except that, when selecting an outgoing or incoming interface, you must reference a normalized interface that refer to an SD-WAN zone—or for configuration done on the FortiGate device, an SD-WAN zone. When you reference a zone, you simplify the configuration by avoiding duplicate firewall policies.

You may need to reference a member in your firewall policy because you want to apply different action on the traffic flowing through that member, such as applying different security profiles and NAT settings. Because you can't reference members in a firewall policy, a workaround is to place a single member in a separate zone, and then reference that zone in the firewall policy.

The example on this slide shows a firewall policy named **DIA** that references the **underlay** zone, which contains port1 and port2 as members. As a result, DIA traffic steered over port1 or port2 is allowed by FortiGate provided it matches the firewall policy criteria, and it passes the security inspection configured on the policy.

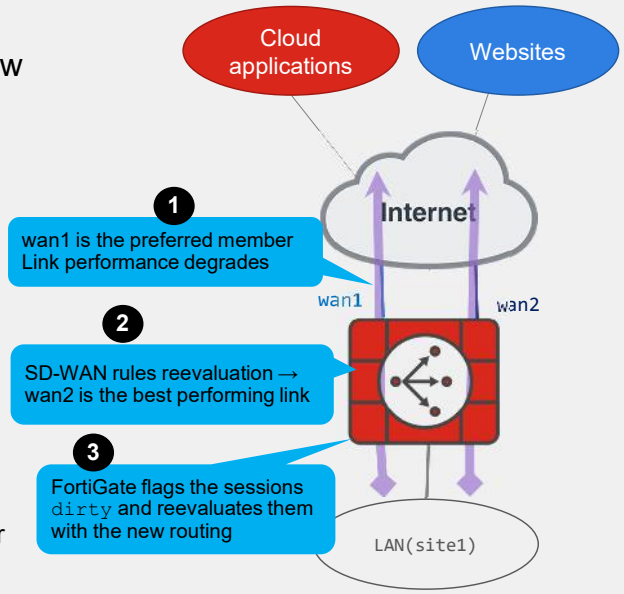


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Session Reevaluation

- FortiGate creates a session for each traffic flow allowed by a firewall policy
  - FortiGate flag these sessions with `may_dirty`
- Which events trigger session reevalutation?
  - Firewall policy change
  - Routing change
  - Network related configuration change
- For which session?
  - Any session flagged as `may_dirty`
- How does session reevaluation affect SD-WAN?
  - SD-WAN can trigger frequent route reevaluation
  - Best quality and lowest cost (SLA) strategies trigger routing changes when link performances changes




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

When FortiGate receives the first packet of a new session—for example, a SYN packet—it evaluates if the traffic should be allowed based on the firewall policies. FortiGate performs route and firewall policy lookups for new sessions when it receives the first packet (original direction). FortiGate also performs a route lookup, but not a firewall policy lookup, for the first reply packet. With the information it collected during the route and firewall policy lookup, FortiGate creates a session entry. Each session entry contains the incoming and outgoing interface, the gateway to use, the ID of the firewall policy that allows the flow, and, when applicable, NAT and SNAT address translation, authentication, and so on.

While handling subsequent packets related to the same traffic flow, FortiGate does not perform additional route or firewall lookups, unless the session is flagged as `dirty`.

FortiGate adds the flag `dirty` to any session that has the flag `may_dirty`, if one of the following events occurs:

- A configuration change affects the firewall policy configuration.
- A routing change occurs—it can be a dynamic routing change or a configuration change that affects the routing.
- A configuration change affects the network-related configuration.

FortiGate uses the first packets in each direction to reevaluates the sessions flagged `dirty`, and then removes the `dirty` flag.

SD-WAN dynamically adjusts the routing to the link performance when the administrator configured rules with the best quality or lowest cost (SLA) strategy. This allows FortiGate to steer the traffic to the best performing link, but consequently, this can also trigger frequent session reevaluation.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Limit the Session Reevaluation

- Session reevalutation can lead to high CPU utilization
- Select which sessions in the VDOM are flagged as `dirty` (default = `check-all`):

```
VDOM level
config system settings
    set firewall-session-dirty < check-all | check-new | check-policy-option >
end
```

  - `check-all`: All sessions are flagged as dirty
  - `check-new`: New sessions are flagged as dirty and existing sessions are not affected.
  - `check-policy-option`: Follow firewall policy-level configuration
- Firewall policy-level configuration (default = `check-all`):

```
Policy Level
config firewall policy
    edit <id>
        set firewall-session-dirty < check-all | check-new >
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

When FortiGate needs to reevaluate a session, it flags the session as `dirty`, and at the same time, it moves offloaded sessions back to the CPU. FortiGate then performs a firewall policy lookup for the first packet received for each existing session. It updates session table entry and resets the flag to `may_dirty`, and if applicable offloads the session. Then, it processes the next packets based on the new firewall settings.

Note that offloaded sessions are handled by the CPU for the packets received while in the `dirty` state.

If the firewall handles a huge number of sessions, flagging all sessions as `dirty` and performing a firewall policy lookup for the sessions, may result in high CPU utilization. To prevent this, you can configure FortiGate to flag only new sessions as `dirty` by setting `firewall-session-dirty` to `check-new`. The result is that FortiGate evaluates only new sessions against the new firewall policy configuration.

The `firewall-session-dirty` setting is available on the VDOM and firewall policy levels. It is set to `check-all` by default, which instructs FortiGate to flag all sessions as `dirty`. To instruct FortiGate to follow the firewall policy-level setting, you must set the VDOM-level setting to `check-policy-option`. Note that the firewall policy-level setting is available only if the VDOM-level setting is set to `check-policy-option`.

Though not specific to SD-WAN configurations, these parameters can help you limit the CPU spikes caused by routing and firewall policy changes on any FortiGate device that handles a high number of sessions.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Limit the Sessions Reevaluation (Contd)

- Session is flagged as `persistent`

```
config system settings
    set firewall-session-dirty check-new
end

# diagnose sys session list
session info: proto=6 proto_state=01 duration=3 expire=3598 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
[...]
state=log npu f00 persistent
statistic(bytes/packets/allow_err): org=3369/19/1 reply=3797/17/1 tuples=2
tx speed(Bps/kbps): 1011/8 rx speed(Bps/kbps): 1140/9
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101
hook=pre dir=org act=noop 10.0.1.101:47774->10.1.0.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.7:22->10.0.1.101:47774(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
[...]
```

persistent flag
No may_dirty flag

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

This slide shows the details of an established SSH session when `firewall-session-dirty` is set to `check-new`.

Note the presence of the `persistent` flag in the session, and the absence of the `may_dirty` flag, which indicates that FortiGate does not perform a new firewall policy lookup if there is a configuration change.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Routing Changes and SNAT Sessions

- By default, SNAT sessions are not flagged as `dirty` after a routing change
  - Exception: The route in use is removed from FIB
- Force reevaluation of SNAT sessions after a routing change (default = `disable`):

```
config system global
    set snat-route-change < enable | disable >
end
```

- If SNAT IP changes during reevaluation, packet is dropped, and session is cleared

```
id=20085 trace_id=51 func=print_pkt_detail line=5746 msg="vd-root:0 received a packet(proto=1, 10.0.1.101:13106->8.8.8.8:2048) from port5. type=8, code=0, id=13106, seq=3."
id=20085 trace_id=51 func=resolve_ip_tuple_fast line=5827 msg="Find an existing session, id-00008483, original direction"
id=20085 trace_id=51 func=vf_ip_route_input_common line=2589 msg="Match policy routing id=2131230721: to 8.8.8.8 via ifindex-4"
id=20085 trace_id=51 func=vf_ip_route_input_common line=2615 msg="find a route: flag=04000000 gw-192.2.0.10 via port2"
id=20085 trace_id=51 func=get_new_addr line=1229 msg="find SNAT: IP-192.2.0.9(from IPPOOL), port-13106"
id=20085 trace_id=51 func=fw_strict_dirty_session_check line=264 msg="SNAT IP 192.2.0.1 != 192.2.0.9, drop"
```

Different SNAT IP; drop the packet and clear the session

- Enable `snat-route-change` if using the same IP address pool for the old and new paths

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

By default, SNAT sessions are not flagged as `dirty` following a routing change that impacts the session. This is true if the route in use is still in the FIB. However, if the route is removed from the FIB, then FortiGate flags the session as dirty, flushes the outgoing interface and gateway information, and reevaluates the session on the next packet received.

To force the reevaluation of SNAT sessions following a related routing change, regardless of whether the route in use is still in the FIB or not, enable the `snat-route-change` setting, as shown on this slide.

Note that during reevaluation of SNAT sessions, if the new route and firewall policy lookup results in a change of the SNAT IP, then FortiGate drops the packet and clears the session. This means that the impacted application could have to initiate a new connection to resume network connectivity, especially if the application is TCP-based.

This slide shows the debug flow output for a SNAT session during reevaluation. Because the SNAT IP of the new path (`192.2.0.9`) is different from the SNAT IP of the current path (`192.2.0.1`), FortiGate drops the packet and clears the session. This also means that, from a connectivity point of view, it makes sense to enable `snat-route-change` only when the new path for the session uses the same SNAT IP, which can be achieved using IP pools.



Vouchers & Dumps are Available | WhatsApp +201224560923

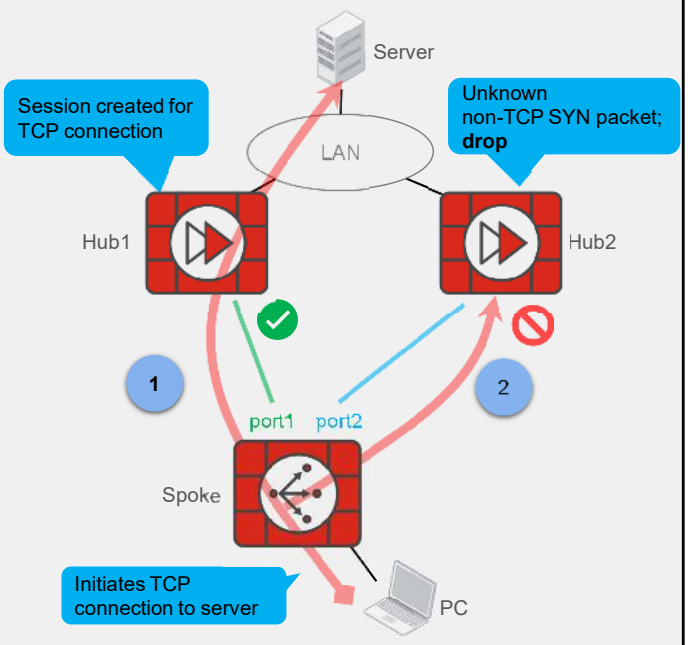
DO NOT REPRINT Brave-dumps.com
© FORTINET

## Interface Stickiness

- Force *established* sessions to keep using outgoing interface and gateway after a route change:

```
config system interface
    edit <interface>
        set preserve-session-route enable
    next
end
```

- Current route must still be present in FIB
  - Otherwise FortiGate flags the session as dirty and reevaluates it
- Not specific to SD-WAN
  - Applies to all sessions through the interface




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

The reevaluation of a dirty session following a route change may result in a failover to another SD-WAN member. If the SD-WAN members are connected to different devices, especially a stateful firewall, it can cause interruption of TCP sessions.

To avoid a route change, when current route is still available but no longer the best route, you can enable the interface-level command shown on this slide. It forces the session to stay on the same SD-WAN member, provided the route in use by the session is still present in the FIB.

However, if the route is removed from the FIB, then FortiGate must flag the session as `dirty`, flush its gateway information, and reevaluate the session.

In the topology shown on this slide, if FortiGate establishes the session through port1, but due to SLA changes, the best route is now through port2, the behavior is as follows:

- With `preserve-session-route` set to `disable` on port1, FortiGate reevaluates the session, and redirects the traffic through port2. Hub2 drops any existing TCP sessions.
- With `preserve-session-route` set to `enable` on port1, FortiGate does not reevaluate the session, and the session remains established through port1 and hub1. Active TCP sessions do not change. FortiGate routes new sessions through port2.

You can configure this setting with the CLI command as shown or this slide, or in the FortiManager GUI, enable the parameter **preserve-session-route** at the interface **Advanced Options** level.

Note that this parameter is interface specific, the administrator can enable it for some interfaces of an SD-WAN zone and not for others. For example, you can decide preserve the sessions when the traffic flows through your main ISP link WAN1 and not when it flows through your backup satellite link WAN2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Interface Stickiness (Contd)

- Session is flagged as `route_preserve`

```
config system interface
    edit "HUB1-VPN1"
        set preserve-session-route enable
    next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 flags=00000000 socktype=0 sockport=0
av idx=0 use=3
state=log may dirty npu f00 route preserve
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101
sdwan_mbr_seq=3 sdwan_service_id=2

# diagnose netlink interface list | grep index=19
if=HUB1-VPN1 family=00 type=768 index=19 mtu=1420 link=0 master=0

# diagnose sys sdwan member | grep (3)
Member(3): interface: HUB1-VPN1, flags=0x4 , gateway: 100.64.1.1, priority: 0 1024, weight: 0
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

This slide shows the details of an ICMP session established through an interface (`HUB1-VPN1`) that has the setting `preserve-session-route` enabled. Note that only relevant lines of the session are displayed.

Also note the presence of the `route_preserve` flag in the session. You can find out the interface name and SD-WAN member ID by using the `diagnose netlink interface list` and `diagnose sys sdwan member` commands, respectively.

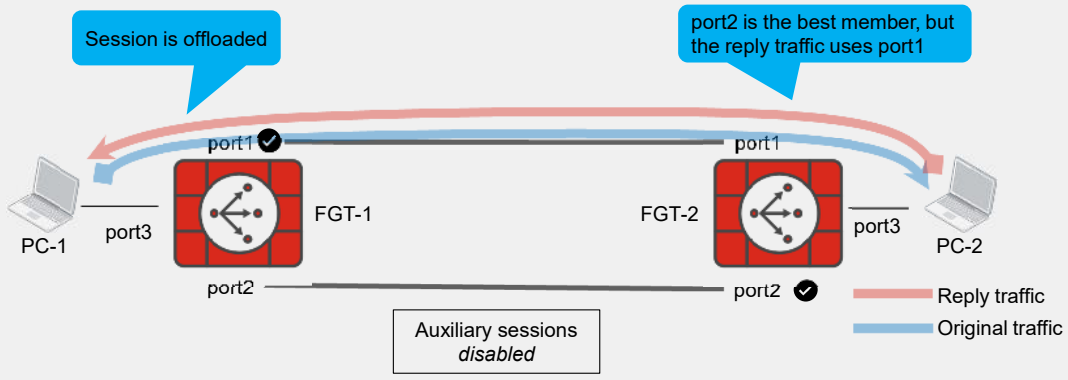


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Auxiliary Sessions

- Dirty sessions are also triggered by a change in the reply traffic interface
  - Sessions handled by system CPU (no hardware offload)
- By default, route lookup for reply traffic considers routes over the original ingress interface only
  - Reply traffic can't be routed over another member with better performance




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

Dirty sessions are also a result of a change in the reply traffic interface. This change is often seen in SD-WAN because a site may switch to a better performing link at any time, which could result in a change in the reply traffic interface for a session. By default, the system CPU handles dirty sessions that are triggered by reply interface changes. Therefore, in this case, hardware offloading is not used. For this reason, a huge amount of traffic handled by these dirty sessions may result in high CPU utilization and poor performance.

In addition, by default, when performing route lookups for the reply direction, FortiGate considers only routes through the same ingress interface used in the original direction. This is done to preserve session symmetry. However, this also prevents reply traffic from switching to a better performing member, which can impact some sensitive applications, such as voice and video.

Auxiliary sessions solve the two previous issues by enabling FortiGate to:

1. Offload asymmetric sessions to hardware by creating an auxiliary session (also known as a reflect session). Symmetric traffic matches the main session and asymmetric traffic matches the auxiliary session. Both sessions can be offloaded to hardware. For FortiGate VMs, although hardware offload does not apply, performance is improved because FortiGate does not have to reevaluate the asymmetric traffic.
2. Select the best route for reply traffic through any member, not necessarily the same interface where the original incoming traffic was received.

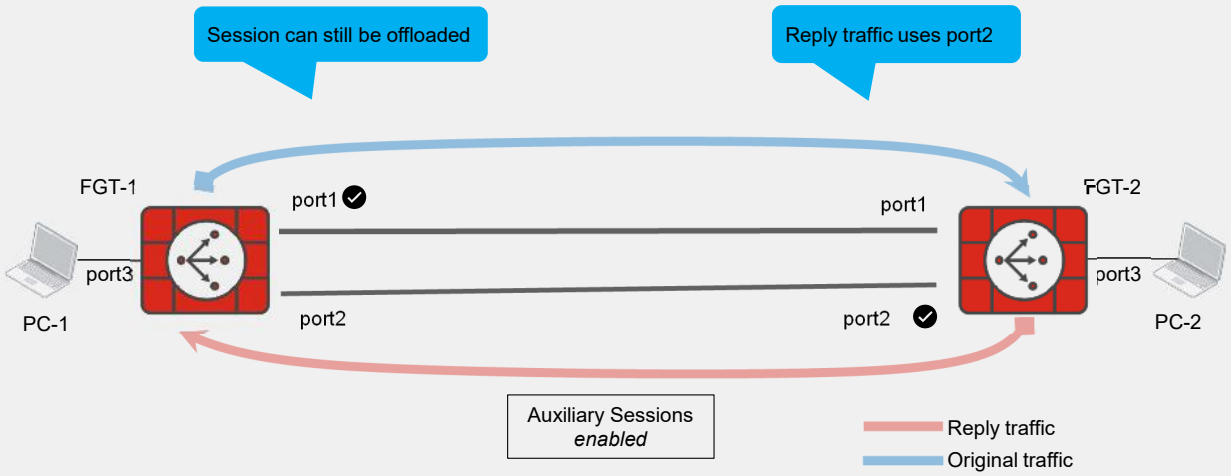
This slide shows two FortiGate devices with **auxiliary sessions disabled** and that are connected over two links. PC-1 initiates a connection to PC-2, and FGT-1 routes the connection over port1 because it's the best port. On FGT-2, the best port is port2. However, when FGT-2 performs a route lookup for the reply traffic, it selects the route over port1 because port1 is the incoming interface in the original direction. Also, both FortiGate devices can offload the session to hardware because the session is symmetric.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Auxiliary Sessions (Contd)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

If you enable auxiliary sessions on both FortiGate devices in the previous topology, FGT-2 can now route the reply traffic through the best performing member, which is port2. FGT-1 can continue to offload the asymmetric traffic because it matches the auxiliary session (or reflect session). If you don't enable auxiliary sessions on FGT-1, FGT-1 uses the system CPU to handle the asymmetric traffic.

Note that the auxiliary session parameter is not limited to FortiGate devices with SD-WAN. You can enable the feature on any FortiGate device that can benefit from reply traffic received on a different interface. It can be temporary, because of asymmetric routing during a migration, or it can be permanent, due to specific topologies conditions.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Auxiliary Sessions (Contd)

- Enable auxiliary sessions per VDOM on the FortiGate CLI (default = `disable`):

```
config system settings
    set auxiliary-session enable
end
```

- Debug flow sample for auxiliary session (FGT-1):

```
trace_id=51 func=print_pkt_detail line=5746 msg="vd-root:0 received a packet(proto=6, 10.0.1.7:22->10.9.31.160:7932) from port2. flag [.], seq 453029597, ack 2210383401, win 11"
trace_id=51 func=resolve_ip_tuple_fast line=5827 msg="Find an existing session, id-00045e02, reply direction"
trace_id=51 func=vf_ip_route_input_common line=2615 msg="find a route: flag=00000000 gw-10.9.31.160 via port3"
trace_id=51 func=fw_forward_dirty_handler line=384 msg="auxiliary ses proto=6 dev=7->6 10.9.31.160/7932=>10.0.1.7/22"
trace_id=51 func=npu_handle_session44 line=1184 msg="Trying to offloading session from port2 to port3, skb.npu_flag=00000400 ses.state=00010280 ses.npu_state=0x04000000"
trace_id=51 func=ip_session_install_npu_session line=353 msg="npu session installation succeeded"
trace_id=51 func=fw_forward_dirty_handler line=394 msg="state=00010280, state2=00000000, npu_state=04000800"
```

- Interface index numbers:

```
# diagnose netlink interface list
if=port1 family=00 type=1 index=5 mtu=1500 link=0 master=0
if=port2 family=00 type=1 index=6 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=7 mtu=1500 link=0 master=0
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

Auxiliary sessions are disabled by default. You can enable the feature per VDOM by running the CLI commands shown on this slide.

This slide also shows a debug flow sample taken on FGT-1 when an auxiliary session is created for an SSH connection. The debug flow shows a line containing the `auxiliary ses` message followed by the index number of the interfaces (or devices) that are used for creating the auxiliary session. In this example, although not displayed on this slide, the session was initially established symmetrically from `port3` to `port1`—interface index numbers `7` and `5`, respectively. After that, FortiGate received a reply packet on `port2`—the first line of the debug flow—which triggered the creation of the auxiliary session for the `port3` to `port2` direction—interface index numbers `7` and `6`, respectively.

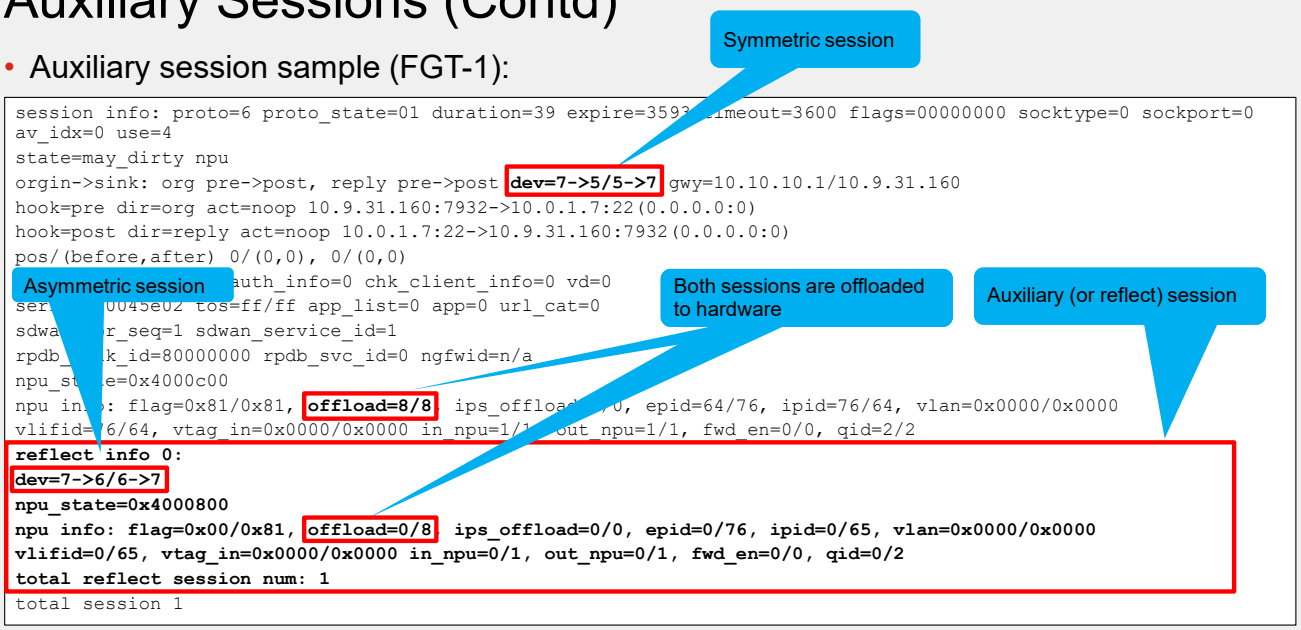


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Auxiliary Sessions (Contd)

- Auxiliary session sample (FGT-1):




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

This slide shows the resulting main session and auxiliary session based on the debug flow output shown on the previous slide. Note that only relevant lines of the session are displayed.

Also note that an auxiliary session is not a separate session, but an extension of the main session used for asymmetric traffic. As a result, FortiGate can offload traffic for both sessions to hardware, which results in higher performance.

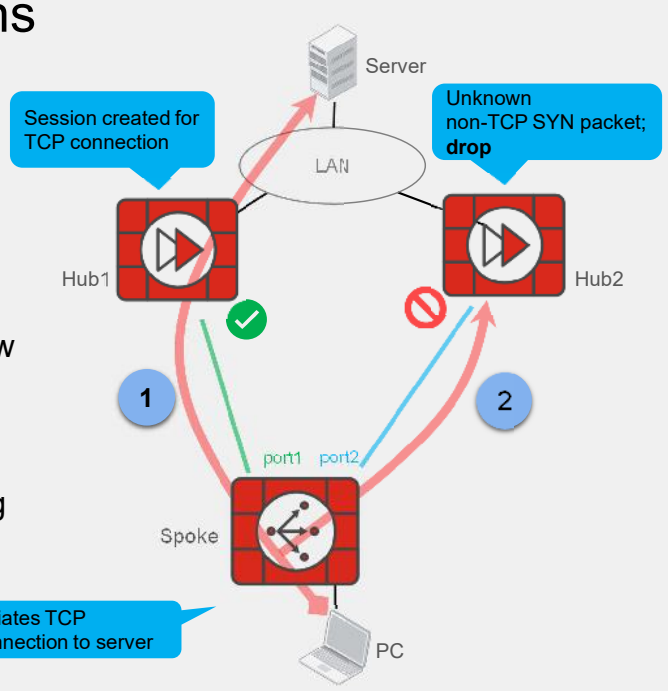


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Cross-FortiGate TCP Sessions

- SD-WAN can steer traffic of an active session to another FortiGate
  - Example: dual-hub and ADVPN topologies
- Cross-FortiGate TCP sessions are dropped because:
  - Packet is not TCP SYN and session is unknown to new FortiGate
- Enable `tcp-session-without-syn` to allow non-TCP SYN packets
  - Enable globally at VDOM level
  - Refine per firewall policy
- Evaluate risk acceptance level before enabling `tcp-session-without-syn`




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

You can configure SD-WAN to steer active sessions to a different member following a route or SLA change that affects the session. If the session in question is a TCP session, the session is dropped on the remote end if the new selected member connects to a different FortiGate device because of its stateful firewall inspection feature. Sessions that are routed across two different FortiGate devices are called cross-FortiGate sessions and are often seen in SD-WAN topologies like the one shown on this slide—dual-hub—or when using auto-discovery VPN (ADVPN). You will learn more about ADVPN in another lesson.

In the topology shown on this slide, the PC is connected behind the spoke FortiGate, and communicates using TCP with the server, which is behind the two hub FortiGate devices. If port1 on Spoke is the best member for steering traffic from the PC to the server, the packets are forwarded to Hub1. Hub1 also creates a session for the TCP connection. Then, if port2 becomes the best member while the connection is still active, Spoke starts forwarding the packets to Hub2. However, Hub2 drops the packets because they are not the initial TCP SYN packet of a three-way handshake, nor do they match any of the existing sessions.

You can solve the previous issue by enabling the `tcp-session-without-syn` setting. When you enable `tcp-session-without-syn`, FortiGate accepts unknown TCP sessions whose first packet isn't a TCP SYN, provided there is a firewall policy that allows the traffic. For the use case described here, enabling it on Hub2 would result in the connection staying up after the packets are forwarded to Hub2.

Note that you must first enable `tcp-session-without-syn` at the VDOM level under `config system settings` and then allow the feature for each firewall policy that requires it.

Enabling `tcp-session-without-syn` makes FortiGate less strict about TCP session acceptance and increases the risk level. You should carefully evaluate the acceptable risk level and enable only on polices that requires this feature.

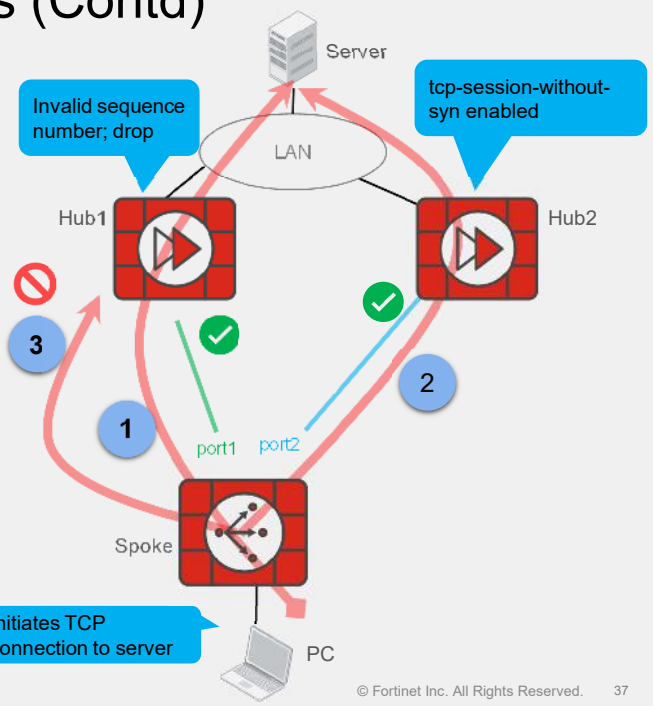


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Cross-FortiGate TCP Sessions (Contd)

- FortiGate checks TCP sequence numbers
- If TCP session is forwarded back to original FortiGate:
  - Packets are dropped because of invalid sequence numbers
    - If old session is still active (default expiration timer: 3600 seconds)
- Disable `anti-replay` to skip TCP sequence number check
  - Enable globally at VDOM level
  - Refine per firewall policy
- Evaluate risk acceptance level before disabling `anti-replay`




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

Continuing with the same dual-hub topology, assume that the administrator enabled `tcp-session-without-syn`, and that the TCP connection was accepted on Hub2 after the routing change on Spoke. Also assume that the connection is still active and continues to be routed to port2, and that no more than 60 minutes have passed since the routing change.

If port1 becomes again the best member, Spoke starts forwarding the packets back to Hub1. Because Hub1 still has a session for the TCP connection in its session table—the default expiration timer for established TCP sessions is 3600 seconds—the packets match the existing session but then get dropped by Hub1 because of invalid sequence numbers. The reason is that FortiGate also checks the sequence numbers of TCP packets. As a result, the sequence numbers of packets received by Hub1 do not match the expected values based on the latest session state recorded by Hub1, which happened just before the routing change to Hub2.

You can solve the previous issue by disabling the `anti-replay` setting. When you disable `anti-replay`, FortiGate doesn't check sequence numbers of TCP packets. As a result, Hub1 accepts the packets after the session is routed back to Hub1.

Note that you must first enable `anti-replay` at the VDOM level under `config system settings` and then allow the feature for each firewall policy that requires it.

Again, by disabling `anti-replay` on FortiGate, you disable a security feature. You should evaluate if the risk is acceptable and consider your device usage and location before doing so.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Cross-FortiGate TCP Sessions (Contd)

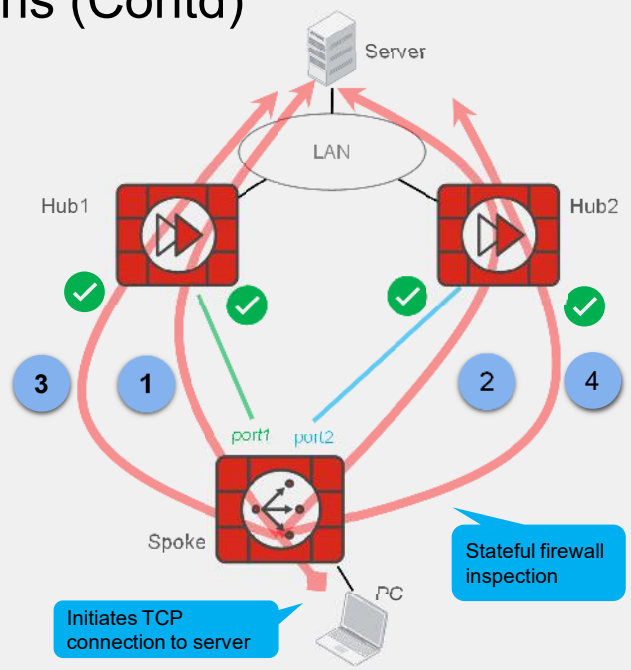
- Enable `tcp-session-without-syn` per VDOM

```
config system settings
    set tcp-session-without-syn enable
end
```

- Enable `tcp-session-without-syn` and disable `anti-replay` per policy:

```
config firewall policy
    edit <id>
        set anti-replay disable
        set tcp-session-without-syn all
    next
end
```

Setting is hidden if it is disabled on the VDOM




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

You can enable `tcp-session-without-syn` and disable `anti-replay` using the FortiGate CLI, as shown on this slide. First, you enable `tcp-session-without-syn` at the VDOM level. Then, at the policy level, you disable anti-replay and activate `tcp-session-without-syn` for `all` or for `data-only` sessions. The default value for each setting are `enable` and `disable`, respectively.

You must configure both settings on the firewall policy level. For the `tcp-session-without-syn` setting, you must first enable the setting per VDOM.

Continuing with the dual-hub topology example, the administrator should enable `tcp-session-without-syn` and disable `anti-replay` on both Hub1 and Hub2. The reason is that active TCP sessions could be routed back and forth between the hubs. Also, although the suggested configuration changes disable stateful firewall inspection for TCP traffic on Hub1 and Hub2, in most situations, this shouldn't represent a security concern because Spoke still performs the stateful firewall inspection for the TCP traffic.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe policy route operation, actions, and FIB validation
- ✓ Identify key routing principles in SD-WAN
- ✓ Understand the route lookup process
- ✓ Configure static routes for zones
- ✓ Understand common session flags
- ✓ Describe session reevaluation triggers
- ✓ Control routing changes in SNAT sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

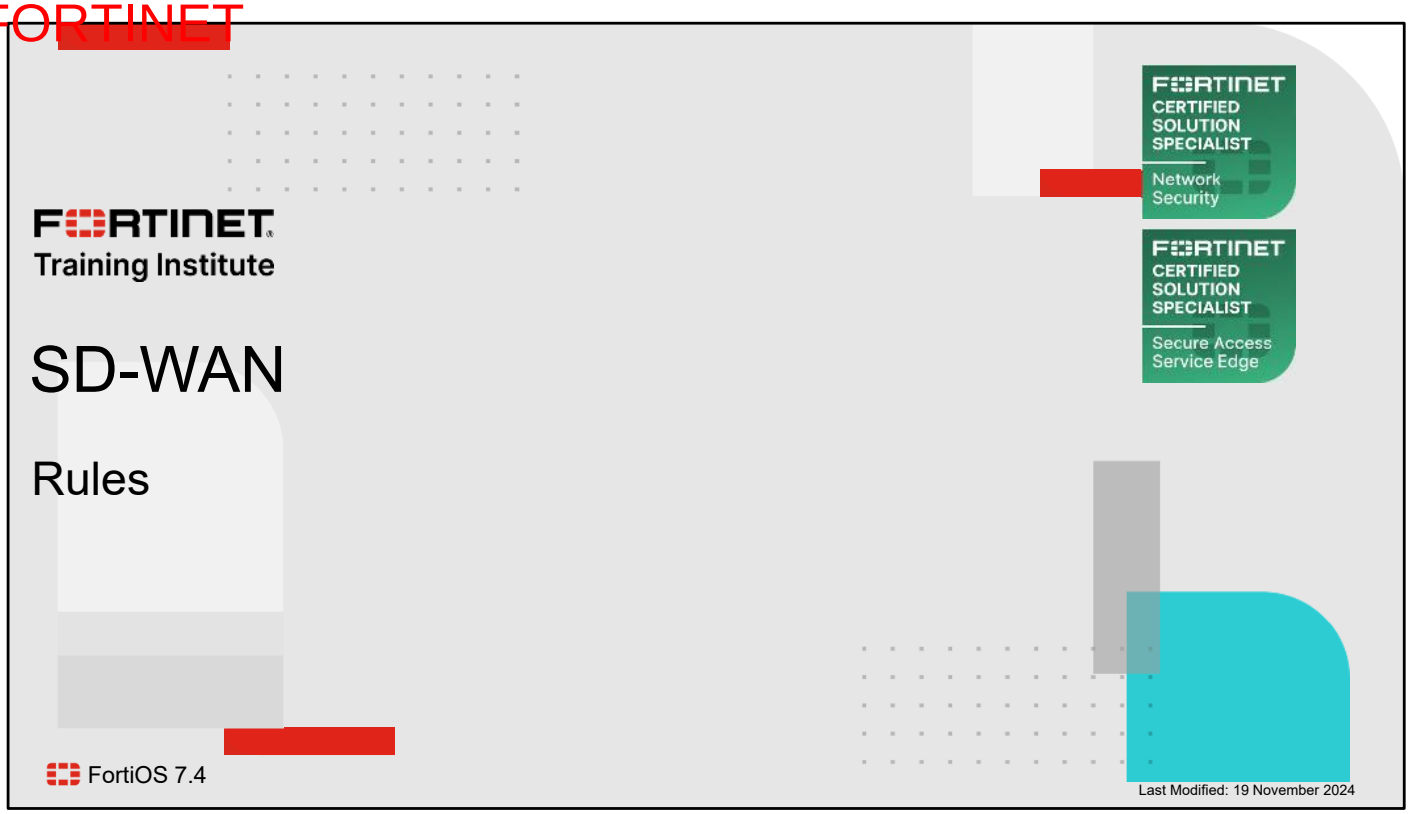
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the routing process in SD-WAN, member static route configuration, and how to control session reevaluation caused by route, interface, or firewall policy changes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

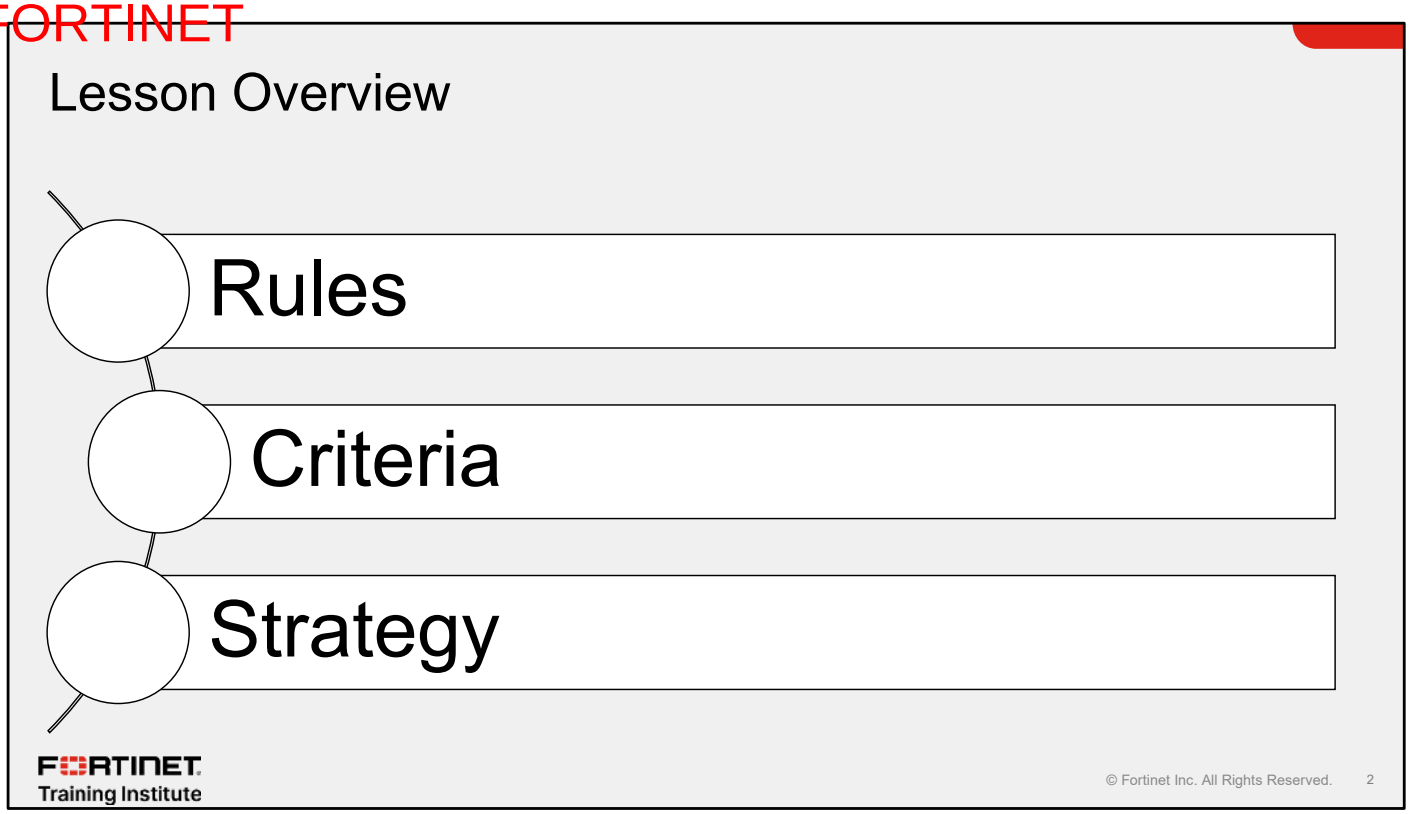



In this lesson, you will learn how SD-WAN rules work, based on the criteria and strategy in use.



Vouchers & Dumps are Available | WhatsApp +201224560923

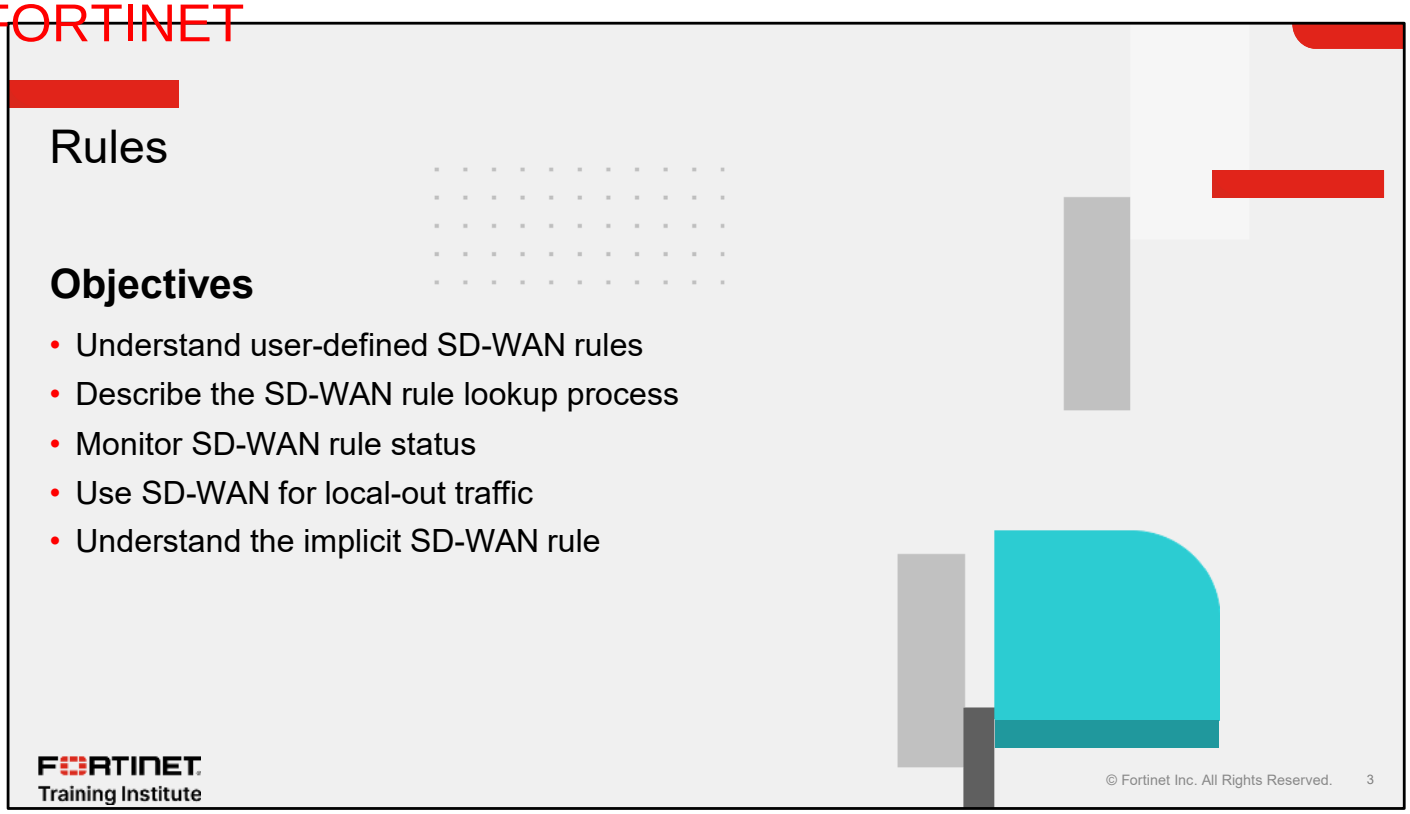
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding SD-WAN rules, you will know the fundamentals of SD-WAN rule configuration and operation.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Rules

- Describe administrator SD-WAN choices
- Two configuration sections:
  - Matching traffic criteria:
    - Define pattern, ISDB, and application to match
  - Forward policy:
    - Select preferred egress members and zones
    - Strategy
    - Required member performance metrics
- Evaluated in descending order:
  - Rules are used to steer traffic
    - Firewall policy required
  - Implicit rule
    - Used if user-defined rules are not matched
    - Traffic is usually load balanced

**Provisioning Templates > SD-WAN > SD-WAN Rules**

| | ID | Name | Source | Destination | Criteria | Members | Performance SLA | Status |
|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | Critical-DIA | LAN-net | Microsoft.Portal<br>Salesforce | Latency | port1<br>port2 | Corp_HC | Enable |
| ☐ | 3 | Corp | LAN-net | Corp-net | | HUB1-VPN1<br>HUB1-VPN2<br>HUB1-VPN3 | SLA (HUB1_HC#1)<br>SLA (HUB1_HC#2) | Enable |
| ☐ | | sd-wan | All | All | Source IP | All | | |

Implicit rule

Evaluation order

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

SD-WAN rules combine traffic matching criteria and traffic steering preferences. They describe the administrator choices related to the SD-WAN solution and the software-defined aspect of it. Remember that even if SD-WAN rules look similar to firewall policies, there purpose differs. SD-WAN rules determine *where* FortiGate steers the traffic, while firewall policies determine *which* traffic FortiGate allows through.

You first define the criteria of the application or traffic to match. Then, you indicate the forward policy to follow for steering traffic across one or more members and zones, including the strategy to apply and the performance metrics to determine the preferred members.

Preferred members are the best alive members based on the strategy in use. FortiGate then uses the preferred members—provided they are acceptable—to steer traffic. For all strategies, by default, FortiGate chooses a single member to steer traffic.

SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom, using the first match. However, unlike firewall policies, SD-WAN rules are used to steer traffic, and *not* to allow traffic. That is, you must also configure corresponding firewall policies to allow the steered traffic.

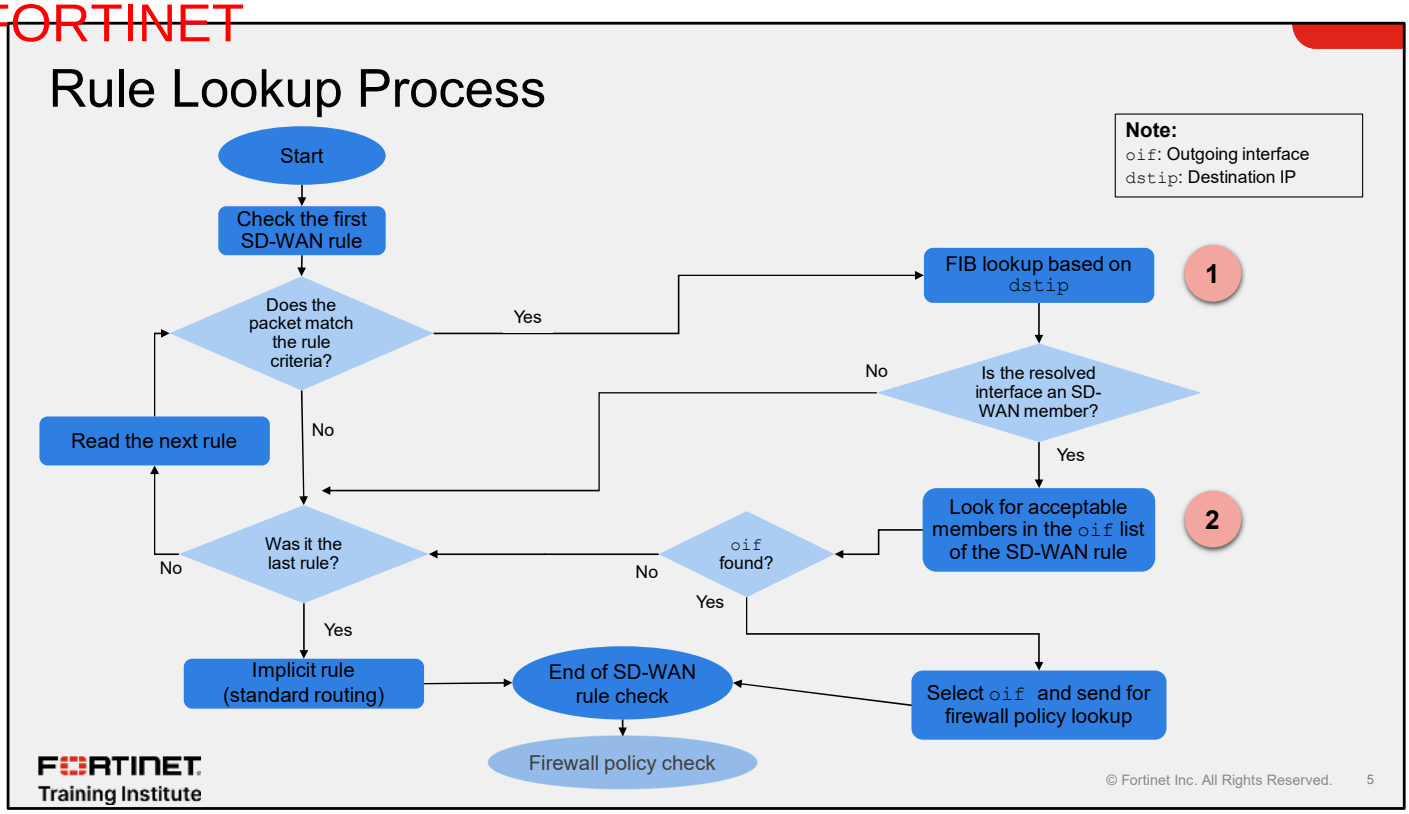
If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. The implicit rule instructs FortiGate to perform standard routing on traffic. Because SD-WAN deployments usually have multiple routes to the same destination—that is, ECMP routes—then traffic that matches the implicit rule is usually load balanced across multiple SD-WAN members.

The example on this slide shows a rule named **Critical-DIA**, which is used to steer internet traffic. The rule steers **Microsoft.Portal** and **Salesforce** traffic to the member with the lowest latency, between **port1** and **port2**. Note that only the most significant parts of rule configuration are shown in the output.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




This slide shows the SD-WAN rule lookup process. SD-WAN rules are essentially policy routes. Like regular policy routes, SD-WAN rules are checked from top to bottom (first match). For each rule, FortiGate maintains an outgoing interface (`oif`) list. The `oif` list sorts the configured members by preference based on the strategy in use. The members that are placed first in the list have higher preference for steering traffic. FortiGate starts the lookup process by comparing the packet against the rule matching criteria. If the packet doesn't match the criteria, FortiGate moves on to the next rule, and so on, until it finds a match. When there is a match, FortiGate proceeds as follows:

1. FortiGate performs a forwarding information base (FIB) lookup for the packet destination IP (`dstip`). If the resolved interface for the FIB best-match isn't an SD-WAN member, then FortiGate moves on to the next rule. This behavior follows the key routing principle: *SD-WAN rules are skipped, if the best route to the destination isn't an SD-WAN member.*

2. If the resolved interface is an SD-WAN member, then FortiGate looks for one or more acceptable members in the `oif` list, starting from the first member in the list. An acceptable member is an alive member that has a route to the destination. This behavior follows the key routing principle: *SD-WAN rules are skipped, if none of the configured members in the rule have a valid route to the destination.*

If FortiGate finds an acceptable member, it forwards the packet to that member—then firewall policy check occurs— and the rule lookup process ends. Otherwise, FortiGate moves on to the next rule. If all rules are skipped, then FortiGate routes the packet using standard routing, hence the key routing principle: *The implicit SD-WAN rule equals standard FIB lookup*.

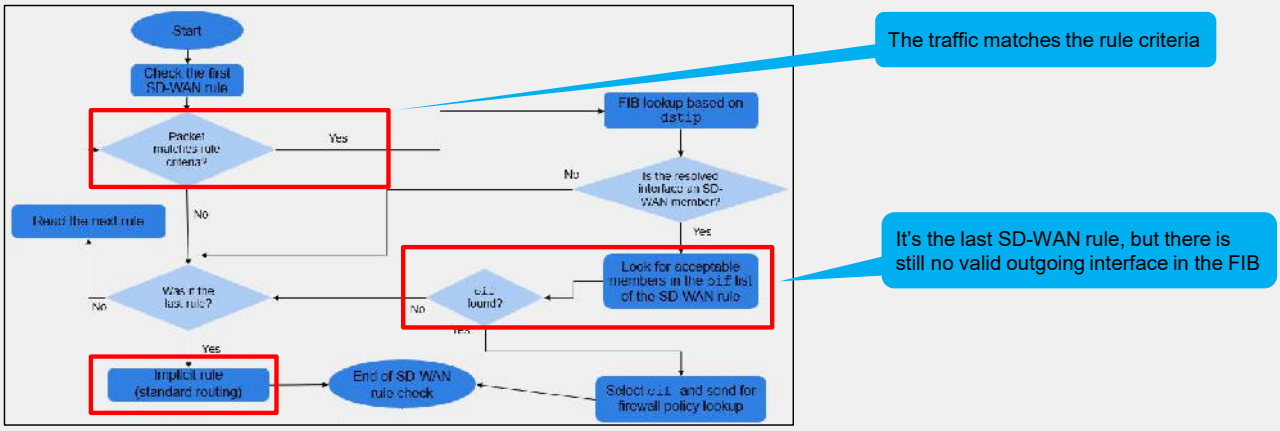


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# SD-WAN Rule Matched—No Route to Destination

- What happens when the traffic matches an SD-WAN rule, but FortiGate has no valid route to the destination?




FortiGate uses the implicit SD-WAN rule and routes the traffic according routing table

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

This slide highlights what happens when the traffic matches one or multiple SD-WAN rules, but FortiGate has no valid route to the destination. In other words, there is no corresponding route in the FIB. In this case, FortiGate skips all SD-WAN rules and routes the packet using standard routing, according to the key routing principle: *The implicit SD-WAN rule equals standard FIB lookup*.

Make sure you consider this principle when you define the routing on an SD-WAN device. FortiGate can use any valid route to steer the traffic, even routes that are not the best route to a destination according to static or dynamic routing principles. Backup routes are useful to benefit from SD-WAN capabilities and its fine-steering decision capabilities.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Viewing Rule Status

- View rule status on the FortiGate CLI:

```
# diagnose sys sdwan service4

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
  Internet Service(1): Tableau-SSH(5111814,0,0,0)
  Src address(1):
        10.0.1.0-10.0.1.255
```

Interface name

Zone name

Matching criteria and rule mode

Outgoing interface list

```
# diagnose firewall proute list
list route policy info(vf=root):

id=2130903043(0x7f030003) vwl_service=3(Corp) vwl_mbr_seq=4 5 dscp_tag=0xfc dictate flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Tableau-SSH(5111814,0,0,0)
hit_count=12 rule_last_used=2024-09-05 16:02:04
```

ID shown in debug flow output

Hit count and last time rule was hit

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

SD-WAN rules are dynamically updated based on the member status and performance. This means that the outgoing interface list can change over time, which is why it is useful to check their current status for troubleshooting purposes.

The best way to check the status of an SD-WAN rule is by running `diagnose sys sdwan service4`—`for IPv4 related rules or diagnose sys sdwan service6 for IPv6 related rules`—on the FortiGate CLI. As shown on this slide, the output indicates the matching criteria in use, the rule mode, and the outgoing interface list. You will learn more about the matching criteria, rule modes, and how FortiGate determines the preferred members in this lesson.

In addition, because SD-WAN rules are essentially policy routes, you can also run the `diagnose firewall proute list` command to display the rule settings from a policy route standpoint. SD-WAN rules are assigned a high ID number. The ID displayed in the `diagnose firewall proute list` command output is the same ID displayed in the debug flow output when a packet matches a rule. The output also includes the outgoing interface list, except that the interface preference is sorted from left to right, as opposed to the `diagnose sys sdwan service4` command, which sorts the interfaces from top to bottom.

For troubleshooting purposes, the output of the `diagnose firewall proute list` command also displays the rule hit count and the last time the rule was hit.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

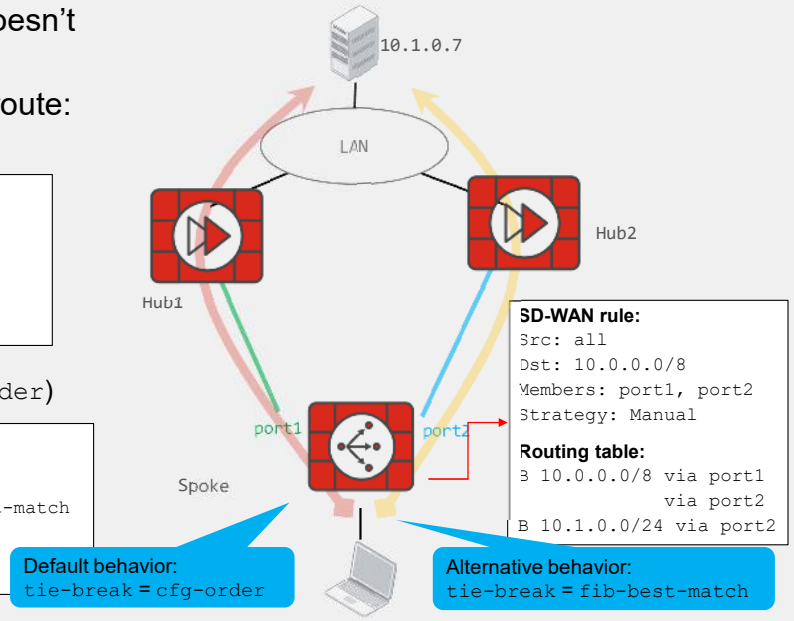
## Choosing the Best Route as the Preferred Member

- By default, the preferred member doesn't have to be the best route
- Choose preferred member by best route:
  - Option 1: Rule level (default = `zone`)

```
config system sdwan
    config service
        edit <id>
           set tie-break fib-best-match
        next
    end
end
```

  - Option 2: Zone level (default = `cfg-order`)

```
config system sdwan
    config zone
        edit <zone>
           set service-sla-tie-break fib-best-match
        next
    end
end
```




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

During the SD-WAN rule lookup, FortiGate checks the member routes twice:

1. When looking for a matching rule: FortiGate skips SD-WAN rules if the best route to the destination isn't an SD-WAN member.
2. After the rule is matched: FortiGate skips SD-WAN rules if none of the configured members in the rule have a valid route to the destination.

In the second member check situation, you can deduce that the preferred member doesn't have to be the best route to the destination. The member just needs to have a valid route to the destination. But what if you want FortiGate to consider only members with the best route to the destination as candidates? Then, you could control the preferred member election just by advertising a better route from the remote site.

The example on this slide shows a dual-hub and single-spoke topology. It includes a simplified version of the SD-WAN rule and routing table on the spoke. In the default behavior (`tie-break` set to `cfg-order`), FortiGate chooses port1 as the preferred member because it has a higher priority based on the configuration order. But if you set `tie-break` to `fib-best-match`, then FortiGate considers the best route to the destination (`10.1.0.7`) when choosing the preferred member in a rule. As a result, FortiGate chooses port2 as the only preferred member candidate because it has the most specific (best route) to the destination. Then, because port2 is the only candidate, it becomes the preferred member. This applies for all strategies. For example, in a lowest-cost strategy, FortiGate selects the preferred member from only those members that have the best route to the destination.

This slide also shows how to configure FortiGate to consider the members with the best route as preferred members. You can apply the configuration at the zone level or, for additional granularity, at the rule level. By default, the rule level setting (`tie-break`) is set to `zone`, which instructs FortiGate to follow the zone-level setting (`service-sla-tie-break`), which, in turn, is set to configuration order (`cfg-order`) by default.



Vouchers & Dumps are Available | WhatsApp +201224560923

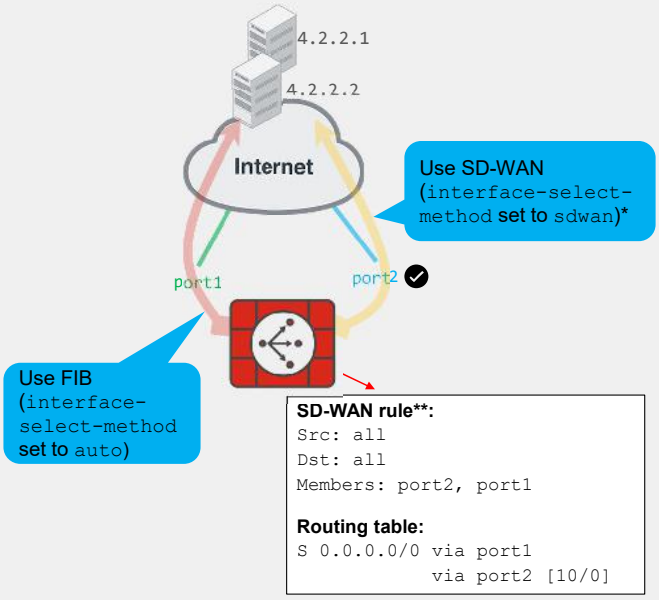
DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Use SD-WAN for Local-Out Traffic

- By default, local-out traffic doesn't use SD-WAN
- Enable SD-WAN for system DNS

```
config system dns
    set primary 4.2.2.1
    set secondary 4.2.2.2
    set interface-select-method sdwan
end
```

- `interface-select-method` is available on multiple features:
  - `config system dns | ntp | sflow | netflow`
  - `config system central-management`
  - `config system fortiguard`
  - `config user radius | ldap | fsso`
  - `config log fortianalyzer setting`
  - `config log syslogd setting`
- Enable SDWAN for ping and traceroute
  - `execute ping-options use-sdwan <yes|no>`
  - `execute traceroute-options use-sdwan <yes|no>`




* SD-WAN routing principles apply
** SD-WAN rule source address must match local IP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

Local-out traffic is defined as the traffic initiated by FortiGate, usually for management purposes. For example, when you ping a device from FortiGate, that's local-out traffic. When FortiGate connects to FortiGuard to download the latest definitions, that's also local-out traffic.

By default, local-out traffic uses the FIB to determine the best route for the destination. However, you can configure FortiGate to use SD-WAN rules for local-out traffic. For that, you must set `interface-select-method` to `sdwan` on the individual feature, so the feature uses SD-WAN to determine the best member to route the traffic to.

This slide shows an example of the system DNS configuration that uses SD-WAN to route system DNS queries. Before enabling SD-WAN for system DNS queries, FortiGate uses port1 because it has the best route for the destination in the FIB (lowest route priority). After enabling SD-WAN for system DNS queries, FortiGate starts using port2 because it's the preferred member for the matching SD-WAN rule.

This slide also shows a list of some of the features that support the `interface-select-method` setting. For troubleshooting purposes, you can also use SD-WAN for the FortiOS ping and traceroute tools.

Note that when you enable SD-WAN for local-out traffic, the same SD-WAN routing principles apply. For example, for a member to be acceptable, the member must have a route in the FIB to the destination. In addition, note that the source address of the SD-WAN rule must match the local IP address used by FortiGate for the local-out connection. Usually this means setting the source address to all addresses to potentially match any SD-WAN member.

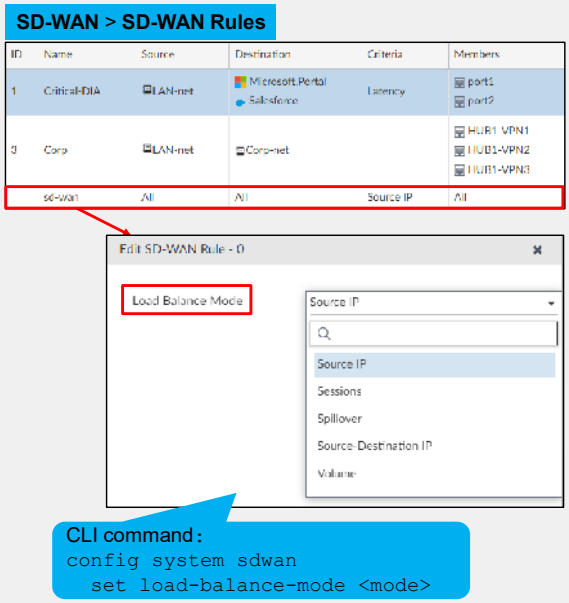


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Implicit Rule and Load Balancing

- Implicit rule means standard FIB
- SD-WAN sites usually have ECMP routes
  - Result: sessions are load balanced
- Load balancing algorithms:
  - **Source IP** (default):
    - Traffic from a source IP is sent to the same member
  - **Sessions**:
    - The higher the member weight, the more sessions are sent to it
  - **Spillover**:
    - Send sessions to first member until spillover limit is reached, then send to next member
  - **Source-Destination IP**:
    - Traffic from a source IP to a destination IP address is sent to the same member
  - **Volume**:
    - The higher the member weight, the more traffic is sent to it




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. When a session matches the implicit rule, FortiGate performs a standard FIB lookup. Because SD-WAN sites usually have multiple routes to the same destination through multiple members, this results in the presence of ECMP routes in the FIB. By default, FortiGate load balances sessions that match ECMP routes.

To load balance sessions, FortiGate uses the algorithm configured in the implicit rule:

- **Source IP**: This is the default algorithm. FortiGate sends sessions sourced from an IP address to the same member. (CLI `source-ip-based`)
- **Sessions**: FortiGate load balances sessions across members based on the member weight. The higher the weight, the more sessions FortiGate sends to the member. (CLI `weight-based`)
- **Spillover**: FortiGate sends sessions to the interface of the first ECMP route until the bandwidth of the interface reaches the configured spillover limit. After the spillover limit is reached, FortiGate uses the interface of the next ECMP route. (CLI `usage-based`)
- **Source-Destination IP**: FortiGate sends sessions with the same source and destination IP address pair to the same member. (CLI `source-dest-ip-based`)
- **Volume**: FortiGate load balances sessions across members based on the measured interface volume and the member weight. Unlike **Sessions**, which doesn't consider the traffic of an interface, the **Volume** algorithm instructs FortiGate to track the cumulative number of bytes of each member and to distribute sessions based on the weight. The higher the weight, the higher the target volume of the interface and, as a result, the more traffic FortiGate sends to it. (CLI `measured-volume-based`)



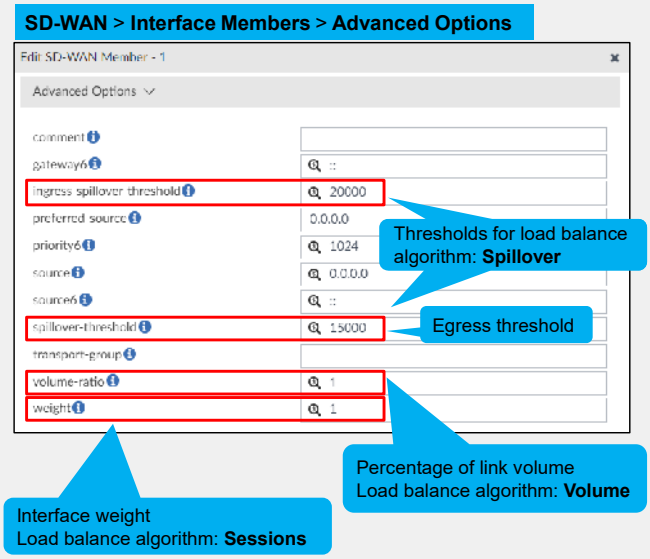
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Implicit Rule and Load Balancing (Contd)

- Weight and thresholds
  - Configured per interface
  - The parameter in use depends on the load balance algorithm selected
- Load balance algorithm parameters
  - Spillover: **ingress-spillover-threshold** and **spillover-threshold** (kbit/s)
  - Session: **weight**
  - Volume: **volume-ratio**
- If using dynamic routes, sessions are distributed equally, regardless of weight or volume ratio
- Formula for session or volume distribution

% sessions or traffic = member value/ (sum of all links values)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

When you set the implicit rule load balancing algorithm to **Sessions** or **Volume**, FortiManager assigns a default weight or a volume ratio of `1` to each member. You can change the weight and the volume ratio by editing the member settings.

When using static routing with the implicit SD-WAN rule, FortiGate uses the weight to calculate the percentage of sessions or traffic sent to each member, using the formula shown on this slide. For example, suppose that you configure two members—A and B—and you assign them weights of 5 and 10, respectively. If you use **Sessions** as the load balancing algorithm, then out of 15 sessions, FortiGate sends 5 to member A—that is, 33.33% of sessions—and 10 to member B—that is, 66.67% of sessions. Similarly, if you use **Volume** as the load balancing algorithm, then FortiGate distributes sessions so member A handles 33.33% of the total *amount of traffic*, while B handles the rest (66.67%).

When you set the load balancing algorithm to **Spillover**, you should also adjust the **Ingress Spillover** and **Egress Spillover** settings of each member. Otherwise, FortiManager keeps the default value (`0`), which disables spillover check.

Note that, with dynamic routing, even if you configured load balancing parameters—sessions, volume, or spillover, FortiGate distributes sessions equally if equal-cost multi-path (ECMP) routes are present. That is, FortiGate supports the load balancing setting only for static ECMP routes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Implicit Rule and Load Balancing Accuracy

- **Sessions** distribution doesn't have to result in proportional bandwidth or volume
  - Traffic varies among sessions
- **Spillover** and **Volume** distribution may exceed the configured threshold and weight
  - Sessions are not flagged as dirty if threshold is reached
  - Sessions stay in the same member until expiration or forced route lookup (route in use is removed)
    - Including long-lived high-bandwidth sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

It's important to understand the expected traffic distribution with the **Sessions**, **Spillover**, and **Volume** algorithms.

For **Sessions**, the weight assigned to members doesn't necessarily translate to the same bandwidth or volume observed on members. FortiGate load balances sessions across members based on the configured weight. Because the bandwidth and lifetime of each session are likely to be different, then the resulting bandwidth and volume are not proportional to the weight. For example, assume that FortiGate sends ten ICMP sessions to a member, and one FTP session to another member. Despite being one session, the bandwidth and volume of traffic transmitted over the member used for routing the FTP session is likely to be higher than the total bandwidth and volume observed on the member used for routing the ten ICMP sessions.

In addition, for **Spillover** and **Volume**, it's fine if the bandwidth exceeds the configured spillover thresholds, or if the amount of traffic on an interface exceeds the expected volume based on the configured weight. The reason is that unlike service-level agreement (SLA) changes in SD-WAN rules, which flag impacted sessions as dirty to force reevaluation, sessions routed using **Spillover** and **Volume** are not flagged as dirty as a result of thresholds being reached. That is, sessions stay in the same member until they expire, or until they are subject to a forced route lookup caused by the removal of the route in use. This means that FortiGate usually doesn't change the routing of existing sessions distributed using **Spillover** and **Volume** algorithms, including that of long-lived high-bandwidth sessions that generate large amounts of traffic.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## System Settings Algorithm vs. Implicit Rule Algorithm

- Both `v4-ecmp-mode` and `load-balance-mode` control the VDOM ECMP algorithm
  - `load-balance-mode` replaces `v4-ecmp-mode` when SD-WAN is enabled
- Differences:
  - `load-balance-mode` supports the volume algorithm, `v4-ecmp-mode` does not
  - `load-balance-mode` uses the weight defined under the SD-WAN member configuration, `v4-ecmp-mode` the weight defined in the static route
  - `load-balance-mode` uses the spillover thresholds defined under the SD-WAN member configuration, `v4-ecmp-mode` the spillover thresholds defined in the interface settings

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

If you are familiar with ECMP, you probably know the `v4-ecmp-mode` setting available under `config system settings`. The `v4-ecmp-mode` setting defines the algorithm that FortiGate uses to load balance sessions that match ECMP routes in the VDOM.

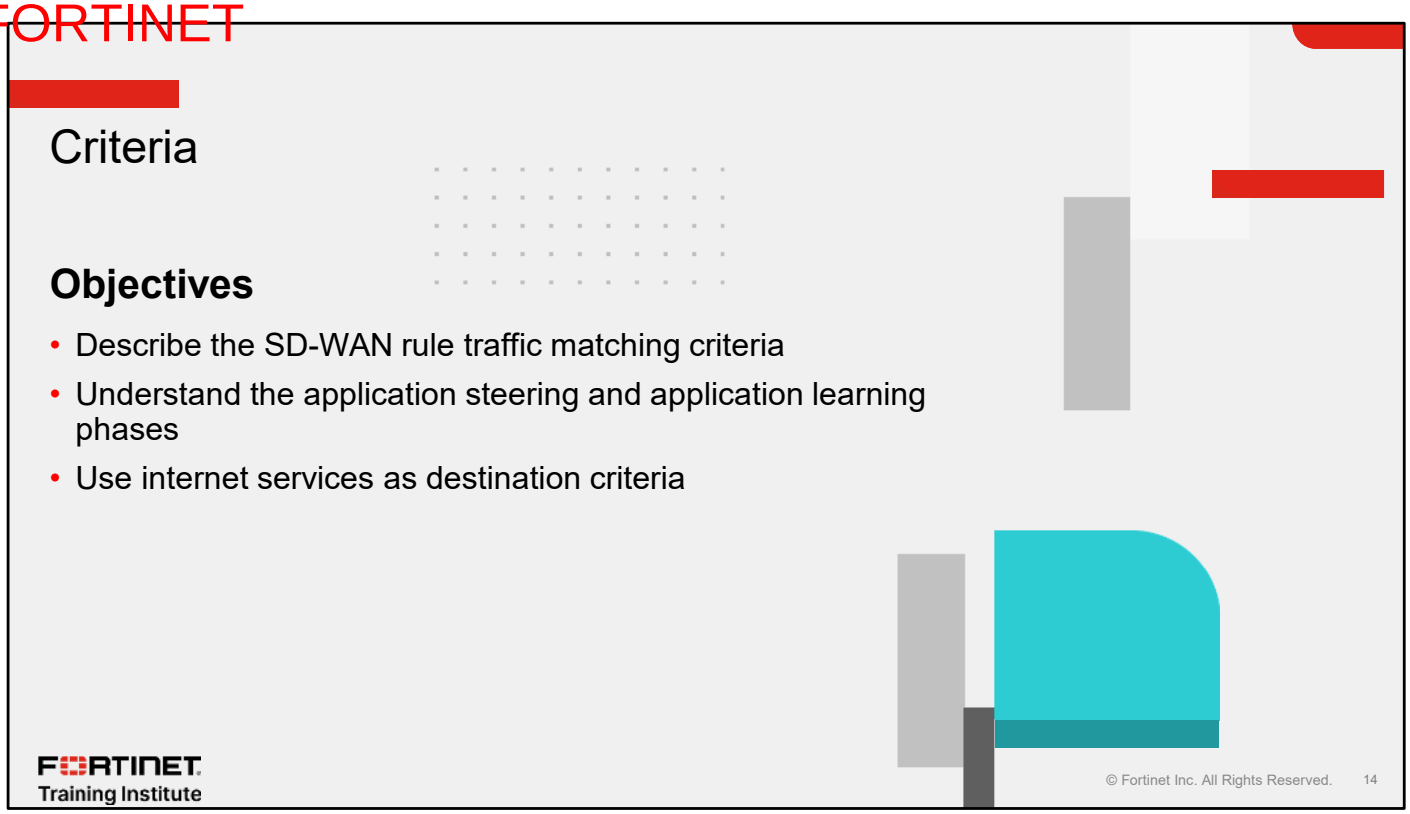
However, when you enable SD-WAN on FortiGate, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, after you enable SD-WAN, you now control the VDOM ECMP algorithm with the `load-balance-mode` setting.

There are some differences between the two settings. The main difference is that `load-balance-mode` supports the volume algorithm, and `v4-ecmp-mode` does not. In addition, the related settings such as weight and spillover thresholds are configured differently. That is, when you enable SD-WAN, the weight and spillover thresholds are defined on the SD-WAN member configuration. When you disable SD-WAN, the weight and spillover thresholds are defined on the static route and interface settings, respectively.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the supported SD-WAN rule traffic matching criteria, you will be able to identify the best criteria to use for matching SD-WAN traffic in your deployment.

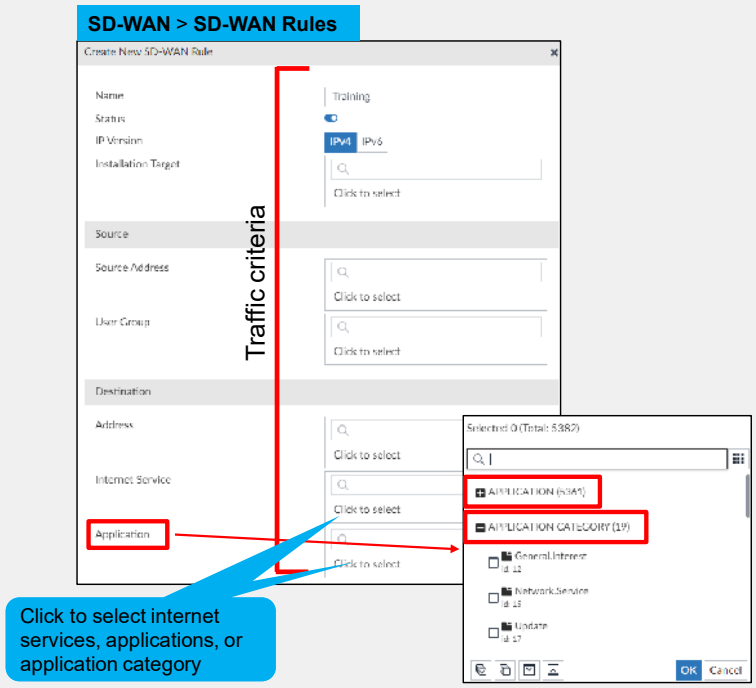


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Criteria

- Rules can match traffic based on:
  - Source
    - IP address
    - Firewall user and user group
  - Destination:
    - IP address
    - Internet service
    - Application or application category
  - Advanced options
    - Source interface
    - Source port or source port range
- IPv4 and IPv6 support




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

You can configure rules to match traffic based on the following main criteria:
- Source IP address, firewall user, and firewall user group.
- Destination IP address and IP protocol
- Internet service, individual service, or group of services
- Application or application category

You can further refine the source traffic definition with the parameters available in the **Advanced Options** section, such as:
- The source interface with the `input-device` and `input-device-negate` settings
- The source port or source port range

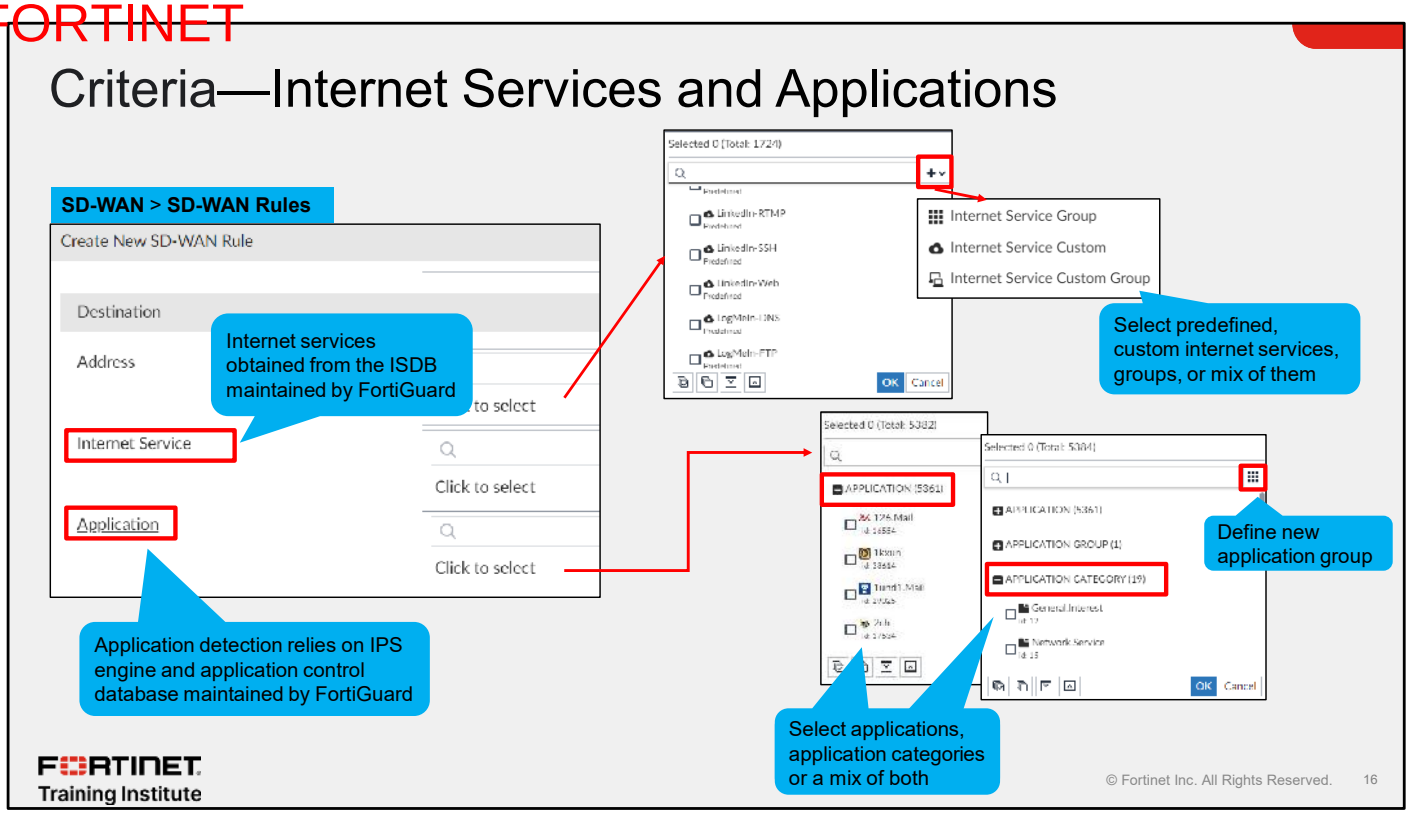
SD-WAN rules offer great flexibility for traffic matching. For example, you can match Netflix traffic sourced from specific authenticated users, or match the ICMP traffic—IP protocol 1—destined to a particular address. However, note that the IP protocol definition field is visible only after you select a destination IP address or address group, and that you cannot combine the definition of the destination per address and protocol with a definition per internet service or application in the same rule.

The example on this slide shows the settings available when you create a new rule using FortiManager. Note that both IPv4 and IPv6 protocols are supported, and that you can select individual internet services and applications, or groups of them.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




You can configure a rule to match traffic based on the destination internet service and the application detected for the traffic. The destination internet service relies on the internet service database (ISDB), and application detection relies on the intrusion prevention system (IPS) engine and the application control database signature.

FortiGuard maintains both databases, and FortiGate periodically gets an updated copy by default. New versions of the IPS engine are also released by FortiGuard, but much less frequently than definitions and databases. When a new IPS engine version is released, FortiGate also downloads it automatically by default.

The example on this slide shows a subset of the internet services and applications available in a rule.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

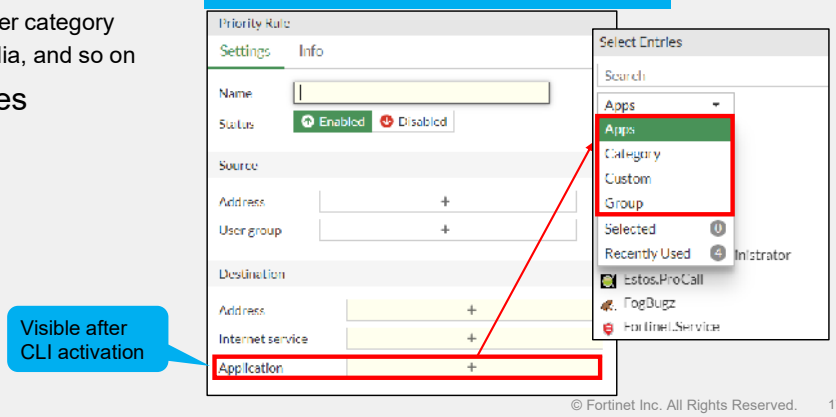
## Criteria—Applications and Application Groups

- Rules can match traffic based on:
  - Applications
    - One or more application from predefined list
    - User defined custom application
  - Application group
    - User defined group of applications
  - Application category
    - Predefined group of applications per category
    - Business, game, proxy, social media, and so on
- Application filter for SD-WAN rules
  - Visible by default on FortiManager
  - Hidden by default on FortiGate GUI

- Enable GUI visibility for application detection on FortiGate

```
config system global
    set gui-app-detection-sdwan enable
end
```

FortiGate: **Network** > **SD-WAN** > **SD-WAN Rules**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

For application detection, you can use applications from the FortiGuard predefined application list, define a custom application, create groups with those applications, or use application categories. Application categories group applications per purpose, for example business, game, social media, and so on. You can also combine application groups with a selection of application definitions.

Note that the **Application** setting is always visible on the FortiManager menu. However, if you decide to configure SD-WAN rules directly from the FortiGate GUI, you need to enable GUI visibility for application detection with the CLI commands shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## ISDB

- Maintained by FortiGuard
- Automatically retrieved by FortiGate
- Each internet service:
  - Is assigned an ID
  - Contains multiple entries indicating:
    - A range of public IP addresses
    - IP protocol
    - Destination port
  - Is loaded to the kernel and can be used in multiple features
  - Indicates the direction the entries are valid for
  - SD-WAN rules support only ISDB entries defined with direction `dst` or `both`
- Supports customized, user created, ISDB entries

```
# diagnose internet-service id-summary
...
id: 1245187 name: "Fortinet-DNS"
id: 1245188 name: "Fortinet-Outbound_Email"
...

# diagnose internet-service id-summary 1245187
Version: 00007.03708
Timestamp: 202405271125
Total number of IP ranges: 2124478
Number of Groups: 24
Group(0), Singularity(90), Number of IP ranges(22025)
...
Group(23), Singularity(4), Number of IP ranges(4926)
Internet Service: 1245187(Fortinet-DNS)
Number of IP ranges: 566
Number of Entries: 1132
Number of IP addresses: 52707
Singularity: 10
Icon Id: 19
Direction: dst
Data source: isdb
Country: 12 32 36 ...
Region: 55 132 159 169 ...
City: 339 615 818 821 ...
```

Can be `dst` (destination), `src` (source), or `both`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

FortiGuard maintains the Internet Service Database (ISDB) and releases updated versions frequently. FortiGate then downloads the most recent version automatically from FortiGuard servers.

Each service in the ISDB is assigned an ID that represents a well-known internet service such as Fortinet-FortiGuard, Google-ICMP, Facebook-Web, and so on. Each ID contains multiple entries, each of them indicating a range of public IP addresses, IP protocol, and destination ports associated with the service.

The internet service entries are loaded in the kernel. You can then reference an internet service in multiple parts of the configuration, such as SD-WAN rules and firewall policies.

Each internet service also indicates the direction of the traffic that the entries are valid for. The direction can be source, destination, or both. For SD-WAN rules, you can use only internet services that are valid for the destination direction, or both source and destination directions. This is because SD-WAN supports internet services for matching only the destination of a packet.

You can use the `diagnose internet-service id-summary` command to display a summary of the internet services in the ISDB. Add the internet service ID to the end of the command to view more details about that specific internet service. The example on this slide show an extract of the output for the internet service ID 1245187—Fortinet-DNS.

When required, to complement the FortiGuard maintained ISDB list, administrators can create custom internet service and custom internet service group with personalized list of entries.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## ISDB (Contd)

- View address ranges, protocol, and ports per internet service ID:

```
# diagnose internet-service id 1245187
Internet Service: 1245187(Fortinet-DNS)
Version: 00007.03708
Timestamp: 202405271125
Number of IP ranges: 1132
...
212.166.61.130-212.166.61.130 country(56) region(2060) city(615) blocklist(0x0) reputation(5),
popularity(5) domain(376) botnet(0) proto(6) port(53)
...
```

- Find internet service by IP, protocol, and port:

```
# diagnose internet-service info root 6 53 212.166.61.130
Internet Service: 1245187(Fortinet-DNS) country(56 Belgium) region(2060 Walloon) city(615 Amay)
```

- Find internet service by IP:

```
# diagnose internet-service match root 212.166.61.130 255.255.255.255
Internet Service: 1245185(Fortinet-Web), matched entry num: 4, matched num: 4
Internet Service: 1245186(Fortinet-ICMP), matched entry num: 2, matched num: 2
Internet Service: 1245187(Fortinet-DNS), matched entry num: 2, matched num: 2
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

You can use the command `diagnose internet-service id` to display detailed information about an internet service. The output indicates the public IP ranges of the service, as well as the protocol and port used for each range.

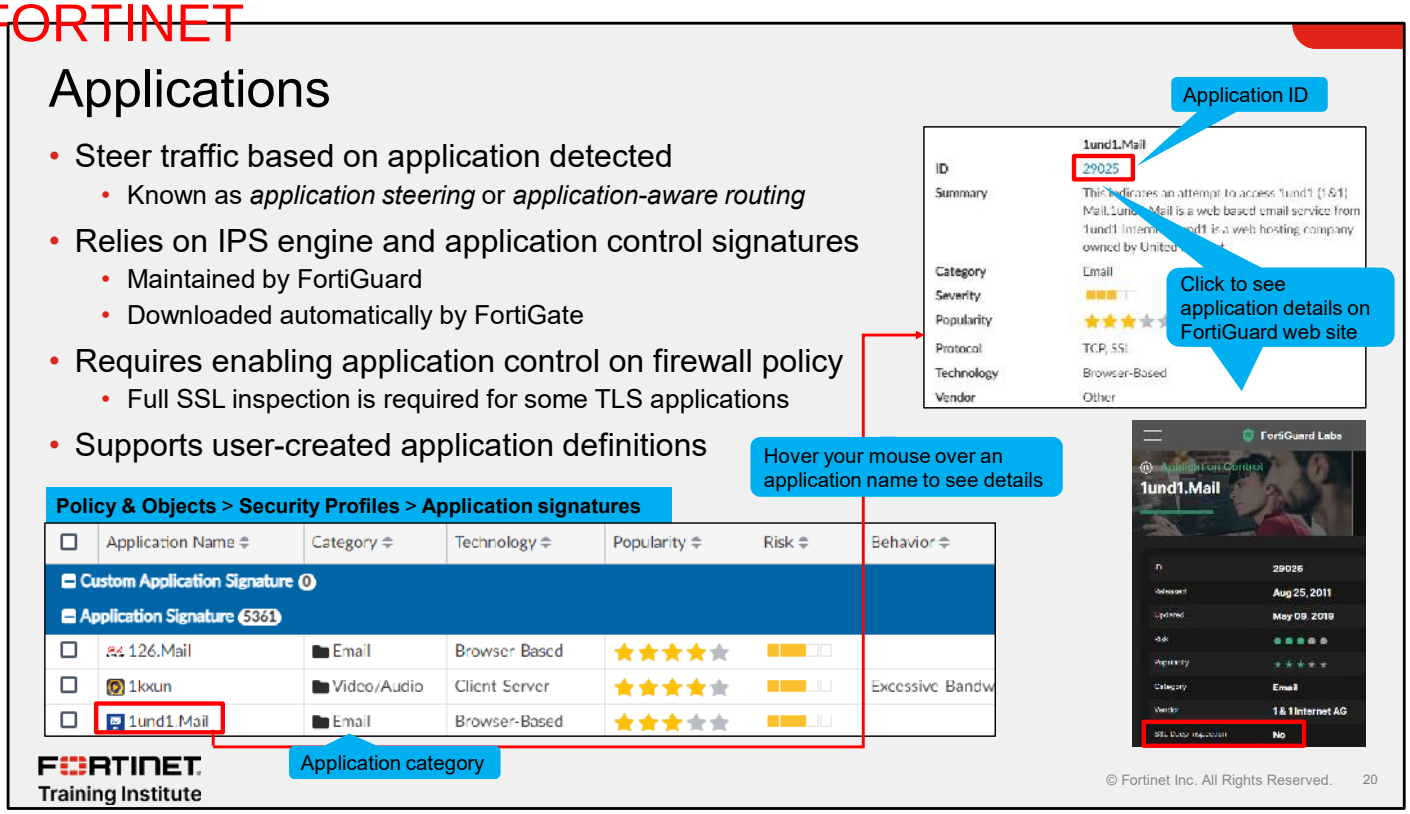
You can also find the internet service that matches a given IP address, protocol, and port by using the `diagnose internet-service info` command. However, if you only know the IP address of the service you want to look up, you can run the `diagnose internet-service match` command instead. Note that the `diagnose internet-service info` and `diagnose internet-service match` commands are global commands and, therefore, require you to indicate the VDOM to perform the lookup on—`root` in the example.

From the last example, you can see that an address range can match multiple internet services. It is common and correspond to application hosted on the same servers.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




You can configure rules to steer traffic based on the application detected by FortiGate. This is known as *application steering* or *application-aware routing.* Application detection relies on the IPS engine, and the application control signatures maintained by FortiGuard. By default, FortiGate automatically downloads the new versions of the IPS engine and the application control database after they are released by FortiGuard. The administrator can create custom application definition to complement the descriptions available in the FortiGuard list. A common use case of user created application definition is to allow FortiGate to recognize a company proprietary application.

For FortiGate to detect applications and, therefore, for SD-WAN to perform application steering, you must enable application control on the firewall policy that allows the SD-WAN traffic. You must also enable full SSL inspection if you want to detect applications that require it. For example, Facebook_Chat—a child application of Facebook—requires full SSL inspection but its parent application, Facebook, does not. Usually, FortiGate can detect a parent TLS application, like Facebook, without full SSL inspection but requires it for detecting child TLS applications like Facebook_Chat. This is because FortiGate must decrypt the TLS traffic to identity the child application. You can identify whether an application requires full SSL inspection by checking the application information page on FortiGuard.

You can access the application list from the FortiManager GUI as shown on this slide. If you hover your mouse over an application name, FortiManager displays details about the application. When you click on the application ID, FortiManager directs you to the FortiGuard page for this application. Another way to access the application information page is by adding the application ID to the end of the URL: `www.fortiguard.com/appcontrol/`.

The FortiManager GUI page and the FortiGuard page also indicates the category in which the application is classified. This is the category that the application category filter uses.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Application Learning

- Application cache
  - 3-tuple: destination address, destination protocol, destination port
  - Dynamically populated from traffic
  - Multiple 3T per application ID
  - 8 hours timeout
- Learning phase
  - No entry in cache for application *App1*
  - Session not identified as application *App1*
  - Session routed by SD-WAN rule and allowed by a policy without application *App1* match
  - IPS engine analyze the flow to populate application cache
  - Application detection must be enabled on the policy that allows the flow
- Known application
  - Received flow matches 3-tuple in cache
  - Session identified as application *App1*
    - Can match SD-WAN with application steering
    - Can match policy rule with application detected

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

FortiGate populates its application cache dynamically by learning from the traffic that flows through it.

Each time FortiGate allows a traffic flow through with a policy that has application control enabled, it sends the traffic to the IPS engine for analysis. Once FortiGate detects an application, it populates the application cache with a 3-tuple entry. The cache consists of a list of application IDs associated with destination addresses, protocol, and port. Note that the application cache can contain multiple 3-tuples for one application, to accommodate multiple servers handling the same application. Entries remain in the cache for 8 hours if they are not matched.

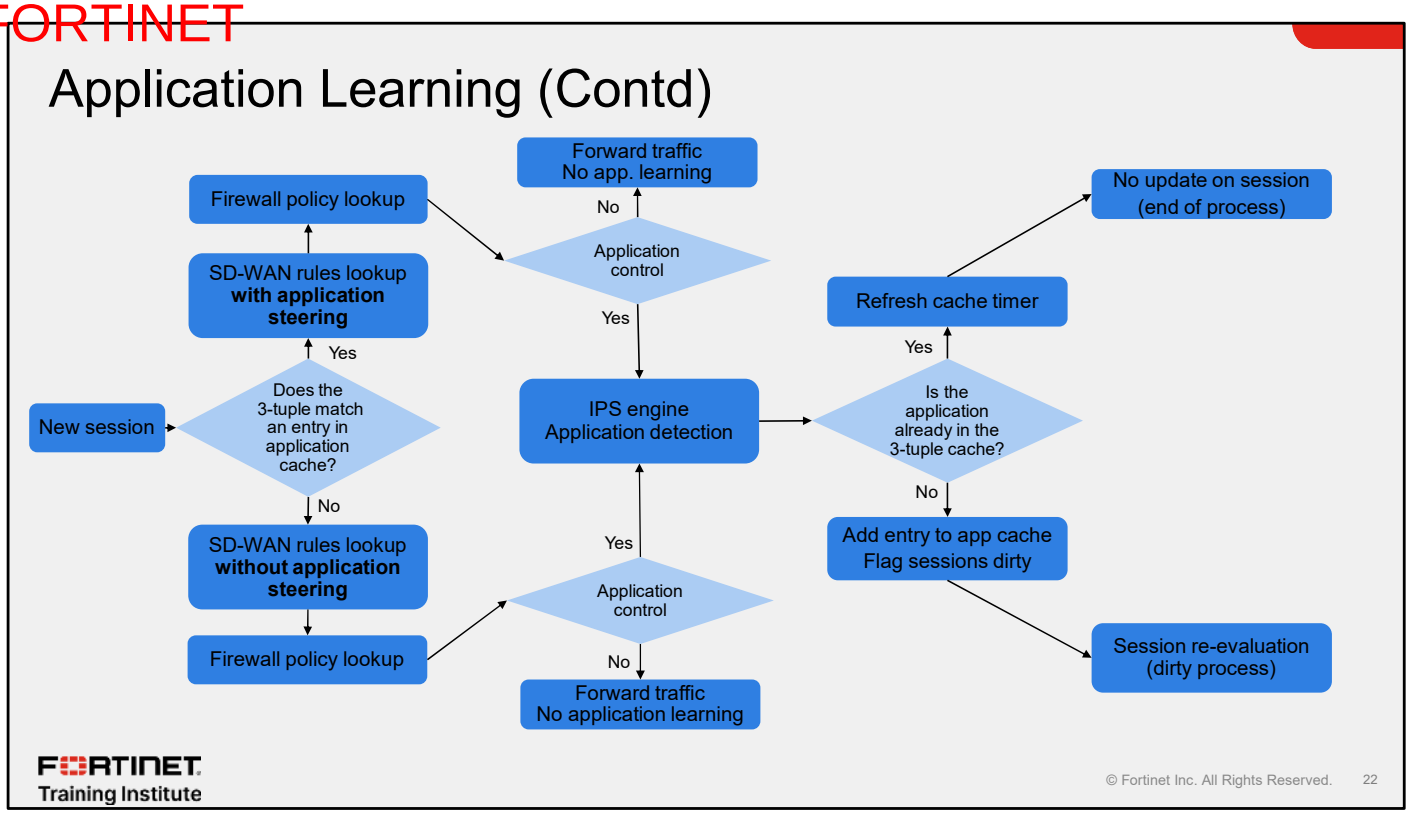
When FortiGate receives traffic, if the destination address, port, and protocol do not match an entry in application cache, FortiGate cannot immediately identify the application. It forwards the traffic using an SD-WAN rule and a firewall policy rule that do not require an application match. If the firewall policy that allows these initial packets stipulates application detection, then the policy triggers application recognition through the IPS engine. The policy allows the flow and, simultaneously the IPS engine analyzes the traffic to identify the application. This is called the application learning phase.

When a 3-tuple from incoming traffic matches an application in the cache, FortiGate can steer the traffic according to application detected and the corresponding SD-WAN rules.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




When you use SD-WAN for application steering, FortiGate must identify the application on the traffic before it can match the right rule. This is called the application learning phase. During this phase, FortiGate will still forward the packets with information already available. Therefore, the first packets of a session may not match the expected rule and member.

When a new session arrives, it matches SD-WAN rules with application steering only if there is a 3-tuple cache entry match. Otherwise, it matches an SD-WAN rule, based on destination address or ISDB entry (explicit or default implicit rule). At the same time, if the firewall policy that allows the traffic has application control, FortiGate begins application analysis. When FortiGate detects a new application, it updates the application cache. This trigger a reevaluation of the sessions (dirty process). If FortiGate flags the session as dirty, it reevaluates the session and can now match an SD-WAN rule using application steering.

It is important to understand that, during the learning phase, when FortiGate has not yet identified an application, the session might match a different rule and therefore might not be routed through the desired SD-WAN link.

Also, note that application learning can occur only if firewall policies enable application detection. You must make sure application detection is enabled on policies that allow traffic during the learning phase.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Viewing the Application Control DB in Kernel

- View the application control database on the FortiGate CLI:

```
# diagnose sys sdwan internet-service-app-ctrl-list
List App Ctrl Database Entry(IPv4) in Kernel:

LinkedIn(16331 23): IP=13.107.42.14 6 443
Salesforce(16920 29): IP=23.205.255.236 6 443
Salesforce(16920 29): IP=23.205.255.239 6 443
```

Multiple 3-tuple for Salesforce application

App. ID | App. category | 3-tuple

- SD-WAN rule correlation:

```
# diagnose sys sdwan service4 2

Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Internet Service(2): Dropbox-SSH(720902,0,0,0) LinkedIn-Web(851969,0,0,0)
  Application Control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
  Src address(1):
        10.0.1.0-10.0.1.255
```

ISDB app ID

Application ID | Application category ID

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

You can view the detected application entries in the application kernel database by running `diagnose sys sdwan internet-service-app-ctrl-list` on the FortiGate CLI. Each entry in the output indicates the application ID, the ID of the application category, and the corresponding 3-tuple. Note that FortiGate maintains one application per 3-tuple but one application can be associated with multiple 3-tuples. If multiple applications are detected for the same 3-tuple, FortiGate uses the most recent detected application for the 3-tuple.

You can filter the output per application ID or per application category with the commands `diagnose sys sdwan internet-service-app-ctrl-list app-id <app-id>` and `diagnose sys sdwan internet-service-app-ctrl-list cat-id <cat-id>`.

FortiGate uses the application ID, ISDB application ID, and 3-tuple to match the SD-WAN rule. In the example shown on this slide, one cache entry is for a LinkedIn connection destined to 13.`107.42.14` on TCP port 443. A connection that matches the cache entry also matches SD-WAN rule ID 2. In the CLI output, you can see that the administrators defined the rule ID 2 to match the traffic per application—for `Facebook` and `LinkedIn`—with the application ID shown as the first numeric value. They also defined it to match traffic per application category — for the `game`—with the application group ID shown as the second numeric value.

Note that entries in the application cache expire eight hours after last detected match.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Viewing the Application ID on the Session:

- Session routed using application steering:

```
session info: proto=6 proto_state=11 duration=5 expire=3596 timeout=3600 refresh_dir=both flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 f02 app_valid
statistic(bytes/packets/allow_err): org=3427/20/1 reply=4749/23/1 tuples=2
tx speed(Bps/kbps): 638/5 rx speed(Bps/kbps): 884/7
orgin->sink: org pre->post, reply pre->post dev=7->20/20->7 gwy=100.64.1.9/10.0.1.101
hook=pre dir=org act=noop 10.0.1.101:43020->10.1.0.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.7:22->10.0.1.101:43020(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=000b2f2d tos=ff/ff app_list=2002 app=16060 url_cat=0
sdwan mbr_seq=4 sdwan_service_id=2
rpdb_link_id=ff000002 ngfwid=n/a
```

Application detection flag

Application ID (SSH)

Member and rule IDs

- Look up application name by ID:

```
# get application name status | grep 16060 -B1
app-name: "SSH"
id: 16060
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

FortiGate writes the application information on the SD-WAN session. The `app` field indicates the application ID. You can look up the application name by using the `get application name status` command, as shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Unexpected Routing During Application Learning

- SSH session *without SNAT*:
  - Packet capture before application is learned (no entry in cache; unexpected member):

```
# diagnose sniffer packet any "host 10.1.0.7 and port 22" 4 | grep HUB1
...
9.612274 HUB1-VPN1 out 10.0.1.101.45366 -> 10.1.0.7.22: syn 2174489972
9.723809 HUB1-VPN1 in 10.1.0.7.22 -> 10.0.1.101.45366: syn 1405985100 ack 2174489973
```

  - After the application is learned, entry is added in cache:

```
# diagnose sys sdwan internet-service-app-ctrl-list

SSH(16060 4294837753): 10.1.0.7 6 22 Mon Sep 02 19:31:31 2024
```

  - Packet capture after application is learned (same session):

```
...
45.728896 HUB1-VPN2 out 10.0.1.101.45366 -> 10.1.0.7.22: psh 2174491574 ack 1405986770
45.740151 HUB1-VPN2 in 10.1.0.7.22 -> 10.0.1.101.45366: psh 1405986770 ack 2174491722
```

  - Packet capture for new session with same 3-tuple (expected member):

```
...
59.423616 HUB1-VPN2 out 10.0.1.101.50214 -> 10.1.0.7.22: syn 2044383473
59.425359 HUB1-VPN2 in 10.1.0.7.22 -> 10.0.1.101.50214: syn 1902219655 ack 2044383474
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

When you use application steering, a session may match an unexpected rule and member when the session 3-tuple doesn't have an entry in the ISDB application cache, or when the session 3-tuple has an entry in the ISDB application cache, but the detected application is different. In both cases, the session may initially match the wrong rule and member.

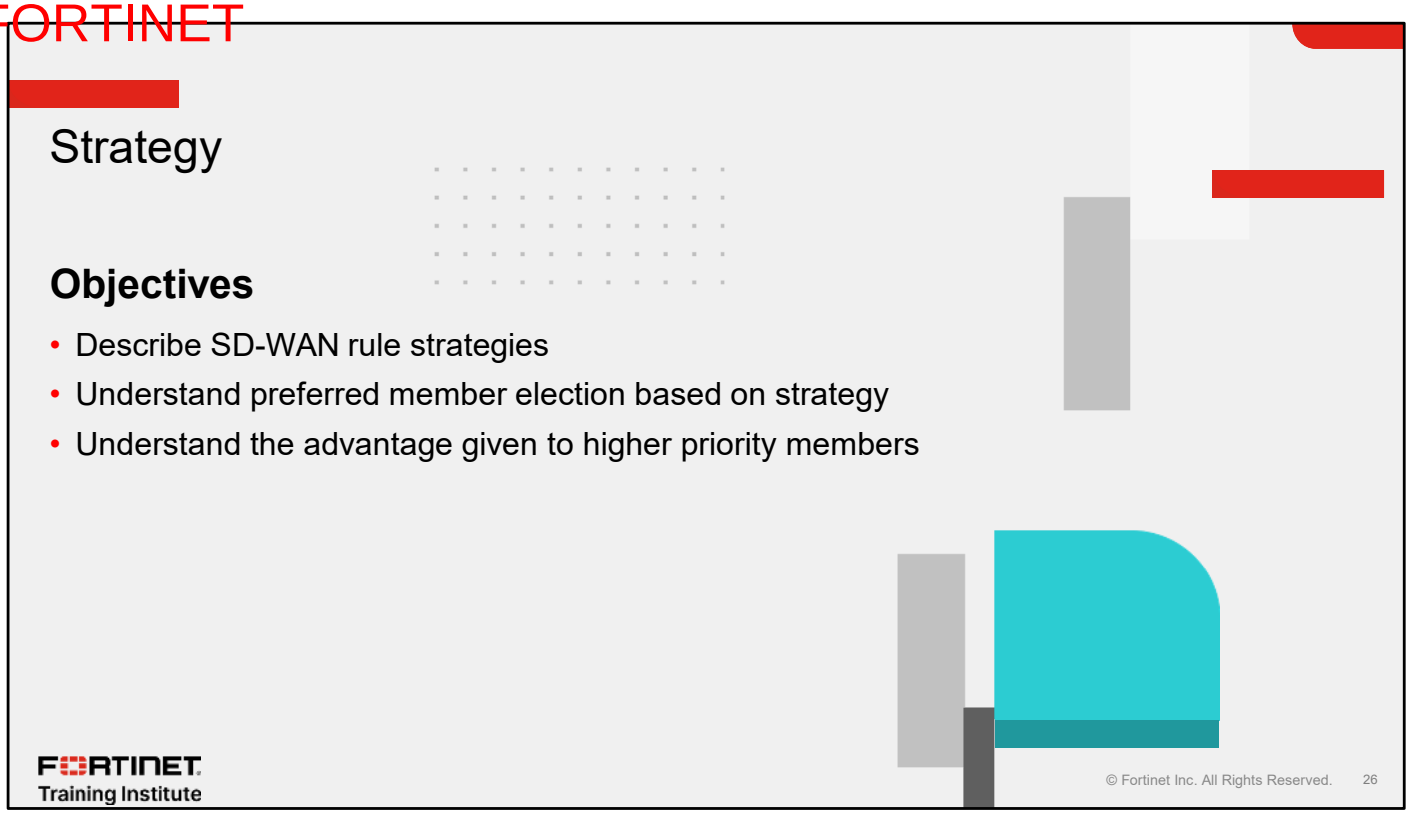
Consider the example on this slide, which shows some packets captured for an SSH session *without SNAT*. The packets are sent to different members before and after the application learning phase is completed. The expected member is `HUB1-VPN2`, but the packets are initially routed to `HUB1-VPN1` because the packet didn't match an entry in the cache. After the application is learned, FortiGate starts routing the packets to `HUB1-VPN2` and adds the 3-tuple to the cache. In addition, FortiGate routes new sessions that match the same 3-tuple in cache to `HUB1-VPN2` right from the start of the connection. Note that FortiGate updates the application database in batch every minute for every application learned over the past 60 seconds.

Also, remember that source network address translation (SNAT) conditions apply. That is, if a session is subject to SNAT, then, by default, FortiGate doesn't flush the routing information of the session after the application is detected—the session is not flagged as dirty. For example, if the SSH sessions shown on this slide were subject to SNAT, then the first session would remain routed through `HUB1-VPN1` even after FortiGate detects the application—unless the default FortiOS SNAT routing behavior is modified. However, subsequent sessions to the same 3-tuple would then be routed to `HUB1-VPN2`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding available SD-WAN rule strategies, you will be able to select and configure the best option to address your requirements.

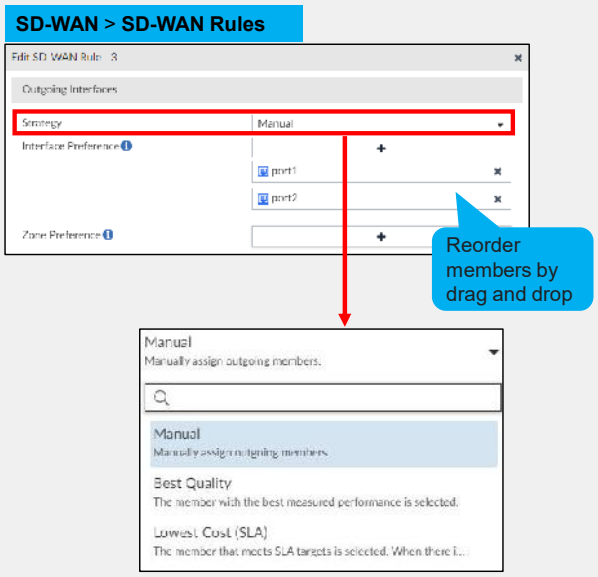


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Strategies

- Define:
  - Requirements for preferred members
- Preferred members:
  - Best candidates to steer traffic
  - Are used only if they have a valid route to the destination
- Member selection:
  - **Manual**:
    - Configuration order-based preference
  - **Best Quality**:
    - Best performing member based on quality criteria
  - **Lowest Cost (SLA)**:
    - Member that meets SLA target (tiebreakers: cost and configuration order)
- Load balancing:
  - By default, each strategy selects a single member
  - Load balancing option to distribute the traffic through multiple members




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

The strategy in a rule defines the requirements for preferred members, and whether the traffic is steered to one or more preferred members. The preferred members are the best members from the `oif` list—based on the strategy in use—that meet the SLA requirements (if applicable). The `oif` list sorts the configured members—**Interface Preference** list in FortiManager—by preference. That is, although the members are the same, their order in the `oif` list, and in **Interface Preference** list, can be different. There are three strategies you can chose from:

- **Manual**: FortiGate prefers members according to configuration order. Member metrics are not considered for member preference.
- **Best Quality:** FortiGate prefers the best-performing member based on the configured quality criteria.
- **Lowest Cost (SLA)**: FortiGate prefers the member that meets the configured SLA target. If multiple members meet the SLA target, member cost, followed by the configuration order, are used as tiebreakers.

You can combine the strategy **Manual** and **Lowest Cost (SLA)** with the **Load Balancing** option to instruct FortiGate to steer the traffic through multiple members. When you combine the strategy manual with the load balancing option, FortiGate distribute the traffic through all members that are up. When you combine load balancing with the lowest cost strategy, FortiGate distribute the traffic through all members that meet the SLA target.

Note that for all strategies, FortiGate must check that the preferred member has a valid route to the destination. If the member doesn't have a valid route, then FortiGate checks the next member in the `oif` list, and so on until it finds an acceptable member. Moreover, all strategies, except **Manual**, consider the member metrics for member preference.

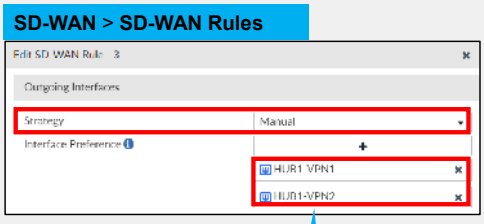


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Manual

- First member in the configuration that is alive is preferred
  - Metrics are not considered (packet-loss, latency, …)
  - Health-check configuration is optional
  - Single preferred member (by default)




```
# diagnose sys sdwan health-check status
Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(101.170), jitter(5.808), mos(4.34[illegible] bandwidth-
up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.420), jitter(0.289), mos(4.403)[illegible]andwidth-
up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3

# diagnose sys sdwan service4
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(2):
    1: Seq_num(4 HUB1-VPN1), alive, selected
    2: Seq_num(5 HUB1-VPN2), alive, selected
  Internet Service(1): Tableau-SSH(5111814,0,0,0)
  Src address(1):
       10.0.1.0-10.0.1.255
```

HUB1-VPN1 is preferred because it is alive and the first member configured in the list

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

When you use the manual strategy, FortiGate builds the `oif` list based on the **Interface Preference** list configuration order. For building the `oif` list, FortiGate does not consider the performance of the member, such as jitter or packet loss . It considers only the member configuration order—also known as the member configuration priority—and whether the member is alive or dead. If the first configured member is dead, then the preferred member becomes the next member in the configuration list that is alive.

Note that the manual strategy *does not* require the configuration of performance SLA. However, when a performance SLA rule is configured to monitor members, it improves the detection of whether a member is alive or dead, because a member is considered alive only if the health-check can reach at least one configured server. Without a health check, members are considered alive or dead according to the interface status (up or down).

In the example shown on this slide, `HUB1-VPN1` and `HUB1-VPN2` are the configured members. However, although `HUB1-VPN1` has a much higher latency than `HUB1-VPN2`, FortiGate still prefers `HUB1-VPN1` for steering traffic because it is alive and has the highest configuration priority.

Do not confuse the member *configuration priority*, or member configuration order, with the ***Priority*** setting available on the SD-WAN member configuration. The latter is used for the priority of static routes when you configure static routes for zones. The former refers to the member priority based on the **Interface Preference** list configuration. Members that are configured first in the list have higher priority over those configured last. The SD-WAN member **Priority** setting is used as a tiebreaker for ECMP routes when matching the implicit SD-WAN rule.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Manual (Contd)

- If HUB1-VPN1 is detected dead, HUB1-VPN2 becomes the preferred member

```
# diagnose sys sdwan health-check status

Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(dead), packet-loss(48.000%) sla_map=0x0
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(111.531), jitter(0.347
Health Check(test_HC):
Seq(5 HUB1-VPN2): state(dead) packet-loss(100.000%) sla_map=0x0


# diagnose sys sdwan service4

Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(2):
    1: Seq_num(5 HUB1-VPN2), alive, selected
    2: Seq_num(4 HUB1-VPN1), dead
  Internet Service(1): Tableau-SSH(5111014,0,0,0)
  Src address(1):
        10.0.1.0-10.0.1.255
```

Health checks are optional for manual rules
If configured, manual rules consider only the member state

Member is alive even if latency is out of SLA

Two health checks for HUB1-VPN2
Manual rules consider the member alive if at least one health check find it alive

HUB1-VPN2 is now the first member in the oif list

Dead members are moved to the bottom of the oif list

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

In the example shown on this slide, FortiGate detects HUB1-VPN1 as dead for the health-check HUB1_HC. HUB1_HC is the only health-check that monitor HUB1-VPN1, and as result, FortiGate moves HUB1-VPN2 to the top of the oif list by assigning it the sequence number 1, for the manual SD-WAN service rule ID 2. Note that HUB1-VPN1 is assigned the sequence number 2 because dead members are moved to the bottom of the list.

The administrator configured two health check to monitor the state of HUB1-VPN2: HUB1_HC and test_HC.

- FortiGate detects HUB1-VPN2 as dead for the health-check test_HC, and alive for the health check HUB1_HC. Because manual rules consider a member as alive if at least one health-check detect that member as alive, the service rule 2 placed HUB1-VPN2 at the top of the member list and use it to steer the traffic.
- The health check HUB1_HC detects a high latency for HUB1-VPN2; the detected latency (111.531) is above the SLA configured for this health check (100). As long as FortiGate can reach the health check server through a member, the state of the member is alive and it is available for manual rules. Remember that manual rules do not consider the link metric.

Note that FortiGate does not use a member to steer the traffic while it declares it *dead*. FortiGate continue monitoring the member status, sending probes if applicable, and will set it back *alive* when the interface is up and, if applicable, it receive probe replies. Not sending traffic to dead members apply to all traffic-steering strategies.

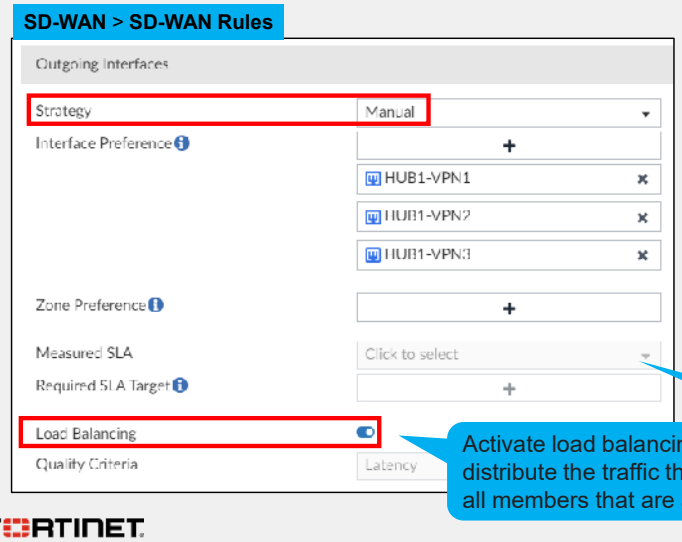


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Manual With Load Balancing

- Load balance sessions across all members
- Default load balancing method: round-robin




Activate load balancing to distribute the traffic through all members that are alive

- Differentiate manual modes on the CLI
  - Manual

```
# diagnose sys sdwan service4
...
  Gen(1)              ... Mode(manual)
  Members(2):
...
```

  - Manual with load balancing

```
# diagnose sys sdwan service4
...
 Gen(1)... Mode(manual  hash-mode=round-robin)
  Members(2):
...
```

No SLA definition for manual rules.
If the administrator configures health check, manual rules use them to determine the link status—alive or dead

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

You can combine the **Manual** strategy with the **Load Balancing** option. Those settings instruct FortiGate to distribute sessions across all available members. The available members are all members defined for the rule that are up. If you defined health check for the member, FortiGate distributes the traffic through all members that are alive, which means all members for which FortiGate can reach a least one health-check server. FortiGate does *not* consider the measured performances with manual strategies.

On the CLI, when you check the rule definition and status with the command `diagnose sys sdwan service4`, you can differentiate both modes as shown on this slide. When load balancing is enabled on the rule, FortiGate displays the selected hash modes—`round-robin` (default), `source-ip`, `source-dest-ip`, `inbandwidth`, `outbandwidth`, `bibandwidth`. You will learn more about each mode in this lesson.

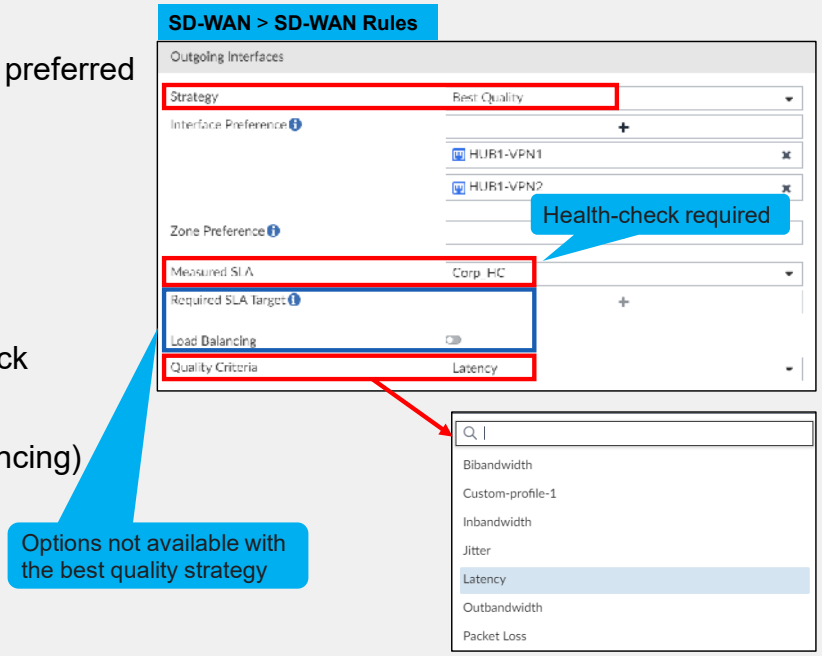


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Best Quality

- Member with best quality becomes preferred
- Multiple quality metrics available
  - Default: latency
- Factors considered for best quality:
  - Member configuration order
  - Link-cost threshold
  - Metric
- Measure quality with on health check
- SLA targets are not considered
- One member is used (no load balancing)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

The best quality strategy instructs FortiGate to select the member with the best measured quality as the preferred member. FortiGate supports multiple metrics to measure the link quality. The default metric is latency. For increased accuracy, FortiGate calculates the quality metric on the last few health-check probes (default 30).

FortiGate determines the member with the best quality using three factors: member configuration order, the `link-cost-threshold` setting, and the value of the metric measured for the member. SLA targets are not considered.

In addition, when you use the best quality strategy, FortiGate uses one member to steer traffic. You cannot combine the best quality strategy with the load balancing option.

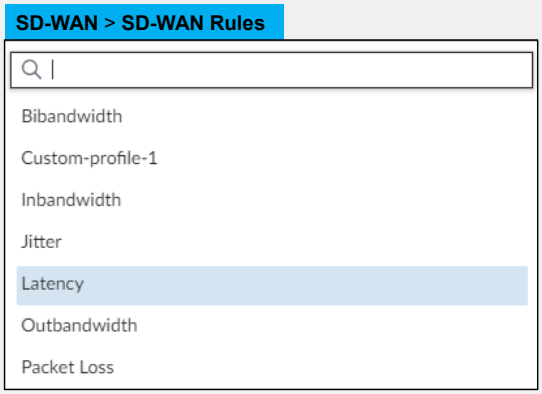


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Best Quality—Metrics

- **Latency** (default)
  - Lower latency, higher preference
- **Jitter**
  - Lower jitter, higher preference
- **Packet Loss**
  - Lower packet loss, higher preference
- Bandwidth:
  - More available bandwidth, higher preference
  - Three measurement options:
    - **Inbandwidth** (ingress)
    - **Outbandwidth** (egress)
    - **Bibandwidth** (bidirectional)
- **Custom-profile-1**
  - Weight-based calculation based on:
    - Latency, jitter, packet loss, and bibandwidth
    - Assign your own weights
  - Lower quality index, higher preference




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

This slide shows the metrics you can choose from to measure the quality of the members in a best quality rule.

For latency, jitter, and packet loss, the lower the metric value, the higher the member preference. The opposite is true for available bandwidth: The more available bandwidth a member has, the higher its preference. Note that FortiGate can measure the available ingress bandwidth, the available egress bandwidth, or the sum of both (bidirectional bandwidth).

When you select the **Custom-profile-1** metric, FortiGate uses a weight-based formula to calculate a value—called the link quality index—that represents the quality of the member based on its latency, jitter, packet loss, and available bidirectional bandwidth. The lower the link quality index, the higher the member preference. The administrator assigns the weight for each metric.

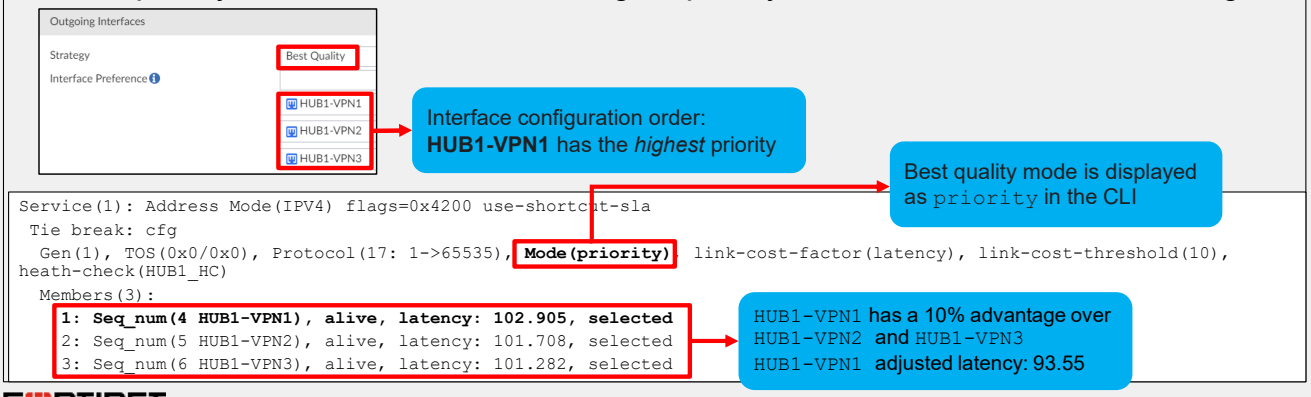


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Best Quality—Link Cost Threshold

- Advantage given to higher priority members
  - Logic: higher priority members have more preference
  - Prevents SLA changes due to slight metric variations
  - Default value: 10 (percentage)
  - Calculation varies among metrics
- Lower priority member is better than a higher priority member if it beats the advantage




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

In addition to the member metric value, FortiGate also considers the member configuration order and the `link-cost-threshold` value to determine the preferred member in a best quality rule. You can identify the preferred member by looking at the output of the `diagnose sys sdwan service4` command. The member that is placed on top of the list is the preferred member.

The `link-cost-threshold` value instructs FortiGate to give an advantage (or handicap) to higher priority members. The member priority is determined from the interface configuration order. Members that are configured first have higher priority over those configured below them. The logic behind `link-cost-threshold` is that higher priority members should have more preference than lower priority members. For this reason, for a lower priority member to be considered better than a higher priority member, the lower priority member must beat the advantage given to the higher priority member.

`link-cost-threshold` is also useful to prevent frequent SLA changes caused by slight variations in the metric, which would in turn result in more CPU activity caused by frequent session re-evaluation. The `link-cost-threshold` setting is expressed as a percentage, and its default value is 10.

The example on this slide shows the output of the `diagnose sys sdwan service4 command` for a rule that uses best quality (shown in the CLI as `priority`) as the strategy. `HUB1-VPN2` and `HUB1-VPN3` have lower latency than `HUB1-VPN1`, but because `link-cost-threshold` is set to `10`, then `HUB1-VPN1`—the *highest* priority member—has an advantage of 10% over other members configured in the rule. The 10% advantage results in an adjusted latency of 93.55 ms for `HUB1-VPN1`, which makes it the lowest latency among the members. For this reason, `HUB1-VPN1` becomes the preferred member.

The advantage is calculated differently depending on the metric in use.

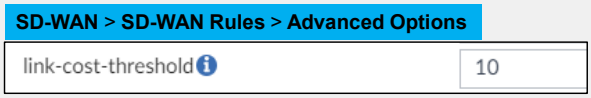


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Best Quality—Link Cost Threshold (Contd)

- Advanced option
  - SD-WAN rule advanced options parameter




- CLI configuration (default = `10`):

```
config system sdwan
    config service
        edit <id>
            set link-cost-threshold <threshold>
        next
    end
end
```

- If `link-cost-threshold` is set to `0`, then the metric comparison is strict
  - Use priority as tiebreaker

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

You can configure the `link-cost-threshold` parameter in the SD-WAN rule advanced options section on FortiManager or using a CLI parameter. This slide shows how to configure the setting using the FortiGate CLI.

If you set `link-cost-threshold` to **0**, then FortiGate performs a strict metric comparison. That is, there is no advantage, and the member with the best metric becomes the preferred. If two or more members have the same metric, FortiGate uses the member priority as the tiebreaker.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Best Quality—Latency, Jitter, and Custom-profile-1

- Objective:
  - Steer traffic to the member with the lowest metric (the advantage is considered)
- Adjusted metric (AM) formula (factors in the advantage):

AM = real metric / (1 + `link-cost-threshold`/100)

- Rules for building the `oif` list (`link-cost-threshold` > 0):
  - A higher priority member (HPM) has advantage over a lower priority member (LPM)
  - An LPM is placed on top of an HPM when its metric is lower than the AM of the HPM
  - An LPM is placed again below an HPM when any of the following occurs:
    - The LPM metric is equal to or higher than the AM of the *highest* priority member (quick recovery)
    - The LPM metric is equal to or higher than the HPM (longer recovery)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

In you configure best quality as the strategy, the way FortiGate determines the preferred member depends on the metric in use. However, for latency, jitter, and custom-profile-1, the method is the same.

When you use latency, jitter, or custom-profile-1 as the metric, FortiGate selects as the preferred member the member with the lowest metric. If `link-cost-threshold` is set to a value higher than zero, FortiGate calculates the adjusted metric (AM) for higher priority members, which factors in the advantage given to them. FortiGate uses the formula shown on this slide to calculate the AM.

This slide shows the rules that FortiGate follows when building the `oif` list. Do not confuse the **Interface Preference** configuration list of a rule with its `oif` list. The latter is dynamic and depends on the member performance. The former refers to the order of the interfaces in the configuration. The rules are the following:

- A higher priority member (HPM) has advantage over a lower priority member (LPM). The advantage depends on the `link-cost-threshold` value.
- An LPM is placed on top of an HPM when its metric is less than the AM of the HPM.
- An LPM is placed again below an HPM when any of the following occurs:
  - The LPM metric is equal to or higher than the AM of the *highest* priority member. This allows for a quick recovery of the *highest* priority member.
  - The LPM metric is equal to or higher than the HPM. This results in a longer recovery of the HPM.

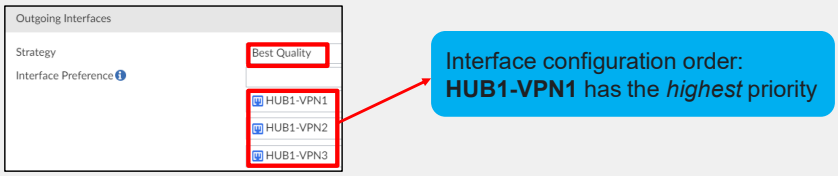


Vouchers & Dumps are Available | WhatsApp +201224560923

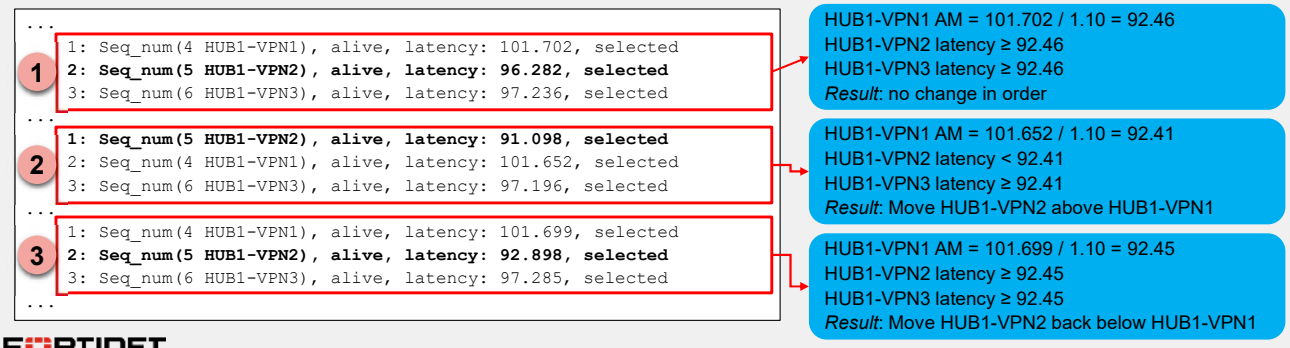
DO NOT REPRINT Brave-dumps.com
© FORTINET

# Best Quality Member—Latency Example 1

- Configuration (Quality Criteria = **Latency**, `link-cost-threshold` = `10`):




- Moving up and down the list (*highest* priority member vs LPM):




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

This slide shows an example of the preferred member election in a best quality rule that uses **Latency** as the metric. For jitter and custom-profile-1 metrics, the same behavior applies.

The configuration shows **HUB1-VPN1** as the *highest* priority member. This slide also shows the output of the `diagnose sys sdwan service4` command taken at different times. Note that only relevant lines of the output are displayed. The example shows how a member competes with the *highest* priority member for a position in the `oif` list.

Focus on the position of HUB1-VPN2 in the list compared to HUB1-VPN1. In the first output, HUB1-VPN2 is placed below HUB1-VPN1 even though it has the lowest real latency among members. This is because FortiGate calculates an adjusted metric (AM) for HUB1-VPN1. The adjusted latency for HUB1-VPN1 is 92.46 milliseconds, which makes it the actual lowest latency among all members, which is why FortiGate selects HUB1-VPN1 as the preferred member.

In the second output, HUB1-VPN2 now becomes the preferred member because its latency is now less than the adjusted latency of HUB1-VPN1. In the third output, HUB1-VPN2 is moved back below HUB1-VPN1 because its latency is again equal to or greater than the adjusted latency of HUB1-VPN1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Best Quality Member—Latency Example 2

- Moving up and down the list (HPM vs LPM):

```
...
1: Seq_num(4 HUB1-VPN1), alive, latency: 101.661, selected
2: Seq_num(5 HUB1-VPN2), alive, latency: 121.462, selected
3: Seq_num(6 HUB1-VPN3), alive, latency: 110.847, selected
...
1: Seq_num(4 HUB1-VPN1), alive, latency: 101.667, selected
2: Seq_num(6 HUB1-VPN3), alive, latency: 109.863, selected
3: Seq_num(5 HUB1-VPN2), alive, latency: 121.464, selected
...
1: Seq_num(4 HUB1-VPN1), alive, latency: 101.785, selected
2: Seq_num(6 HUB1-VPN3), alive, latency: 121.270, selected
3: Seq_num(5 HUB1-VPN2), alive, latency: 121.491, selected
...
1: Seq_num(4 HUB1-VPN1), alive, latency: 101.568, selected
2: Seq_num(5 HUB1-VPN2), alive, latency: 121.396, selected
3: Seq_num(6 HUB1-VPN3), alive, latency: 121.565, selected
...
```

1. HUB1-VPN2 AM = 121.462 / 1.10 = 110.42
   HUB1-VPN3 latency ≥ 110.42
   *Result*: no change in order
2. HUB1-VPN2 AM = 121.464 / 1.10 = 110.42
   HUB1-VPN3 latency < 110.42
   *Result*: Move HUB1-VPN3 above HUB1-VPN2
3. Don't consider AM
   HUB1-VPN3 latency < HUB1-VPN2 latency
   *Result*: no change in order
4. Don't consider AM
   HUB1-VPN3 latency ≥ HUB1-VPN2 latency
   *Result*: Move HUB1-VPN3 back below HUB1-VPN2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

This slide shows another example of the preferred member election in a best quality rule that uses latency as the metric. The configuration is the same as the one shown on the previous slide. The example shows how members other than the *highest* priority member, compete for a position in the `oif` list.

Focus on the position of HUB1-VPN3 in the list compared to HUB1-VPN2. In the first output, HUB1-VPN3 is placed below HUB1-VPN2 even though HUB1-VPN3 has a lower latency. This is because FortiGate considers the adjusted latency (AM) for HUB1-VPN2, which is 110.42 ms and equal to or lower than the real latency of HUB1-VPN3.

In the second output, HUB1-VPN3 is now placed on top of HUB1-VPN2 because its latency is now lower than the adjusted latency of HUB1-VPN2. In the third output, HUB1-VPN3 is still placed on top of HUB1-VPN2 even though its latency is no longer lower than the adjusted latency of HUB1-VPN2. This is because FortiGate doesn't consider the advantage when moving a lower priority member back down the interface list. That is, FortiGate considers only the members' real latency and priority.

In the fourth output, HUB1-VPN3 is now moved back below HUB1-VPN2 because its latency is now equal to or higher than the real latency of HUB1-VPN2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Best Quality—Bandwidth

- Objective:
  - Steer traffic to the member with the *highest* available bandwidth
  - Available bandwidth (AvBW) is based on interface settings and usage
- Adjusted bandwidth difference (ABWD) formula (factors in the advantage):

ABWD = LPM AvBW * `link-cost-threshold`/100

- Available bandwidth difference (AvBWD) formula:

AvBWD = LPM AvBW – HPM AvBW

- Rules for building the `oif` list (`link-cost-threshold` > 0):
  - A higher-priority member (HPM) has advantage over a lower-priority member (LPM)
    - Higher priority, higher preference
  - An LPM is placed on top of an HPM when the AvBWD is higher than the ABWD
  - An LPM is placed again below an HPM when any of the following occurs:
    - The AvBWD is equal to or lower than the ABWD (quick recovery)
    - The AvBW of LPM is equal to or lower than the AvBW of the HPM (longer recovery)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

When you use inbandwidth, outbandwidth, or bibandwidth as the metric, FortiGate selects the member with the *highest* available bandwidth as the preferred member. The available bandwidth depends on the interface settings and usage.

If you set the `link-cost-threshold` to a value higher than zero, FortiGate calculates the adjusted bandwidth difference for lower-priority members, which factors in the advantage given to the higher-priority members and is calculated using the formula shown on this slide. The formula is a basic percentage calculation of the available bandwidth of the lower priority member based on the `link-cost-threshold` setting.

FortiGate also calculates the difference in available bandwidth between a lower-priority member and a higher-priority member using the formula shown on this slide.

This slide also shows the rules that FortiGate follows to build the `oif` list using bandwidth as the metric. The rules are the following:

- A higher-priority member (HPM) has advantage over a lower-priority member (LPM). The advantage depends on the `link-cost-threshold` value.
- An LPM is placed on top of an HPM when the available bandwidth difference is higher than the adjusted bandwidth difference.
- An LPM is placed again below an HPM when any of the following occurs:
  - The available bandwidth difference is equal to or lower than the adjusted bandwidth difference. This allows for a quick recovery of the *highest* priority member.
  - The available bandwidth of the LPM is equal to or lower than the available bandwidth of the HPM. This results in a longer recovery for the HPM.

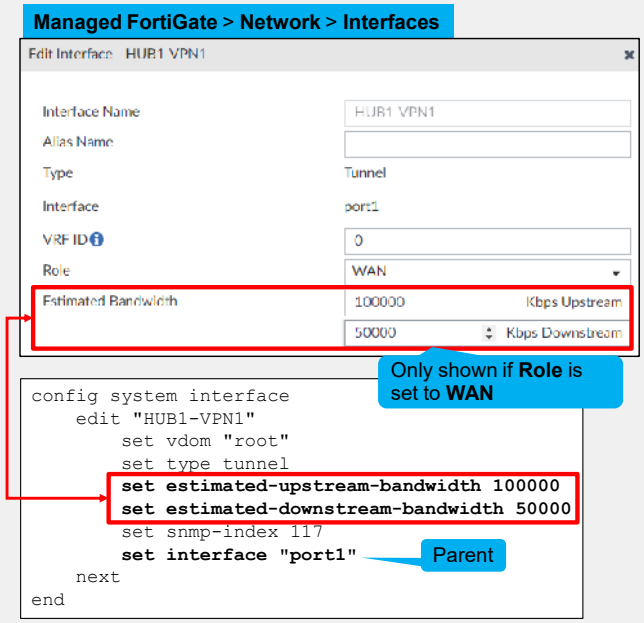


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Best Quality—Member Maximum Bandwidth

- FortiGate requires maximum bandwidth for members
  - Manually defined using `estimated-upstream-bandwidth` and `estimated-downstream-bandwidth`
  - Or automatically obtained from:
    - Physical speed (physical interfaces)
    - Parent interfaces (VLAN and tunnel interfaces)
      - Use parent physical speed as last resource
  - The bibandwidth metric uses the sum of upstream and downstream bandwidth




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

When you use a bandwidth metric in a best quality rule, FortiGate must know the maximum bandwidth of the members to calculate their available bandwidth.

The maximum bandwidth of a member is obtained from the values defined for the `estimated-upstream-bandwidth` and `estimated-downstream-bandwidth` interface settings. If the settings are not defined, then FortiGate uses the actual physical interface speed. For example, for a 100 Mbps interface with undefined maximum bandwidth settings, FortiGate resolves to use 100 Mbps for both upstream and downstream maximum speeds. For the bidirectional bandwidth metric, FortiGate just adds the upstream and downstream speeds.

For VLAN and tunnel interfaces with undefined maximum bandwidth settings, FortiGate resolves to use the bandwidth values of the parent interfaces. For example, an IPsec tunnel that is bound to port1 and that has undefined maximum bandwidth settings obtains its maximum bandwidth from port1 settings. If port1 has no maximum bandwidth values defined, then the IPsec tunnel uses the physical speed of port1.

The example on this slide shows the maximum bandwidth settings on FortiManager, and the equivalent CLI settings on FortiGate. Note that FortiManager displays the maximum bandwidth settings only if you select **WAN** as the interface **Role**.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Best Quality—Member Available Bandwidth

- Outbandwidth example:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(priority), link-cost-factor(outbandwidth), link-cost-threshold(10),
heath-check(HUB1_HC)
  Members(2):
    1: Seq_num(4 HUB1-VPN1), alive, outbandwidth: 99995Kbps  selected
    2: Seq_num(5 HUB1-VPN2), alive, outbandwidth: 99995Kbps  selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

Available bandwidth

- Bibandwidth example:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(priority), link-cost-factor(bibandwidth), link-cost-threshold(10),
heath-check(HUB1_HC)
  Members(2):
    1: Seq_num(4 HUB1-VPN1), alive, bibandwidth: 149980Kbps  selected
    2: Seq_num(5 HUB1-VPN2), alive, bibandwidth: 149980Kbps  selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

This slide shows sample outputs for the `diagnose sys sdwan service4` command when using outbandwidth and bibandwidth as metrics. Note that the bandwidth value displayed in the output refers to the available bandwidth.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Best Quality—Bandwidth Used by Member

- Available bandwidth:

```
# diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(bibandwidth), link-cost-threshold(10),
heath-check(HUB1_HC)
  Members(2):
    1: Seq_num(4 HUB1-VPN1), alive, bibandwidth: 139234Kbps  selected
    2: Seq_num(5 HUB1-VPN2), alive, bibandwidth: 149997Kbps  selected
  Src address(1):
        0.0.0.0-255.255.255.255
  Dst address(1):
        10.1.0.7-10.1.0.7
```

Available bandwidth is updated every 10 seconds

- Used bandwidth:

```
# diagnose sys link-monitor interface HUB1-VPN1
Interface(HUB1-VPN1): state(up, since Tue Sep 03 08:44:45 2024), bandwidth(up:519189bps, down:15097bps), session
count(IPv4:63, IPv6:0), tx(24754785 bytes), rx(23261162 bytes), latency(2.08), jitter(0.49), packet-loss(0.00).

# diagnose sys link-monitor interface HUB1-VPN2
Interface(HUB1-VPN2): state(up, since Tue Sep 03 08:44:45 2024), bandwidth(up:4769bps, down:15097bps), session
count(IPv4:2, IPv6:0), tx(13157864 bytes), rx(23640548 bytes), latency(1.91), jitter(0.41), packet-loss(0.00).
```

Used bandwidth

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 41

The available bandwidth displayed by the `diagnose sys sdwan service4` command is updated every 10 seconds based on the used bandwidth and the maximum bandwidth of the member.

The used bandwidth is measured by the link monitor process (`lnkmtd`), and you can view the measured values by running the `diagnose sys link-monitor interface` command, as shown on this slide.

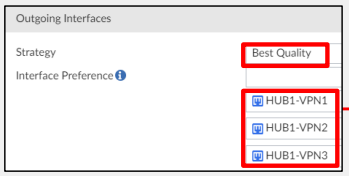


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Best Quality Member—Bandwidth Example 1

- Configuration (Quality Criteria = **Outbandwidth**, `link-cost-threshold` = `10`)




Interface configuration order; **HUB1-VPN1** has the *highest* priority

- Moving up and down the list (*highest* priority member vs LPM):

```
...
1: Seq_num(4 HUB1-VPN1), alive, outbandwidth: 9100Kbps, selected
2: Seq_num(5 HUB1-VPN2), alive, outbandwidth: 9999Kbps, selected
3: Seq_num(6 HUB1-VPN3), alive, outbandwidth: 4999Kbps, selected
...
1: Seq_num(5 HUB1-VPN2), alive, outbandwidth: 9999Kbps, selected
2: Seq_num(4 HUB1-VPN1), alive, outbandwidth: 8999Kbps, selected
3: Seq_num(6 HUB1-VPN3), alive, outbandwidth: 4999Kbps, selected
...
1: Seq_num(4 HUB1-VPN1), alive, outbandwidth: 9000Kbps, selected
2: Seq_num(5 HUB1-VPN2), alive, outbandwidth: 9999Kbps, selected
3: Seq_num(6 HUB1-VPN3), alive, outbandwidth: 4999Kbps, selected
...
```

1. ABWD = 999.9
   AvBWD = 9999 – 9100 = 899
   AvBWD ≤ ABWD
   *Result*: no change in order
2. ABWD = 999.9
   AvBWD = 9999 – 8999 = 1000
   AvBWD > ABWD
   *Result*: Move HUB1-VPN2 above HUB1-VPN1
3. ABWD = 999.9
   AvBWD = 9999 – 9000 = 999
   AvBWD ≤ ABWD
   *Result*: Move HUB1-VPN2 back below HUB1-VPN1

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 42

This slide shows an example of the preferred member election in a best quality rule that uses **Outbandwidth** as the metric.

The configuration shows HUB1-VPN1 as the *highest* priority member. This slide also shows the output of the `diagnose sys sdwan service4` command taken at different times. Note that only relevant lines of the output are displayed. The example shows how a member competes with the *highest* priority member for a position in the `oif` list.

Focus on the position of HUB1-VPN2 in the list compared to HUB1-VPN1. In the first output, HUB1-VPN2 is placed below HUB1-VPN1 even though it has more available bandwidth. This is because FortiGate considers the adjusted available bandwidth difference. The ABWD is 999.9 kbps, while the AvBWD is 899 kbps. Because AvBWD is equal to or lower than the ABWD, then the higher priority member (HUB1-VPN1) is considered better.

In the second output, HUB1-VPN2 now becomes the preferred member because the AvBWD is now higher than the ABWD. In the third output, HUB1-VPN2 is moved back below HUB1-VPN1 because the AvBWD is again equal to or lower than the ABWD.

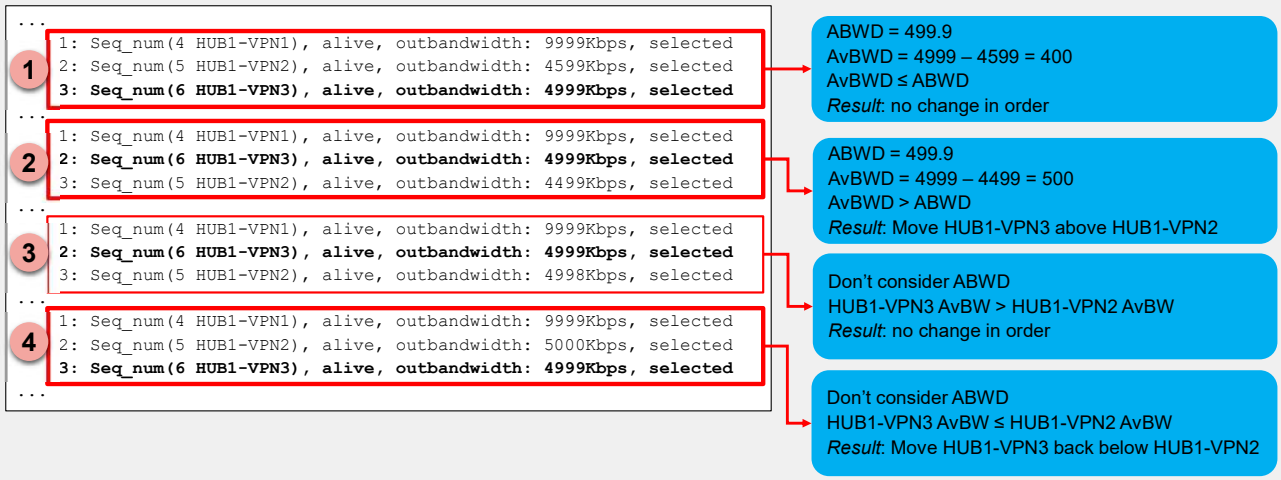


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Best Quality Member—Bandwidth Example 2

- Moving up and down the list (HPM vs LPM):




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

This slide shows another example of the preferred member election in a best quality rule that uses outbandwidth as the metric. The configuration is the same as the one shown on the previous slide. The example shows how members other than the *highest* priority member, compete for a position in the list.

Focus on the position of HUB1-VPN3 in the list compared to HUB1-VPN2. In the first output, HUB1-VPN3 is placed below HUB1-VPN2 even though it has more available bandwidth (AvBW). This is because FortiGate considers the adjusted available bandwidth difference (ABWD). The ABWD is 499.9 kbps, while the AvBWD is 400 kbps. Because AvBWD is equal to or lower than the ABWD, then the higher priority member (HUB1-VPN2) is considered better.

In the second output, HUB1-VPN3 is now placed on top of HUB1-VPN2 because the AvBWD is now higher than the ABWD. In the third output, HUB1-VPN3 is still placed on top of HUB1-VPN2 even though the AvBWD is no longer higher than the ABWD. This is because FortiGate doesn't consider the ABWD when moving a lower priority member back down the interface list. That is, FortiGate prefers the member with the *highest* available bandwidth.

In the fourth output, HUB1-VPN3 is now moved back below HUB1-VPN2 because the available bandwidth is now equal to or lower than HUB1-VPN2.



Vouchers & Dumps are Available | WhatsApp +201224560923

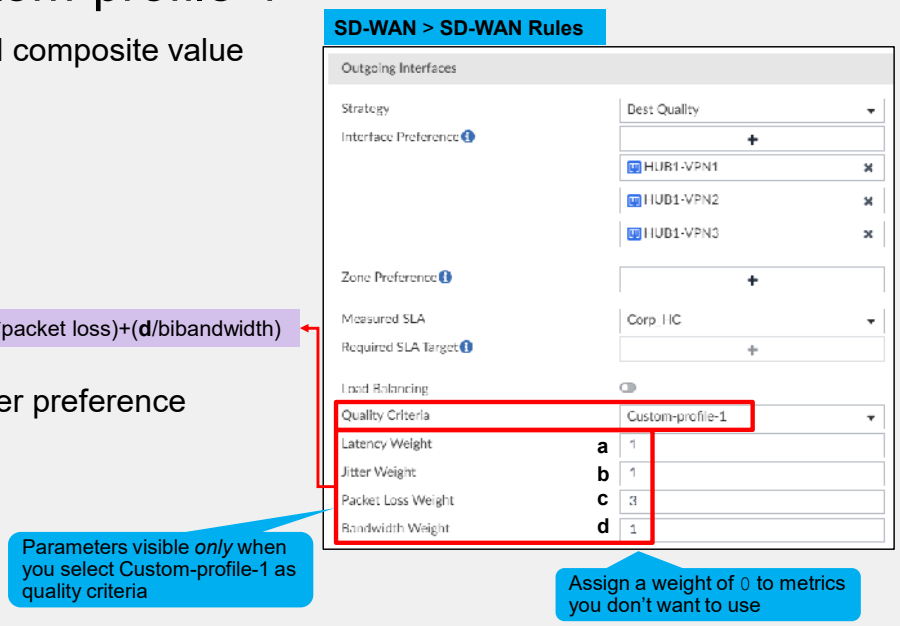
DO NOT REPRINT Brave-dumps.com
© FORTINET

## Best Quality—Custom-profile-1

- Link quality is a weight-based composite value of:
  - Latency
  - Jitter
  - Packet loss
  - Bibandwidth
- Formula:

Link quality index = (**a***latency)+(**b***jitter)+(**c***packet loss)+(**d**/bibandwidth)

- Lower link quality index, higher preference




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

The custom-profle-1 metric uses a formula that calculates a composite value out of the latency, jitter, packet loss, and bibandwidth. The composite value is called the link quality index, and the formula to calculate it is shown on this slide.

For each metric, you set the weight to use in the formula. The weight enables you to influence the link quality index by one or more metrics. The higher the metric weight, the more influence the metric has on the link quality index. For example, if you consider packet loss the most important metric, then you should assign the highest weight to it. On the contrary, if you just want to ignore a metric, assign it a weight of `0`.

In the example shown on this slide, the link quality index considers all four metrics. However, packet loss has the highest weight among the four.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Best Quality—Custom-profile-1 (Contd)

- Custom-profile-1 example:

```
# diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(10), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(custom-profile-1),
link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1), alive, custom1: 1,891: 0.000% 1.531 0.360 20460Kbps, selected
    2: Seq_num(5 HUB1-VPN2), alive, custom1: 1,743: 0.000% 1.342 0.401 20460Kbps, selected
    3: Seq_num(6 HUB1-VPN3), alive, custom1: 7,313: 2.000% 1.013 0.300 19999980Kbps, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

Link quality index

Packet loss, latency, jitter, and bibandwidth

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 45

This slide shows a sample output for the `diagnose sys sdwan service4` command when using custom-profile-1 as the metric. The output includes the link quality index value, followed by the measured values for packet loss, latency, jitter, and bidirectional bandwidth.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA)

- Most common strategy when link quality matter
- Factors considered for preferred member:
  - SLA targets
    - The more SLA targets a member meets, the higher its preference
  - Member cost
    - Retrieved from member configuration
  - Member configuration order
    - Based on the rule interface preference configuration
- Optional load balancing
  - Disabled (default)
    - Single preferred member
  - Enabled
    - Distribute the traffic between acceptable members




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 46

The lowest cost (SLA) strategy instructs FortiGate to select the preferred member based on the following factors:

- SLA target: You must select one or more SLA targets. FortiGate then checks whether the members meet the selected SLA targets.
- Member cost: The cost that you configured for the member. The default cost for members is zero. FortiGate considers the cost with the logic: the lower the member cost, the higher its preference.
- Member configuration order: Based on the rule **Interface Preference** configuration. Members that are configured first have higher priority over those configured last.

FortiGate first checks how many SLA targets a member meets. The more SLA targets it meets, the higher its preference. Note that even though you can select one or more SLA targets in a rule, each selected SLA target must be from a different performance SLA. That is, each SLA target must point to a different server.

If there are two or more members that meet the same number of SLA targets, then FortiGate uses the member cost as the tiebreaker, and then the member priority as the last tiebreaker.

By default, one member only—the preferred member (if acceptable)—is used to steer traffic. That is, no load balancing is performed. Also, if none of the members meet the SLA target, as long as the members are alive, FortiGate builds the `oif` list based on members cost and configuration order. When you enable the **Load Balancing** option, FortiGate distributes the traffic through all members that meet the SLA requirements.

The lowest cost (SLA) strategy allows the administrator to fine tune what is considered a good link and limits the risk of too frequent link changes. For these reasons, administrators usually prefer this strategy to the best quality strategy.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Lowest Cost (SLA) Member—Example 1

- Rule configuration:



Interface configuration order:
**HUB1-VPN1** has the *highest* priority

- Member configuration order as tiebreaker:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0) selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0) selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0) selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

Lowest Cost (SLA) mode is displayed as `(sla), sla-compare-order` in the CLI

SLA map

- All members meet SLA target (**HUB1_HC#1**) and have the same cost (`0`)
- Use priority (`cfg_order`) as tiebreaker
- Resulting order: 1: HUB1-VPN1
  2: HUB1-VPN2
  3: HUB1-VPN3

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 47

This slide shows an example of the preferred member election in a lowest cost (SLA) rule.

The configuration shows **HUB1-VPN1** as the *highest* priority member. The output of the `diagnose sys sdwan service4` command shows `sla(0x1)` for all members. This means that all members meet the SLA target (**HUB1_HC#1**).

Because all members meet the SLA target and have the same cost, then the member configuration order is used as the tiebreaker. The result is that the members are ordered in the same way they are configured and, therefore, HUB1-VPN1 becomes the preferred member.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Understand SLA Target Maps—Two SLA Targets

- `sla_map` uses a bitmask to reference SLA targets and indicates their status
  - The `sla_map` value represents the hexadecimal value of a binary number
  - Number of bits = number of configured SLA targets
  - First configured SLA target is assigned bit 0, second configured SLA target bit 1, and so on
  - Bit of SLA target is set to 1 if met, otherwise to 0
- Possible `sla_map` values for two SLA targets:

| `sla_map (hex)` | SLA Target #2 (Bit 1) Value = $2^1 = 2$ | SLA Target #1 (Bit 0) Value = $2^0 = 1$ |
|---|---|---|
| `0x3` | Pass (1) | Pass (1) |
| `0x2` | Pass (1) | Fail (0) |
| `0x1` | Fail (0) | Pass (1) |
| `0x0*` | Fail (0) | Fail (0) |

* Also means that there are no SLA targets configured

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 48

With the previous strategy description, lowest cost (SLA), you discovered the `sla_map` field in the output of the `diagnose sys sdwan health-check status` command. This field indicates whether the member meets the configured SLA targets or not. The `sla_map` field uses a bitmask representation to reference the SLA targets and their status. Follow these rules to understand the `sla_map` field:

- The `sla_map` value represents the hexadecimal value of a binary number.
- The number of bits in the binary number equals the number of configured SLA targets.
- The first configured SLA target is assigned bit 0, the second configured SLA target bit 1, and so on.
- If the member meets the SLA target, the bit of the SLA target is set to 1, otherwise to 0.

This slide shows a table with all the possible `sla_map` values when you configure two SLA targets for a member. For example, an `sla_map` of `0x2` means that SLA targets 2 is met, but not SLA target 1 (2 = 2 + 0). In the lab exercises you will practice with SD-WAN rules configured with two SLAs. The table on this slide show the `sla_map` values that you can expect.

Note that an `sla_map` of `0x0` has two possible meanings. If you configure one or more SLA targets for a member, `0x0` means that none of the SLA targets are met. However, `0x0` can also mean that you didn't configure any SLA target for the member. Therefore, make sure to check the performance SLA configuration to identify whether there are SLA targets configured or not.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Understand SLA Target Maps—Three SLA Targets

- Possible `sla_map` values for three SLA targets:

| sla_map (hex) | SLA Target #3 (Bit 2) Value = $2^2$ = 4 | SLA Target #2 (Bit 1) Value = $2^1$ = 2 | SLA Target #1 (Bit 0) Value = $2^0$ = 1 |
|---|---|---|---|
| 0x7 | Pass (1) | Pass (1) | Pass (1) |
| 0x6 | Pass (1) | Pass (1) | Fail (0) |
| 0x5 | Pass (1) | Fail (0) | Pass (1) |
| 0x4 | Pass (1) | Fail (0) | Fail (0) |
| 0x3 | Fail (0) | Pass (1) | Pass (1) |
| 0x2 | Fail (0) | Pass (1) | Fail (0) |
| 0x1 | Fail (0) | Fail (0) | Pass (1) |
| 0x0* | Fail (0) | Fail (0) | Fail (0) |

* Also means that there are no SLA targets configured

- Each lowest cost (SLA) rule supports multiple SLA targets
  - A same rule accepts only one target for each test server
- Multiple rules can use the same SLA target

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 49

This slide shows a table with all the possible `sla_map` values when you configure three SLA targets for a member. For example, an `sla_map` of `0x6` means that SLA targets 3 and 2 are met, but not SLA target 1 (6 = 4 + 2 + 0). Expand or reduce the table according to the number of SLA targets configured in your setup.

You configure multiple SLA targets for a single test server, and you can configure SLA targets associated to different test servers. However, each lowest cost (SLA) rule accepts only one SLA target for each server. If you want to associate multiple SLA targets to one rule, each must point to a different test server.

You can use the same SLA target for multiple rules, and if you configured multiple targets for one server, you can associate each of them to a different rule.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA) Member—Example 2

- Member cost as tiebreaker:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(5), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(6 HUB1-VPN3), alive, sla(0x1)  gid(0), cfg_order(2), local cost(1), selected
    2: Seq_num(5 HUB1-VPN2), alive, sla(0x1)  gid(0), cfg_order(1), local cost(2), selected
    3: Seq_num(4 HUB1-VPN1), alive, sla(0x0)  gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

- HUB1-VPN1 doesn't meet the SLA target and is placed last in the list
- HUB1-VPN3 is better than HUB1-VPN2 because it has a lower cost
- Resulting order: 1: HUB1-VPN3
  2: HUB1-VPN2
  3: HUB1-VPN1

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 50

This slide shows another example of the preferred member election in a lowest cost (SLA) rule.

HUB1-VPN1 doesn't meet the SLA target—reported as sla(0x0), which is why it is placed at the bottom of the list. HUB1-VPN3 and HUB1-VPN2 meet the SLA target. However, HUB1-VPN3 is placed on top because it has a lower cost (1) than HUB1-VPN2 (2). The result is that HUB1-VPN3 becomes the preferred member.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA) Member—Example 3

- All members fail the SLA target:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(21), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
Members(3):
    1: Seq_num(4 HUB1-VPN1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3), alive, sla(0x0), gid(0), cfg_order(2), local cost(1), selected
    3: Seq_num(5 HUB1-VPN2), alive, sla(0x0), gid(0), cfg_order(1), local cost(2), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

- None of the members meet the SLA target
- Choose preferred member (HUB1-VPN1) based on cost and `cfg_order`
- Resulting order: 1: HUB1-VPN1
  2: HUB1-VPN3
  3: HUB1-VPN2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 51

This slide shows another example of the preferred member election in a lowest cost (SLA) rule.

None of the members meet the SLA target. Therefore, FortiGate determines the best egress member based on:

- First, the interface configured cost—the member with the lowest value takes precedence.
- Then the configuration order, which determines the priority if two members have the same cost.

In this example, FortiGate places HUB1-VPN1—`cfg_order(0)`, the *highest* priority member according to the configuration order—is placed on the top of the list because it's local cost is zero (0), then HUB1-VPN3 (cost=1) and HUB1-VPN2 (cost=2).



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Lowest Cost (SLA) Member—Example 4

- Rule configuration with two SLA targets:




- Only HUB1-VPN3 meets both SLA targets:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(7), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(6 HUB1-VPN3), alive, sla(0x3), gid(0), cfg_order(2), local cost(0), selected
    2: Seq_num(4 HUB1-VPN1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2), alive, sla(0x2), gid(0), cfg_order(1), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-
```

**SLA map**
(0x3) match both
(0x1) match target 1
(0x2) match target 2
*(0x0) no target match*

- Only HUB1-VPN3 meets both SLA targets (**HUB1_HC#1** and **Corp_HTTP#1**)
- Use `cfg_order` as tiebreaker for HUB1-VPN1 and HUB1-VPN2
- Resulting order: 1: HUB1-VPN3
  2: HUB1-VPN1
  3: HUB1-VPN2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 52

This slide shows an example of the preferred member election in a lowest cost (SLA) rule when two SLA targets are used.

Because HUB1-VPN3 is the only member that meets both SLA targets, it becomes the preferred member. Both HUB1-VPN1 and HUB1-VPN2, meet only one SLA target, and both have the same cost, therefore FortiGate uses the `cfg_order` as the tiebreaker between the two of them.

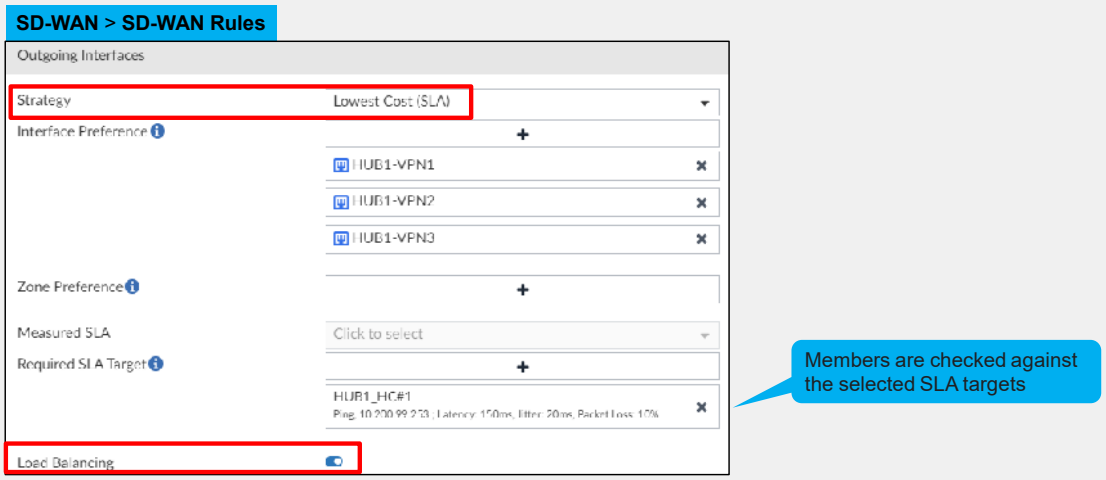


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA) With Load Balancing

- Load balance sessions across all members that satisfy the SLA targets
- Default load balancing method: round-robin




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 53

When you enable the **Load Balancing** option with the **Lowest Cost (SLA)** strategy, FortiGate distributes sessions across preferred members. Member preference is based on the number of SLA targets that members meet. That is, members that meet the most SLA targets are preferred and are therefore used for session distribution.

After FortiGate identifies the preferred members, it load balances sessions across the members. Note that FortiGate doesn't consider the member cost, priority, and configuration order. FortiGate considers only the number of SLA targets the member meets.

This strategy replaces the maximize bandwidth (SLA) strategy that was available with FortiGate versions prior to 7.4.1. On upgrade, FortiGate converts any SD-WAN rule defined with the maximize bandwidth (SLA) strategy to a rule defined with the strategy lowest cost (SLA) and the load balancing option enabled. Therefore, the upgrade does not modify the rule behavior.



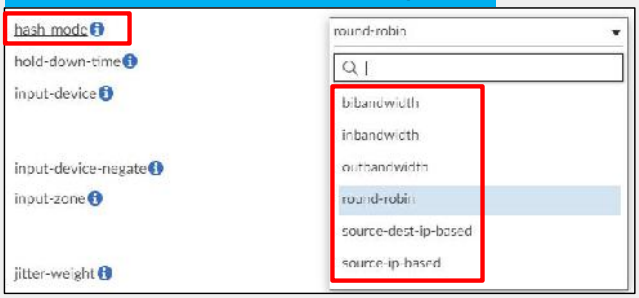
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Load Balancing Methods

- Define how FortiGate distributes sessions across selected members
  - `round-robin` (default): Equal and circular distribution
  - `source-ip-based`: Traffic from a source IP address is sent to the same member
  - `source-dest-ip-based`: Traffic from a source IP address to a destination IP address is sent to the same member
  - `Inbandwidth`: Use member with the most available incoming bandwidth
  - `Outbandwidth`: Use member with the most available outgoing bandwidth
  - `Bibandwidth`: Use member with the most available bidirectional bandwidth

**SD-WAN > SD-WAN Rules > Advanced Options**




```
config system sdwan
    config service
        edit <id>
            set load-balance enable
            set mode <manual | sla>
            set hash-mode <select mode>
        next
    end
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 54

For strategies that allow load balancing—**Manual** and **Lowest Cost (SLA)**—FortiGate load balances sessions across the members using one of the following algorithms:

- `round-robin`: This is the default algorithm. FortiGate load balances sessions across members equally using a circular distribution.
- `source-ip-based`: FortiGate sends sessions sourced from an IP address to the same member.
- `source-dest-ip-based`: FortiGate sends sessions with the same source and destination IP address pair to the same member.
- `inbandwidth`: FortiGate sends sessions to the member with the most available incoming bandwidth.
- `outbandwidth`: FortiGate sends sessions to the member with the most available outgoing bandwidth.
- `bibandwidth`: FortiGate sends sessions to the member with the most available bidirectional bandwidth.

Note that FortiGate doesn't consider the member cost, priority, and configuration order. With the manual strategy FortiGate considers all members that are alive. With the lowest cost (SLA) strategy, FortiGate considers only the number of SLA targets the member meets.

The load balancing method, called **hash-mode**, is an advanced option. You can configure the setting as shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA) With Load Balancing—Example 1

- All members meet the SLA targets configured:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(16), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(6 HUB1-VPN3), alive, sla(0x3), gid(3), num of pass(2)  selected
    2: Seq_num(4 HUB1-VPN1), alive, sla(0x3), gid(3), num of pass(2)  selected
    3: Seq_num(5 HUB1-VPN2), alive, sla(0x3), gid(3), num of pass(2)  selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

- All members meet the two configured SLA targets (**HUB1_HC#1** and **Corp_HTTP#1**)
- Sessions are load balanced across all members using `round-robin`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 55

This slide shows an example of the election of preferred members in a **Lowest Cost (SLA)** rule with load balancing.

The output of the `diagnose sys sdwan service4` command shows that all members meet the two configured SLA targets, and that the load balancing algorithm configured for the rule is `round-robin`. Because all members meet the same number of SLA targets, FortiGate load balances sessions across all members using the round-robin algorithm. Note that member cost, priority, and configuration order are irrelevant.

In the CLI output, FortiGate shows the lowest cost (SLA) *with* a load balancing strategy as `Mode (sla hash-mode=<configured mode>)`. It describes the lowest cost (SLA) strategy *without* load balancing as, `Mode(sla), sla-compare-order`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA) With Load Balancing—Example 1 (Contd)

- Round-robin distribution for six sessions (two sessions for each member):

```
# diagnose sniffer packet any "port 5201 and udp" 4 0 l | grep HUB1
Using Original Sniffing Mode
interfaces=[any]
filters=[port 5201 and udp]
1 2024-09-03 03:31:18.160185 HUB1-VPN1 out 10.0.1.101.35239 -> 10.1.0.7.5201: udp 4
  2024-09-03 03:31:18.161245 HUB1-VPN1 in 10.1.0.7.5201 -> 10.0.1.101.35239: udp 4
2 2024-09-03 03:31:18.161878 HUB1-VPN2 out 10.0.1.101.38872 -> 10.1.0.7.5201: udp 4
  2024-09-03 03:31:18.162679 HUB1-VPN2 in 10.1.0.7.5201 -> 10.0.1.101.38872: udp 4
3 2024-09-03 03:31:18.163186 HUB1-VPN3 out 10.0.1.101.56150 -> 10.1.0.7.5201: udp 4
  2024-09-03 03:31:18.164248 HUB1-VPN3 in 10.1.0.7.5201 -> 10.0.1.101.56150: udp 4
4 2024-09-03 03:31:18.164760 HUB1-VPN1 out 10.0.1.101.57251 -> 10.1.0.7.5201: udp 4
  2024-09-03 03:31:18.165681 HUB1-VPN1 in 10.1.0.7.5201 -> 10.0.1.101.57251: udp 4
5 2024-09-03 03:31:18.166217 HUB1-VPN2 out 10.0.1.101.56499 -> 10.1.0.7.5201: udp 4
  2024-09-03 03:31:18.167065 HUB1-VPN2 in 10.1.0.7.5201 -> 10.0.1.101.56499: udp 4
6 2024-09-03 03:31:18.167559 HUB1-VPN3 out 10.0.1.101.53358 -> 10.1.0.7.5201: udp 4
  2024-09-03 03:31:18.168626 HUB1-VPN3 in 10.1.0.7.5201 -> 10.0.1.101.53358: udp 4
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 56

This slide shows the distribution of six sessions that match the rule configured in example 1. You can see that FortiGate sends one session through each member using a circular distribution (round-robin) for a total of two sessions for each member.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Lowest Cost (SLA) With Load Balancing—Examples 2 and 3

- One preferred member:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(18), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(6 HUB1-VPN3), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(5 HUB1-VPN2), alive, sla(0x1), gid(2), num of pass(1), selected
    3: Seq_num(4 HUB1-VPN1), alive, sla(0x1), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

- HUB1-VPN3 meets the most SLA targets
- Send sessions to HUB1-VPN3 only

- None of the members meet any of the SLA targets:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
 Tie break: cfg
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HUB1-VPN1), alive, sla(0x0), gid(1), num of pass(0), selected
    2: Seq_num(5 HUB1-VPN2), alive, sla(0x0), gid(1), num of pass(0), selected
    3: Seq_num(6 HUB1-VPN3), alive, sla(0x0), gid(1), num of pass(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

- All members have the same SLA status
- Load balance sessions across all members using `round-robin`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 57

This slide shows two more examples of the preferred members selection in a lowest cost (SLA) with load balancing rule. The configuration is the same as the one shown on the previous slide.

The first example on this slide shows HUB1-VPN3 as the only preferred member. This is because HUB1-VPN3 is the member that meets the most SLA targets. As a result, sessions are sent to HUB1-VPN3 only.

In the second example, none of the members meet any of the SLA targets. Because all members have the same SLA status, then FortiGate load balances sessions across all of them.



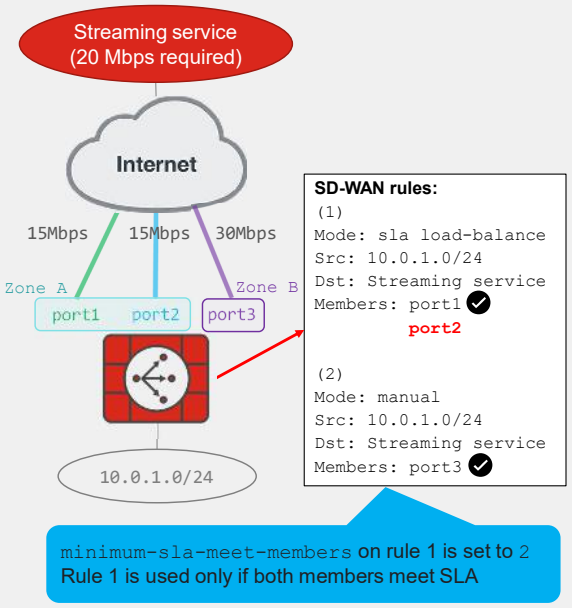
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Consider Number of Members That Meet SLA

- Define minimum number of members that meet *at least one* SLA target
- Supported by lowest cost (SLA) modes only
- Lowest Cost (SLA) With Load Balancing
  - Useful to ensure minimum bandwidth for service
- GUI configuration
  - SD-WAN rule advanced option
- CLI configuration (default = `0`; no check):

```
config system sdwan
    config service
        edit <id>
            set minimum-sla-meet-members <num>
        next
    end
end
```




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 58

For lowest cost (SLA), with or without load balancing, you can define the minimum number of members that must meet *at least one* of the SLA targets configured in a rule, so the rule remains active. If the number of members that meet the SLA is below the minimum threshold, the rule is disabled and skipped during the rule matching stage. The setting that controls this behavior is `minimum-sla-meet-members` and it is set to `0` by default, which means that the minimum number of members is not considered.

The `minimum-sla-meet-members` setting is particularly useful for load balancing rules, because it can be used to ensure that the bandwidth required for a given service is available. Consider the example on this slide, which shows a FortiGate with three internet underlays, each of them supporting a different speed. The example also includes a simplified version of two SD-WAN rules configured to steer traffic to an internet streaming service. Because port3 is an expensive link, the administrator wants to use port3 only as a backup for port1 and port2.

FortiGate then determines that port1 is the only preferred member for rule 1 because port1 is the only member that meets the SLA. If the administrator leaves `minimum-sla-meet-members` to `0` (default value), then FortiGate would use rule 1 for the streaming service, which would then result in a service impact because the minimum required bandwidth (20 Mbps) is not available. However, if the administrator sets `minimum-sla-meet-members` to `2`, then FortiGate disables rule 1 because the rule doesn't meet the minimum number of members that pass at least one SLA. The result is that the administrator can now have FortiGate use rule 2 for the streaming service only when rule 1 doesn't have enough bandwidth.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Effect of minimum-sla-meet-members

- Set to 0 (no check; HUB1-VPN1 is the only egress member used to steer the traffic):

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla [...]
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HUB1-VPN1), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(6 HUB1-VPN3), alive, sla(0x1), gid(2), num of pass(1), selected
    3: Seq_num(5 HUB1-VPN2), alive, sla(0x0), gid(1), num of pass(0), selected
```

HUB1-VPN1 meets two SLA targets
HUB1-VPN3 meets one SLA target
HUB1-VPN2 doesn't meet any SLA targets

- Set to 2 (no change in rule status, HUB1-VPN1 is the only egress member):

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla [...]
  Gen(8), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HUB1-VPN1), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(6 HUB1-VPN3), alive, sla(0x1), gid(2), num of pass(1), selected
    3: Seq_num(5 HUB1-VPN2), alive, sla(0x0), gid(1), num of pass(0), selected
```

- Set to 3 (rule is disabled and skipped):

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla [...]
Gen(3), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(sla  hash-mode=round-robin)
  Service disabled caused by no minimum SLA meet.
  Members(3):
    1: Seq_num(4 HUB1-VPN1), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(6 HUB1-VPN3), alive, sla(0x1), gid(2), num of pass(1), selected
    3: Seq_num(5 HUB1-VPN2), alive, sla(0x0), gid(1), num of pass(0), selected
```

Rule is disabled and skipped during rule matching

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 59

This slide shows the effect of the `minimum-sla-meet-members` setting, when the administrator configured multiple health-check for each member. The result is based on the minimum-sla-meet-members value and the rule SLA status.

The rule status indicates that HUB1-VPN1 passes two SLA targets, HUB1-VPN3 one SLA target, and HUB1-VPN2 no SLA targets. If the number of SLA targets for each member doesn't change, then the effect of the `minimum-sla-meet-members` setting value is as follows:

- If set to `0` (default value), FortiGate doesn't enforce a minimum threshold. The rule is active and HUB1-VPN1 becomes the preferred member because it has the best SLA status. It is the only member with two SLA passed.
- If set to `2`, FortiGate checks if the number of members that meet at least one SLA is equal to or higher than `2`. Because HUB1-VPN1 and HUB1-VPN3 meet at least one SLA target, then the rule passes the minimum threshold and remains active, and HUB1-VPN1 continues to be the preferred member.
- If set to `3`, FortiGate checks if the number of members that meet at least one SLA is equal to or higher than `3`. Because only two members meet at least one SLA target, then the rule is disabled because it doesn't pass the minimum threshold. The rule is skipped during the rule matching process.

Note that the result might not correspond to what the administrator expects. With `minimum-sla-meet-members` set to `2` and two health checks for each member, under some conditions the rule remains active, but FortiGate steer the traffic through a single member. To keep the rule active only if two members are available to steer the traffic, and avoid the situation described above, the administrator should configure only one health check for each SD-WAN member.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe the rule operation and lookup process
- ✓ Configure FortiGate to filter preferred members based on best route
- ✓ Describe the implicit rule and available load balancing algorithms
- ✓ Describe the supported criteria for matching SD-WAN traffic
- ✓ Understand application steering, its learning phase, and expected behavior
- ✓ Describe internet services and their role in rules
- ✓ Understand strategies and the preferred member election process
- ✓ Identify preferred members when monitoring the rule status

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 60

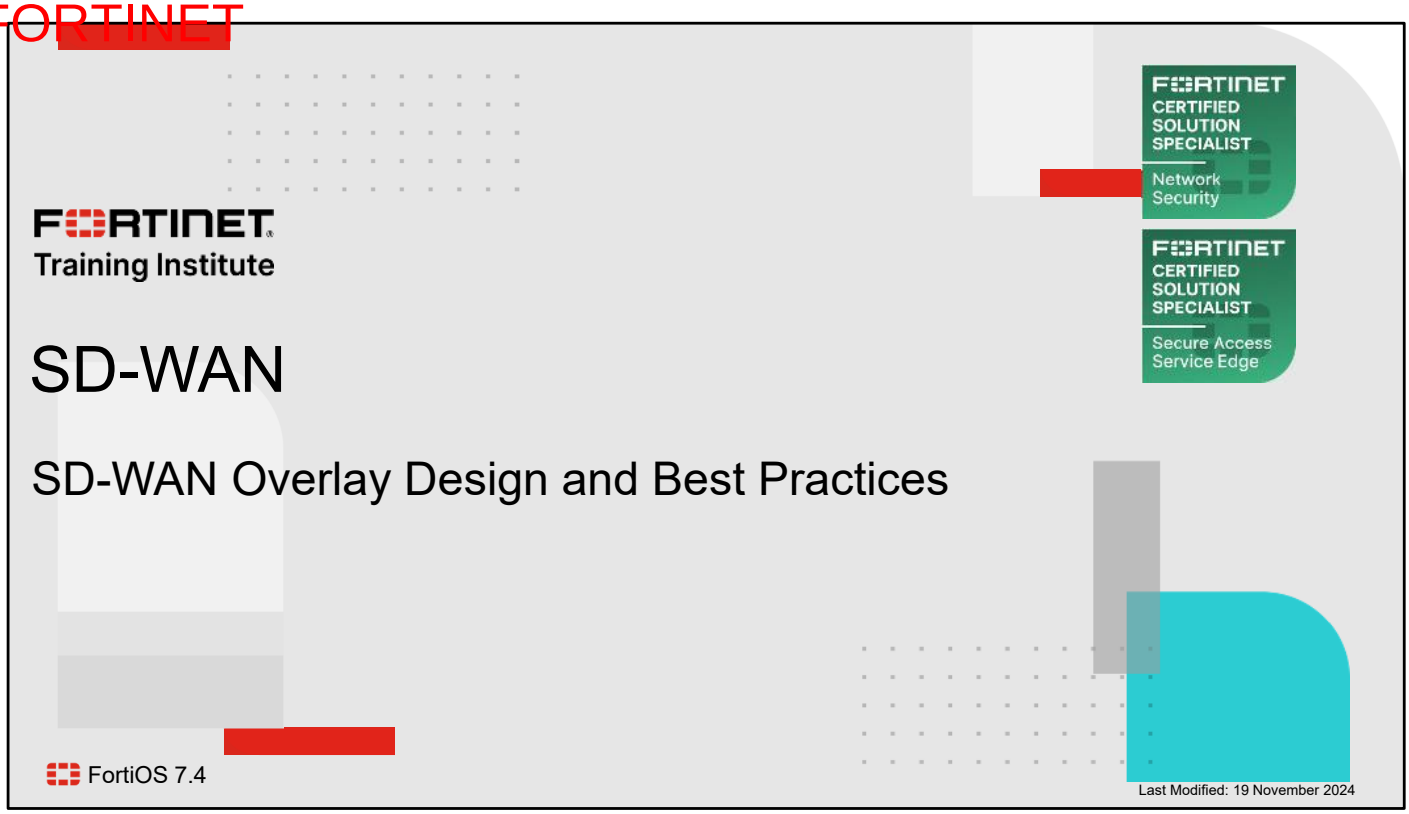
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how SD-WAN rules work, based on the criteria and strategy configured.



Vouchers & Dumps are Available | WhatsApp +201224560923

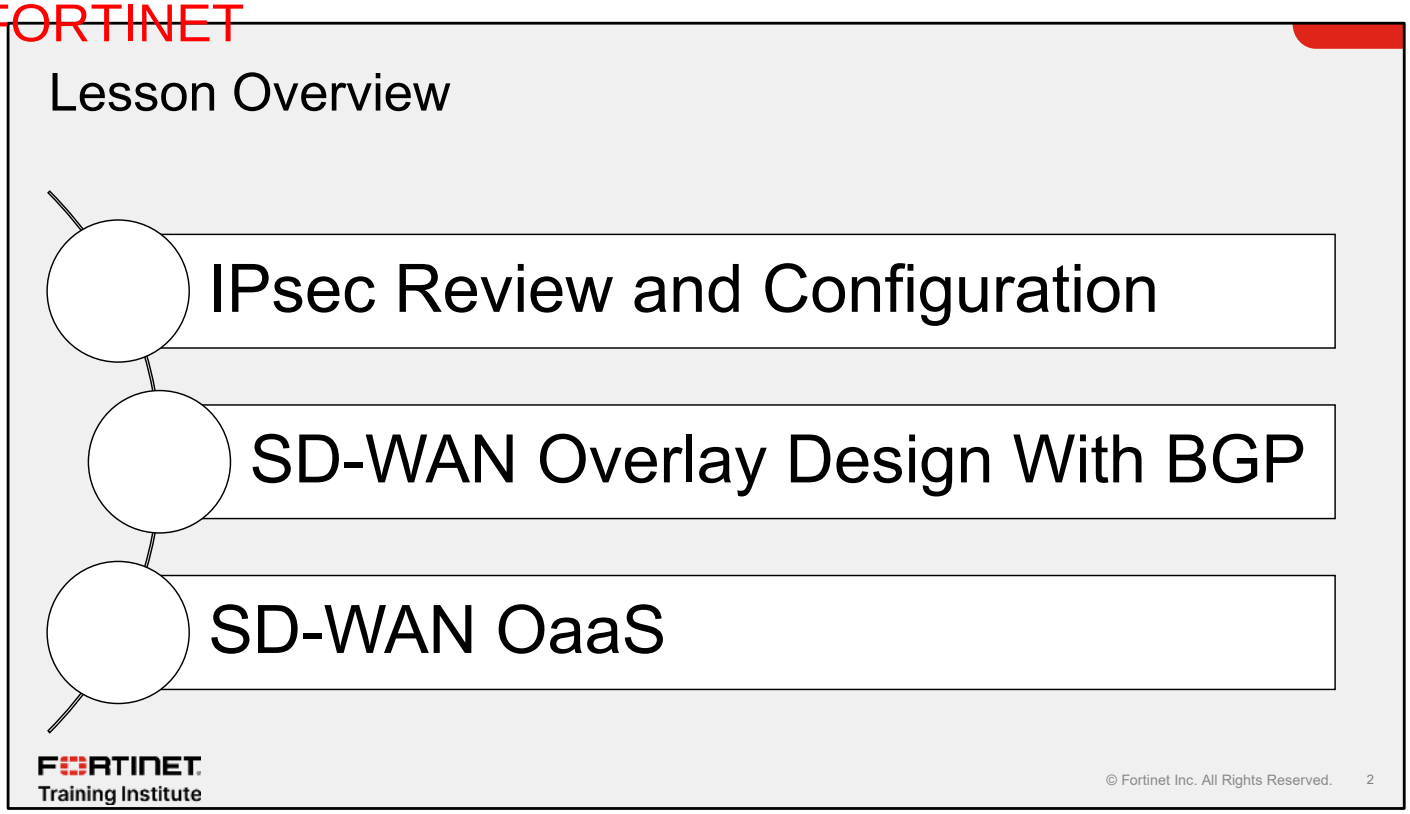
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about the SD-WAN overlay design and advanced IPsec features that are useful for SD-WAN deployments.


Vouchers & Dumps are Available | WhatsApp +201224560923

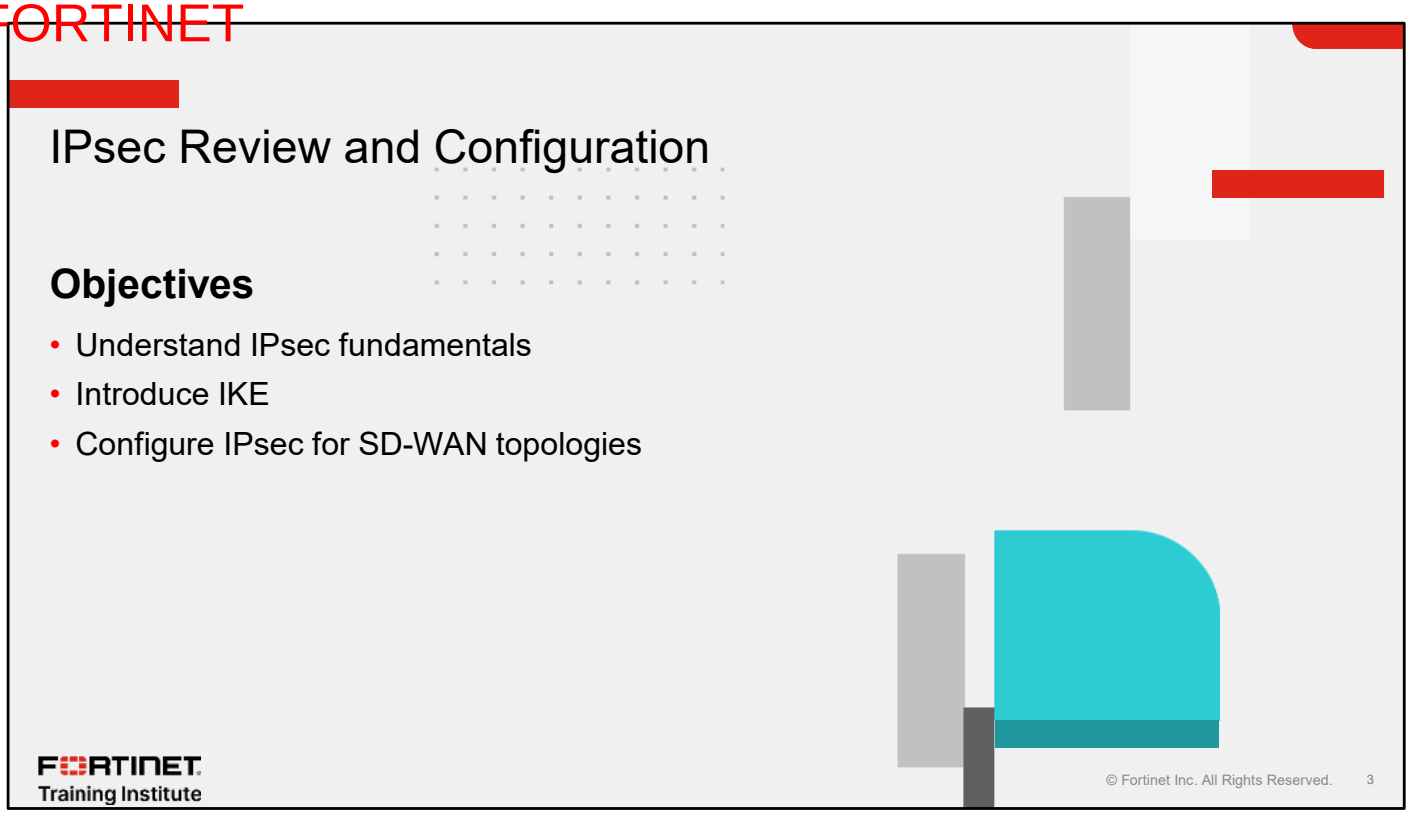
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By reviewing IPsec, you will be able to recall the basics of the protocol and understand the impact of the IPsec parameters used in SD-WAN overlay tunnel configurations.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## IPsec Review

- Suite of protocols for securing IP communications
  - Most used tunneling protocol for SD-WAN overlays
- Authenticates and/or encrypts packets:
  - Internet key exchange (IKE)
    - UDP 500 (no NAT-T)
    - UDP 4500 (NAT-T)
  - Encapsulating security payload (ESP)
    - Provides both data integrity and encryption
    - IP proto 50 (no NAT-T)
    - UDP 4500 (NAT-T)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

IPsec is a suite of protocols for authenticating and encrypting traffic between two peers. Because of its security features, IPsec is the tunneling protocol that is most used for building SD-WAN overlays.

The two most-used protocols in the IPsec suite are:

- IKE, which facilitates the handshake, tunnel maintenance, and disconnection. By default, IKE uses UDP port 500.
- ESP, which ensures data integrity and encryption. ESP uses IP protocol number 50.

The ESP protocol usually has problems crossing devices that are performing network address translation (NAT). One of the reasons is that ESP does not use port numbers, like TCP and UDP do, to differentiate one tunnel from another. To solve this, NAT traversal (NAT-T) was added to the IPsec specifications. When you enable NAT-T on both ends, peers can detect when NAT is performed along the path. If NAT is found, then the following occurs on both peers:

- IKE negotiation switches to using UDP port 4500.
- ESP packets are encapsulated in UDP port 4500.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## IKE Review

- Negotiates the tunnel private keys and encryption
- Allows parties involved in a transaction to set up their security associations (SAs)
  - SAs are the basis for building security functions into IPsec
  - In normal two-way traffic, the exchange is secured by a pair of IKE SAs
- Phases:
  - Phase 1 (IKEv1) — IKE_SA_INIT and IKE_AUTH exchanges (IKEv2) → Outcome: IKE SA
  - Phase 2 (IKEv1) — CREATE_CHILD_SA exchange (IKEv2) → Outcome: IPsec SA
- Versions
  - IKEv1
    - Legacy, well known
  - IKEv2
    - Simplified negotiation process to create SAs
    - More features: network ID, EAP authentication, IKE SA integrity algorithm, and so on
    - Recommended for SD-WAN

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

IKE negotiates the private keys and encryption that the device uses to create an IPsec tunnel.

In order to create an IPsec tunnel, both devices must establish their SAs and secret keys, which are facilitated by the IKE protocol. The SAs are the basis for building security functions into IPsec. An SA is simply the bundle of algorithms and parameters being used to encrypt and authenticate data travelling through the tunnel. In normal two-way traffic, this exchange is secured by a pair of SAs: one for each traffic direction. Essentially, both sides of the tunnel must agree on the security rules. If both sides cannot agree on the rules for sending data and verifying each other's identity, then the tunnel is not established. SAs expire and need to be renegotiated by the peers after they have reached their lifetime.

IKE uses two distinct phases: phase 1 and phase 2. Each phase negotiates different SA types. The SA negotiated during phase 1 is called IKE SA, and the SA negotiated during phase 2 is called IPsec SA. IKE SAs are used for setting up a secure channel to negotiate IPsec SAs. IPsec SAs are used for encrypting and decrypting the data sent and received, respectively, through the tunnel.

The are two IKE versions: IKEv1 and IKEv2. IKEv1 is the legacy, well known version of the protocol. Though still present in the field, it is deprecated and should not be used for new deployments. Administrators should move to IKEv2, because it supports more features and is easier to operate. For example, IKEv2 exclusively supports the network ID feature, which enables the administrator to establish multiple tunnels between the same local and remote gateways, which can be required during failover scenarios involving SD-WAN and auto-discovery VPN (ADVPN). You will learn more about the network ID feature and ADVPN in this lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# IKE Mode Config

- Alternative to DHCP over IPsec
- IKE standard
- Dial-up VPN clients get virtual IP address from the dial-up server
- FortiGate acts as:
  - IKE mode config server (dial-up server)
  - IKE mode config client (dynamic IPsec tunnel)

- Dial-up server—mode-cfg server

```
Config vpn ipsec phase1-interface
   edit HUB1-VPN1
      set type dynamic
      set mode-cfg enable
      set ipv4-start-ip 192.168.1.65
      set ipv4-end-ip 192.168.1.124
      set ipv4-netmask 255.255.255.192
   end
end
```

Range of IP addresses to assign to the clients

- Dial-up client—mode-cfg client

```
Config vpn ipsec phase1-interface
   edit HUB1-VPN1
      set type static
      set mode-cfg enable
      set assign-ip enable
   end
end
```

Default parameters

Accept the IP address assigned by the server

* These examples show the portion of the configuration related to `mode-cfg`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

IPsec allows dynamic tunnel establishment. This allows a device, usually a branch, to establish a tunnel with a server that doesn't have details about every remote endpoint. This server is called the dial-up server. This configuration is common in hub-and-spoke topologies. The IKE standard defines a process to assign virtual remote IP addresses to the devices that establish dynamic IPsec tunnels. This process is called the IKE mode config. On the FortiGate CLI, you activate it with the command `set mode-cfg enable`.

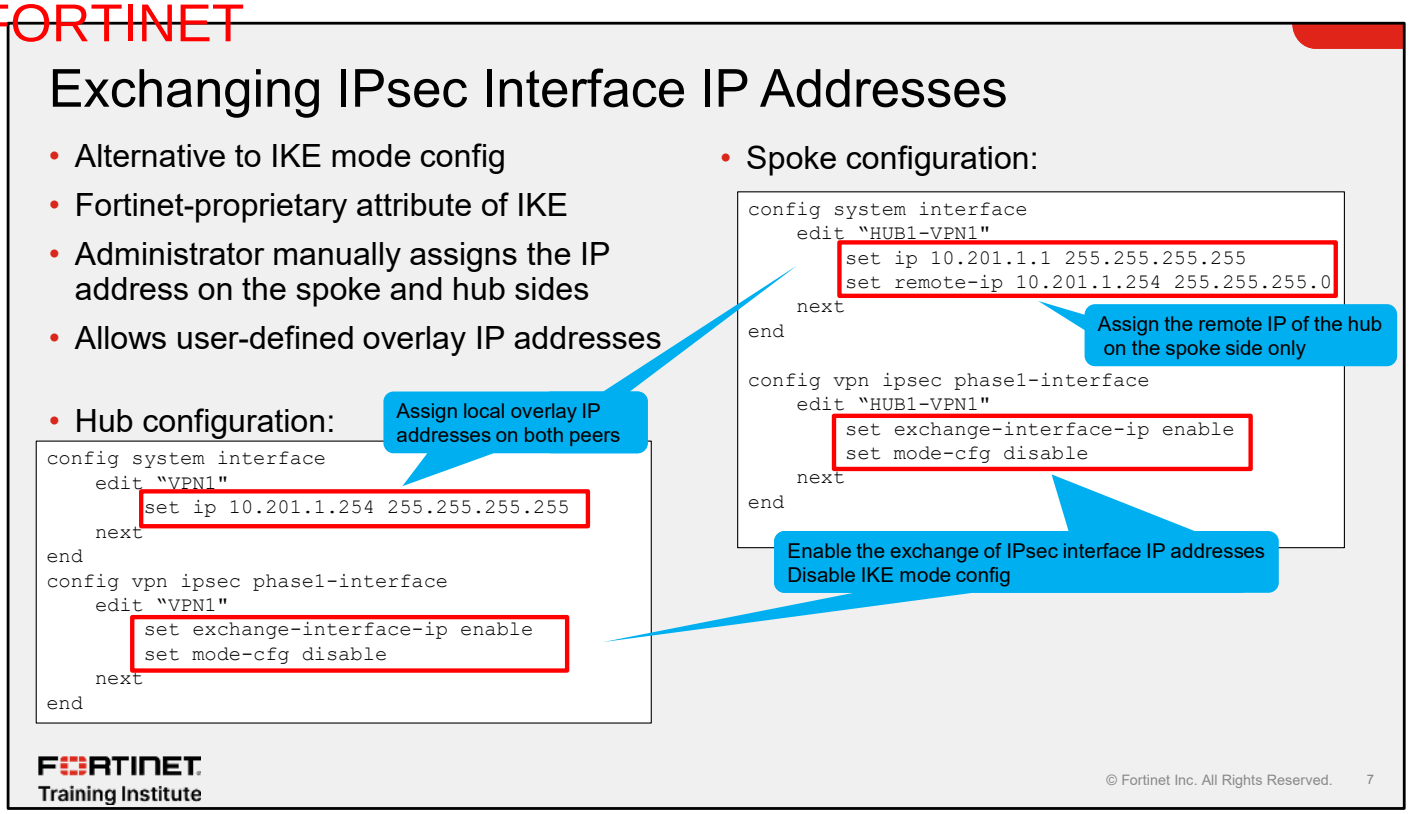
The example on this slide shows the configuration of a server that assigns the IP addresses to the client from an address range. The administrator can configure IKE mode-cfg server FortiGate devices to assign IP addresses from a range, a named firewall address group, a DHCP server, or a RADIUS server.

On the dial-up client, the default tunnel type, `static`, and the parameter `mode-cfg enable`, allow the client to accept the IP address assigned to the IPsec interface with the command `set assign-ip enable`.

The SD-WAN overlay template configures the hub devices as dial-up servers. assigns IP addresses from the range defined by the administrator, and configures the branch devices as dial-up clients.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




The example IPsec configuration used for the SD-WAN overlay topology shown in this lesson makes use of IKE mode config to assign the IP addresses of the spoke overlays. Although its configuration is simple, IKE mode config doesn't allow you to define fixed IP addresses on the spoke side. That is, the address assigned to an overlay depends on the addresses that are available during tunnel negotiation.

An alternative to IKE mode config is the IPsec exchange interface feature. Instead of using IKE mode config to assign addresses automatically, you manually assign the address on the spoke and hub sides, and then have IKE exchange them during tunnel negotiation, so each gateway knows the remote overlay IP address. The result is that you can assign a fixed address to a spoke overlay, which can then be used for monitoring and identification purposes.

This slide shows the changes that are required on the hub and spoke to exchange the IPsec interface IP addresses using IKE. The configuration changes are the same on the hub and the spoke, except that you assign different local IP addresses on each side, and on the spoke FortiGate, you must also define the hub IP address. Also, when defining the hub IP address, use the overlay subnet netmask (/24 in the example) as the netmask, instead of /32. Using the overlay subnet netmask is useful for next hop resolution when reflecting routes using IBGP.

Note that FortiGate uses a Fortinet-proprietary attribute to exchange the IP addresses. This means that, unlike IKE mode config, which is a standard IPsec feature, you can exchange IP addresses using IKE only, when both gateways are FortiGate devices.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## The net-device Parameter

- Configured on IPsec phase 1 interface
- Fortinet-proprietary attribute
- net-device enable
  - Creates a dynamic interface for dial-up tunnels
  - Dedicated interface per dialer (phase1name_index)
  - Helps with monitoring and troubleshooting
  - Not recommended for devices with many dial-up tunnels
- net-device disable (default)
  - Improves the tunnel set-up and tear-down rates
  - Shared network interface per phase1
  - Tunnel ID for each dynamic tunnel
- Recommended settings for SD-WAN topologies
  - Hub: disabled
  - Spokes: enabled

```
Branch1_fgt#
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        ...
        set net-device enable
        ...
    next
end
```

Setting on branches

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

The net-device parameter is a FortiGate-specific parameter configured at the IPsec phase1-interface level. This parameter determines if FortiGate creates a kernel interface for each tunnel or not. When enabled, FortiGate creates a dynamic interface for each dial-up tunnel with a phase 1 name and an index. While this easily identified interface can be useful for monitoring and troubleshooting, its creation consumes CPU resources and can slow down the tunnel set-up and tear-down rates. When net-device is disabled, a tunnel ID is generated for each dynamic tunnel. This ID, in the form of an IP address, is used as the gateway in the route entry to that tunnel.

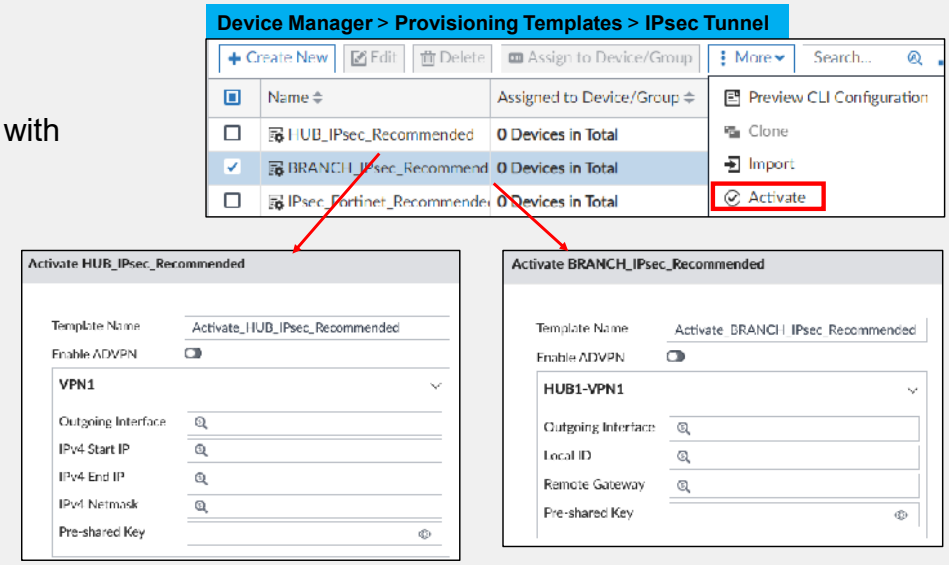
On SD-WAN topologies, Fortinet recommends that you keep net-device disabled on the hub (default setting) and enable net-device on the spokes. If you configure SD-WAN on the hub device, FortiOS does not allow you to configure dynamic IPsec tunnels as SD-WAN members.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# FortiManager—Recommended IPsec Templates

- Predefined templates
  - IPsec
  - Branch IPsec
  - Hub IPsec
- Simplified configuration with recommended settings
- Activate template




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

If you don't want to use the SD-WAN overlay template to help with IPsec VPN tunnel configuration for the hub-and-spoke topology, you can use the predefined IPsec tunnel templates available on FortiManager. In both cases, FortiManager uses the same recommended settings to build IPsec tunnels.

When you use the predefined templates, you need to define only the main parameters, as shown on this slide. The BRANCH_IPsec_Recommended and HUB_IPsec_Recommended templates will add the parameters discussed on previous slides, like tunnel type or net-device settings. Later, you can edit the prepared template for fine-tuning and to apply advanced settings.

Note that you can also use the templates to enable ADVPN, and set the corresponding recommended parameters, on your hub-and-spokes topology.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## FortiManager—Recommended IPsec Templates (Contd)

- Hub template main settings
  - ike-version 2
  - type **dynamic**
  - **net-device disable**
  - **mode-cfg enable**
  - add-route disable
  - IP address assignment
  - network-overlay enable
  - network-id
- Hub parameters to add manually
  - Phase 2
    - keepalive
  - VPN interface
    - IP address
    - remote IP subnet
- Branch template main settings
  - ike-version 2
  - type **static**
  - **net-device enable**
  - **mode-cfg enable**
  - add-route disable
  - IP address assignment
  - network-overlay enable
  - network-id
  - **local ID**
  - Phase2 auto-negotiate enable
- Branch parameters to add manually
  - Phase 2
    - keepalive

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

When you use the SD-WAN overlay template or recommended IPsec templates for the hub and branches, FortiManager will prepare IPsec templates with the following parameters:

For hubs:

- dynamic tunnel type for dial-up server
- net-device disable

For branches:

- static tunnel type (remote end IP address is known)
- net-device enable

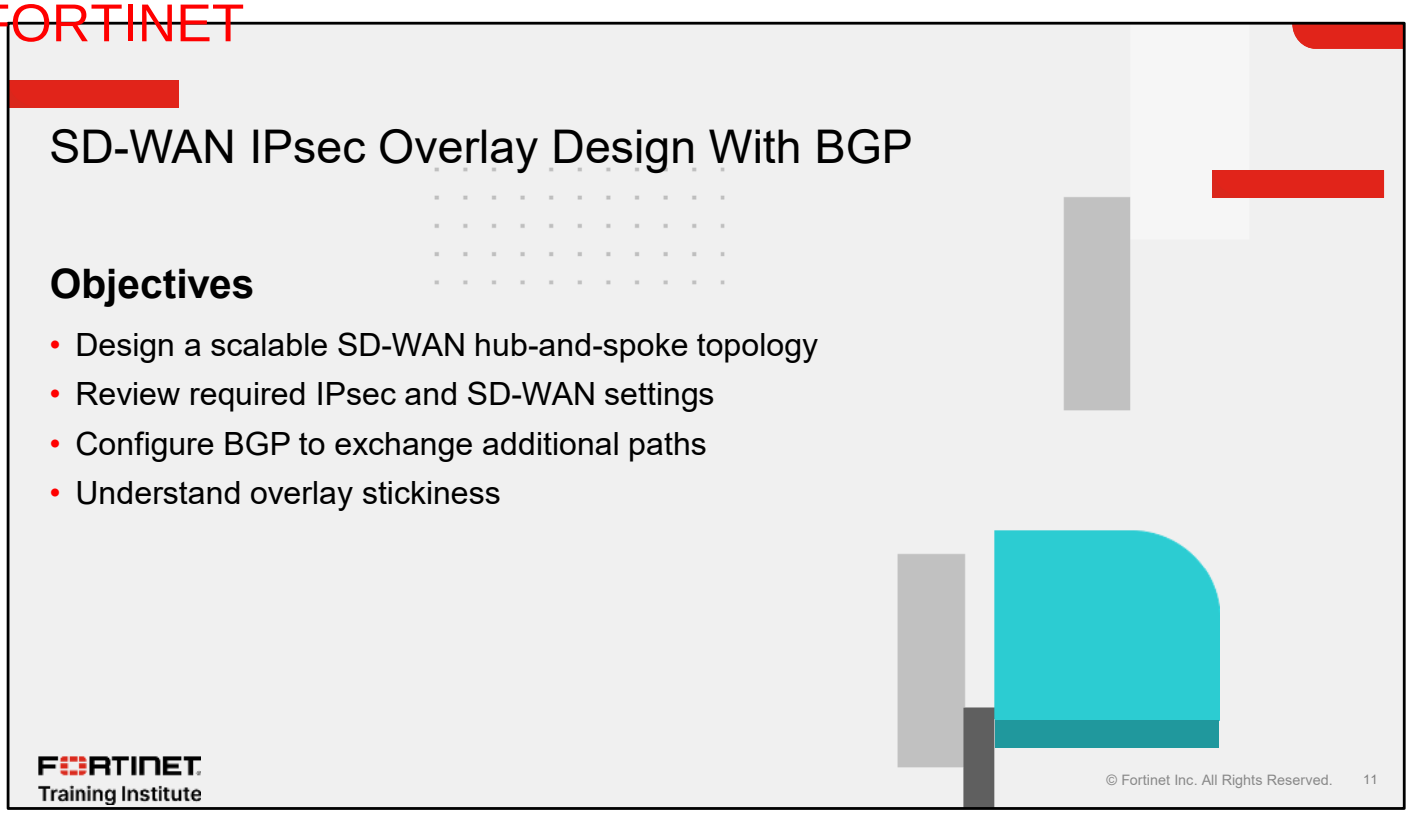
These parameters correspond to the recommended settings for IPsec overlay tunnel configuration.

The templates will also enable network-overlay and configure network-id for hubs, and, for branches, local-id and network-id. Optionally, you can edit the templates to add keepalives for both types of devices.

For the hub, you need to complete the template configuration with the VPN interface IP address and remote IP subnet settings. This can be done with the CLI template.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

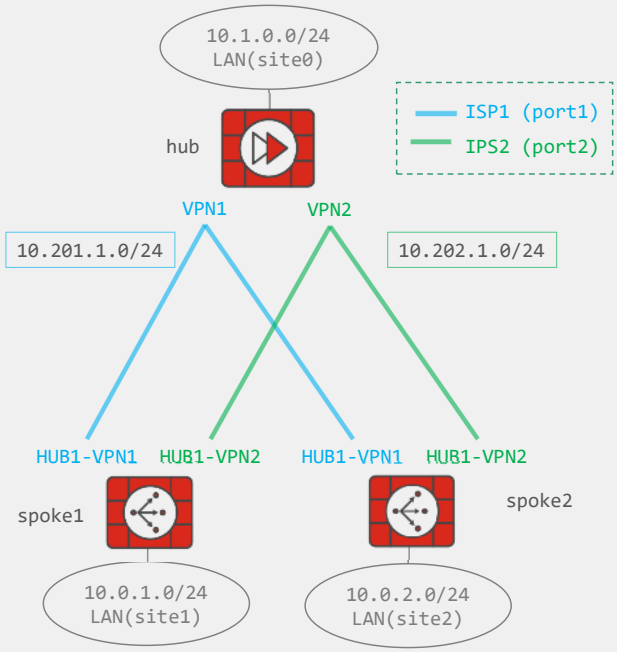
By demonstrating competence in SD-WAN IPsec overlay design, you will be able to understand the configuration required to deploy a scalable SD-WAN network that uses IPsec and BGP as base building blocks. You will also understand how FortiGate devices can exchange all available paths, which is convenient for SD-WAN, and you will be able to improve performance by forcing overlay stickiness.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Standard SD-WAN Overlay Design With IPsec

- Hub-and-spoke topology
  - Dial-up tunnels
    - Hub: server
    - Spokes: client
  - Group overlays per ISP (higher performance)
- SD-WAN
  - Usually deployed on the spokes only
  - Sometimes required on the hub too
  - Support for ADVPN
- Routing
  - Dynamic routing is preferred (more scalable)
  - Multiple paths (all sites exchange their prefixes)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

The topology shown on this slide represents a standard SD-WAN deployment using IPsec overlays.

The IPsec overlays follow a hub-and-spoke design. The hub is located at the customer's central office or datacenter, and the spokes (also known as branches or edges) are distributed across all remote sites (branch offices, retail stores, remote workers, and so on). The hub acts as a dial-up IPsec server for the spokes and has a separate dial-up server configuration for each underlay interface. The result is that each dial-up server configuration defines a point-to-multipoint (PTMP) overlay. To have multiple alternative paths to all subnets in the network, each spoke usually connects to all overlays.

For better performance, it's recommended to group overlays per ISP. That is, it's better to deploy same-ISP overlays than cross-ISP overlays. By connecting tunnels over the same ISP, you should get better performance because the latency is usually lower than the latency of packets crossing multiple ISPs.

Most of the IPsec overlay traffic is initiated from the spokes to the hub. Spokes access workloads protected by the hub. The workloads are located on the hub, or on a network that is reachable through the hub. Because most of the traffic is initiated in the spoke-to-hub direction, SD-WAN is usually deployed on the spokes only. However, in some cases, traffic is also initiated in the hub-to-spoke direction, which is why SD-WAN may also be required on the hub side.

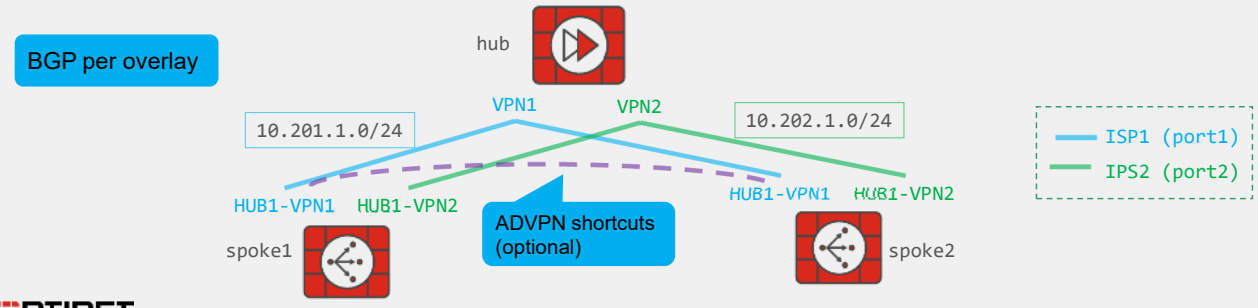
A dynamic routing protocol, usually as BGP, is used to exchange routing information through the overlays. The topology also shows the IP subnets used for the overlays. The overlays established over the ISP1 underlay (port1) are assigned an address in the `10.201.1.0/24` subnet, and the overlays established over the ISP2 underlay (port2) are assigned an address in the `10.202.1.0/24` subnet. The goal is for all sites to exchange their prefixes over all available overlays, and to support ADVPN with SD-WAN, if needed. Although static routing is possible, dynamic routing is preferred for scalability reasons.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Topology Built With the SD-WAN Overlay Template

- The SD-WAN overlay template defines hub-and-spoke topologies with:
  - IPsec tunnels for the overlay links
  - One or multiple links from each spoke to one or two hubs
  - Dynamic routing with IBGP
  - BGP per overlay
  - A loopback IP address on each FortiGate used to define health check
  - Optional: ADVPN shortcuts allowed




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

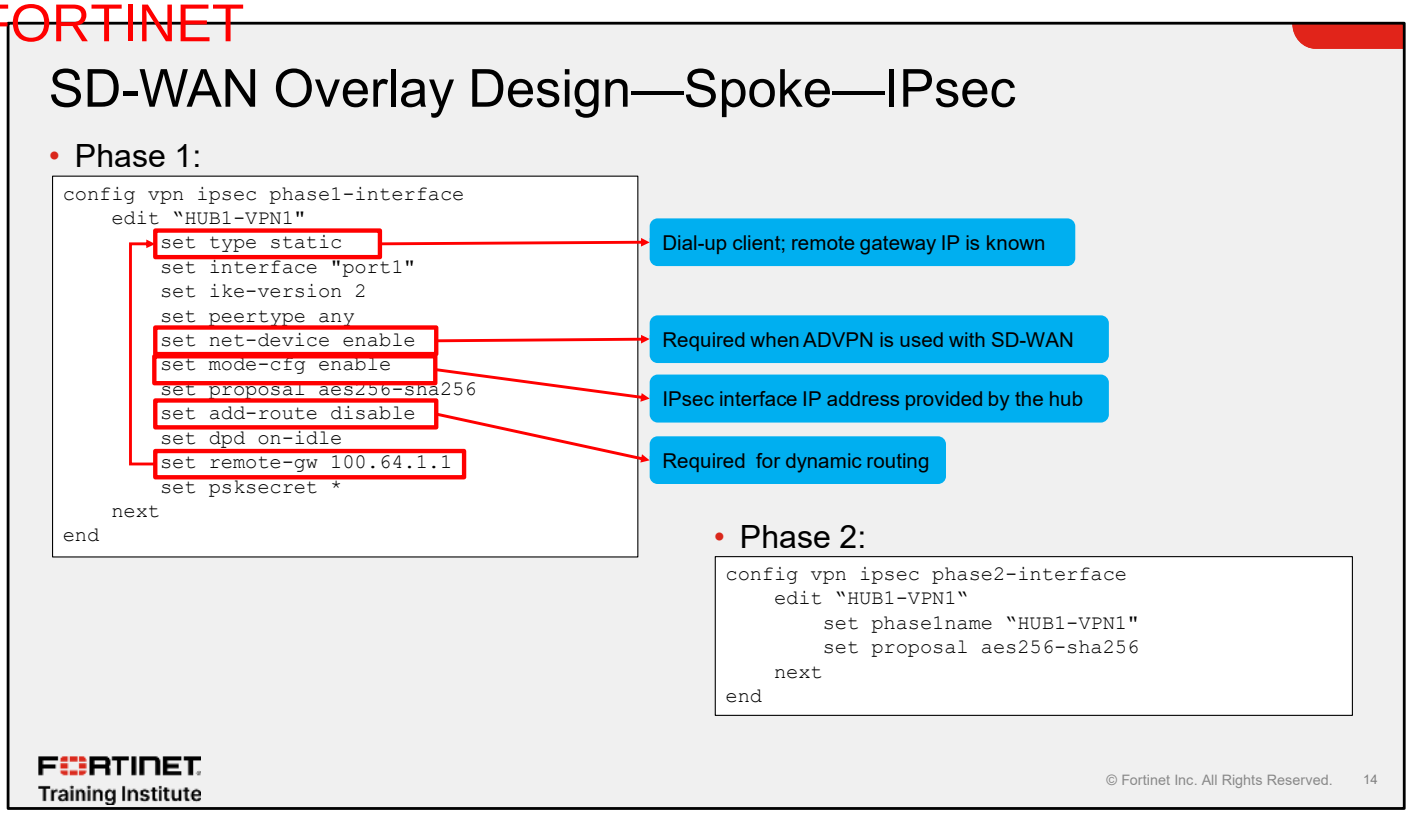
The SD-WAN overlay template defines a hub-and-spoke SD-WAN topology with IPsec to secure the overlay links. For the routing protocol on overlay links, it defines an IBGP topology with BGP neighbor relationships for each overlay for the branches-to-hub routing. This BGP design is called *BGP per overlay*. These types of design are widely deployed in the field and suitable for small-to-medium sized topologies, with or without ADVPN. This is the topology that you will deploy in the lab exercises.

For SD-WAN topologies, administrators can choose between multiple BGP designs, such as *BGP on loopback* or *dynamic BGP*. You will learn more about these designs, their advantages, and their limitations, in another lesson.

In this lesson, you will learn about the main IPsec and BGP parameters used for SD-WAN topologies with BGP on loopback.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




This slide shows an example of the IPsec configuration required on the spoke for the ISP1 overlay. This lesson covers the relevant settings for SD-WAN at a high level, based on the configuration that FortiManager would apply with the SD-WAN overlay template.

The tunnel is bound to the `port1` underlay. The configuration is the same for the ISP2 overlay, except the binding interface (port2) and the IP address of the remote gateway. The tunnel type is set to `static` (dial-up client) because the IP address of the remote gateway (the hub) is known. In this case, the address corresponds to the address assigned to port1 on the hub.

The IKE version is 2. IKEv2 is recommended for increased security level, and for SD-WAN, because of its benefits for ADVPN. Both `net-device` and `add-route` are disabled. The former allows for better performance on large deployments and is also required for adding dial-up IPsec tunnels as SD-WAN members. You can disable `add-route` if you plan to use a dynamic routing protocol to exchange routing information through the tunnels.

You must enable the `net-device` settings if you want to support ADVPN shortcuts in SD-WAN. Although disabling `net-device` provides better performance, enabling the setting should not represent a concern, because the number of overlays deployed on the spokes is usually low.

The phase 2 configuration is the same as in the hub. The encryption domain is open to let SD-WAN, the forwarding information base (FIB), and the firewall policies dictate the traffic forwarding policy.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# SD-WAN Overlay Design—Spoke—Interfaces

- IPsec interface:

```
config system interface
    edit "HUB1-VPN1"
        set vdom "root"
        set allowaccess ping
        set type tunnel
        set interface "port1"
    next
    edit "HUB1-VPN2"
        set vdom "root"
        set allowaccess ping
        set type tunnel
        set interface "port2"
    next
end
```

IP address is assigned automatically through IKE mode config

Enable ICMP access for troubleshooting purposes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

This slide shows an example of the system interfaces configuration on the spokes.

You don't have to assign an IP address for the overlays. Their IP addresses are obtained using IKE mode configuration. Enabling `ping` access is useful for troubleshooting.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Overlay Design—Spoke—BGP

- IBGP configuration:

```
config router bgp
    set as 65000
    set router-id 10.200.99.1
    set ibgp-multipath enable
    config neighbor
        edit "192.168.1.61"
            set interface "HUB1-VPN1"
            set remote-as 65000
            set update-source "HUB1-VPN1"
        next
        edit "192.168.1.125"
            set interface "HUB1-VPN2"
            set remote-as 65000
            set update-source "HUB1-VPN2"
        next
    end
    config redistribute "connected"
        set status enable
        set route-map "port5 only"
    end
```

- Allow ECMP for IBGP routes
- One neighbor per overlay
- Bind BGP packets to overlay
- IBGP AS number—identical for local and remote AS
- Use, as source IP for BGP packets, the address of the selected interface (recommended)
- Advertise IGP prefix (connected route) to peers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

This slide shows an example of the IBGP configuration on the spokes.

IBGP is used—both the local AS and remote AS are the same (65000). IBGP is preferred over external BGP (EBGP) because IBGP preserves the next hop for prefixes, which is convenient for ADVPN. With SD-WAN, ECMP is expected because of the multipath nature of SD-WAN. If using IBGP, you must enable `ibgp-multipath` to support ECMP for IBGP routes.

Each entry in `config neighbor` defines the IP address of the BGP neighbor for the overlay. For instance, `192.168.1.61` is the IP address of the hub overlay established over ISP1, and `192.168.1.125` is the IP address of the hub overlay established over ISP2.

The `interface` and `update-source` settings indicate the source interface and source IP address to use for BGP packets, respectively. This is important because of the multipath nature of SD-WAN. FortiOS performs a route lookup to determine the outgoing interface for BGP packets. Binding the BGP packets to an interface and a source address ensures that there are no cross-overlay BGP peerings between the spoke and the hub.

Note that in this setup, `update-source` is redundant and not required. The `interface` setting automatically forces the source IP address to be that of the selected interface. `update-source` is more useful for cases in which the source IP address for BGP is different from the source interface. A common example is when using a loopback interface address as the source IP. However, even when redundant, it's still a good practice to configure the `update-source` setting for consistency purposes.

The entry in `config redistribute "connected" instructs the spoke` to inject the IGP prefix from port5 (`10.0.1.0/24`) into the BGP table so it is advertised to peers. This corresponds to LAN subnet connected to the spoke.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# SD-WAN Overlay Design—Spoke—SD-WAN

- SD-WAN:

```
config system sdwan
    config zone
        edit "overlay"
        next
    end
    config members
        edit 4
            set interface "HUB1-VPN1"
            set zone "overlay"
        next
        edit 5
            set interface "HUB1-VPN2"
            set zone "overlay"
        next
    end
    config health-check
        edit "HUB1_HC"
            set server "10.200.99.253"
            set protocol ping
            set members 4 5
        next
    end
...
```

Points to loopback address on the hub

```
...
    config service
        edit 1
            set name "HTTP"
            set mode priority
            set protocol 6
            set start-port 80
            set end-port 80
            set dst "Corp-net"
            set src "LAN-net"
            set health-check "HUB1_HC"
            set priority-zone "overlay"
        next
    end
end
```

Define `priority-members` or `priority-zone`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

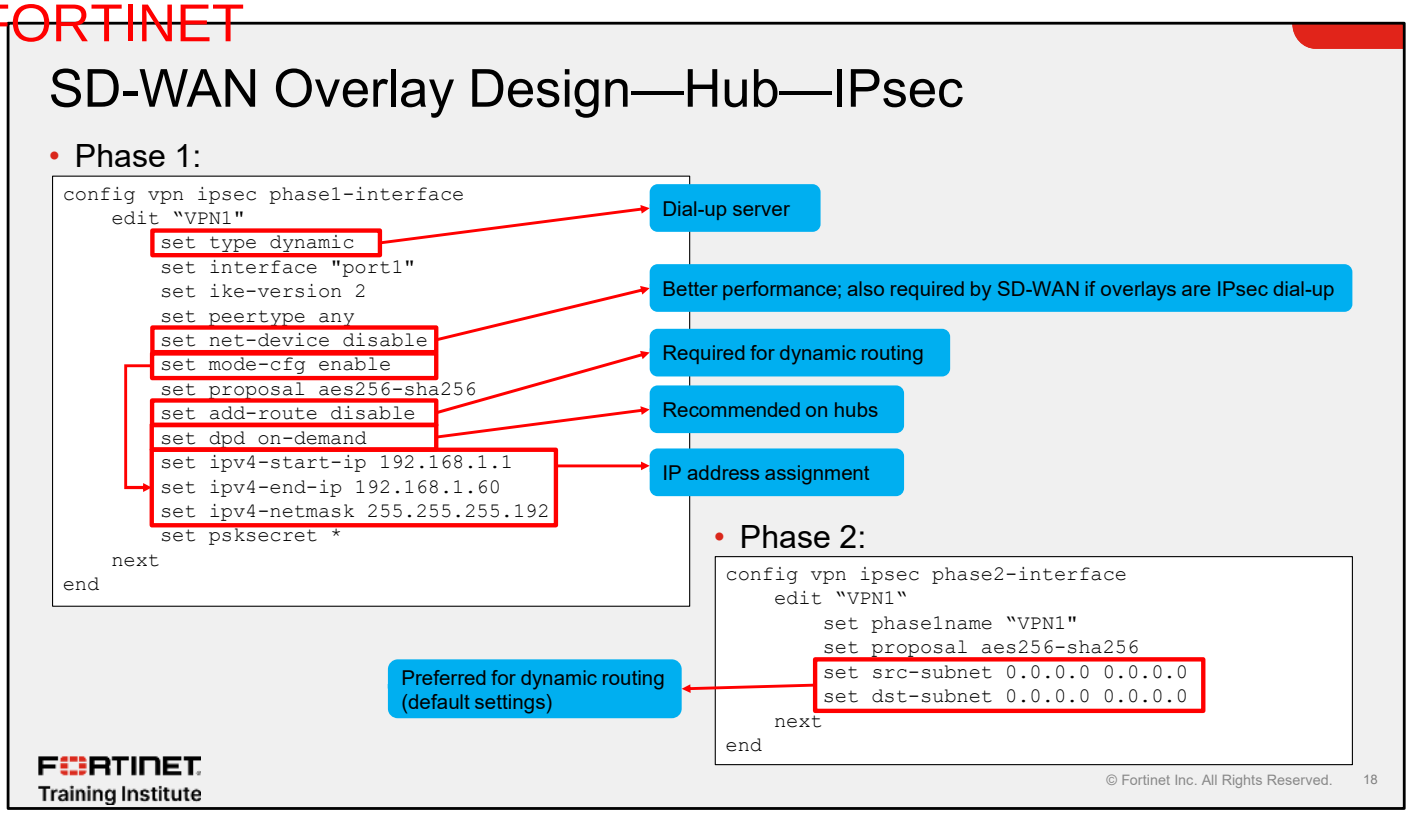
This slide shows an example of the SD-WAN configuration for the IPsec dial-up tunnels on the spokes.

The configuration is fairly simple. The two overlays are placed in the `overlay` zone. The `VPN` performance SLA uses ping to actively measure the health and performance of the overlays against `10.200.99.253`, which is the address of the loopback interface on the hub.

A best quality SD-WAN rule is configured to steer HTTP traffic from the LAN subnet (`10.0.1.0/24`) to the corporate subnet (`Corp-net`, `10.0.0.0/8`). The rule uses the `HUB1_HC` performance SLA to determine the best quality member in the `overlay` zone and define the destination interface as a priority zone. For each service, the administrator can define the destination with a list of interface or with a zone, which means all interfaces from the zone.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




This slide shows an example of the IPsec configuration required on the hub for the dial-up ISP1 overlays. Some settings are the same used on the spoke (dial-up client), so this slide focuses on settings that are specific for the hub.

The tunnel is bound to the `port1` underlay. The configuration is the same for the dial-up ISP2 overlays, except the binding interface (port2) and the mode config address range (`192.168.1.64/26`). The type of the tunnel is set to `dynamic` (dial-up server). That is, tunnels can be initiated only from the spoke side. Dynamic works better for hub-and-spoke deployments because it reduces the amount of configuration required on the server side, while it enables spokes to have dynamic IP addresses or be located behind NAT devices.

For dead peer detection (DPD), it's recommended to use `on-demand` mode on dial-up servers, like the hub. When you use on-demand mode, FortiGate sends DPD probes if there is only outbound traffic through the tunnel, but no inbound. On-demand mode is more convenient on hubs because of the reduced overhead. The more passive a hub is, the better it scales.

To assign IP addresses to overlays on spokes, `mode-cfg` is enabled. The `ipv4-xxx` settings are also defined to indicate the IP address range and netmask to use. The phase 2 configuration is simple. Sites exchange their prefixes using dynamic routing, so it's more convenient to leave the encryption domain open. This way, SD-WAN, the FIB, and the firewall policies dictate the traffic forwarding policy.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# SD-WAN Overlay Design—Hub—Interfaces

- IPsec interface:

```
config system interface
    edit "VPN1"
        set vdom "root"
        set allowaccess ping
        set ip 192.168.1.61 255.255.255.255
        set type tunnel
        set remote-ip 192.168.1.62 255.255.255.192
        set interface "port1"
    next
    edit "VPN2"
        set vdom "root"
        set allowaccess ping
        set ip 192.168.1.125 255.255.255.255
        set type tunnel
        set remote-ip 192.168.1.126 255.255.255.192
        set interface "port2"
    next
end
```

An IP address is assigned automatically through IKE mode config

Remote IP expected address range, automatically set through IKE mode config

Enable ICMP access troubleshooting purposes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

This slide shows an example of the system interfaces configuration on the hub.

Through the IKE mode config, FortiGate assigns the tunnel interface IP address by selecting one address from the address range defined by the administrator. It also defines the remote-ip address range, which corresponds to the addresses assigned to the spoke IPsec VPN interfaces through the IKE mode config.

It is recommended that you enable ping access, which is useful for troubleshooting.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# SD-WAN Overlay Design—Hub—BGP

- IBGP configuration:

```
config router bgp
    set as 65000
    set router-id 10.200.99.253
    set ibgp-multipath enable
    config neighbor-group
        edit "VPN1"
            set interface "VPN1"
            set remote-as 65000
            set update-source "VPN1"
            set route-reflector-client enable
        next
        edit "VPN2"
            set interface "VPN2"
            set remote-as 65000
            set update-source "VPN2"
            set route-reflector-client enable
        next
    end
...
```

Standard BGP settings for each group of spokes (one group per overlay)

Bind BGP packets to overlay (recommended)

Spokes can learn prefixes from other spokes (required for ADVPN topology only)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

This slide shows an example of the BGP configuration on the hub. Some settings are the same as those used on the spoke, so this slide focuses on only those settings that are specific to the hub

Because the remote BGP speakers—the spokes—are dial-up clients, it's convenient to define a `neighbor-group` for overlays established over each underlay. This way, the BGP peerings are always initiated from the spokes—expected because spokes are dial-up clients. FortiGate then applies the common settings in the `neighbor-group` to each BGP peering.

Inside each `neighbor-group` entry, the `interface` and `update-source` settings indicate the source interface and source IP address to use for BGP packets, respectively. Those settings are optional on the hub and not configured by the SD-WAN overlay template. As for the spokes, binding the BGP packets to an interface and a source address ensures that there are no cross-overlay BGP peerings between the spoke and the hub.

With `route-reflector-client` setting enabled, spokes can learn about each other's prefixes. You need to enable route reflector on the hub only if you plan to enable ADVPN.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# SD-WAN Overlay Design—Hub—BGP (Contd)

- IBGP configuration:

```
...
    config neighbor-range
        edit 1
            set prefix 192.168.1.0 255.255.255.192
            set neighbor-group "VPN1"
        next
        edit 2
            set prefix 192.168.1.64 255.255.255.192
            set neighbor-group "VPN2"
        next
    end
    config redistribute "connected"
        set status enable
        set route-map "port5_only"
    end
end
```

Define the IP address range for each neighbor group

BGP peers from `192.168.1.0/26` match the `VPN1` group

Advertise IGP prefix (connected route) to peers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

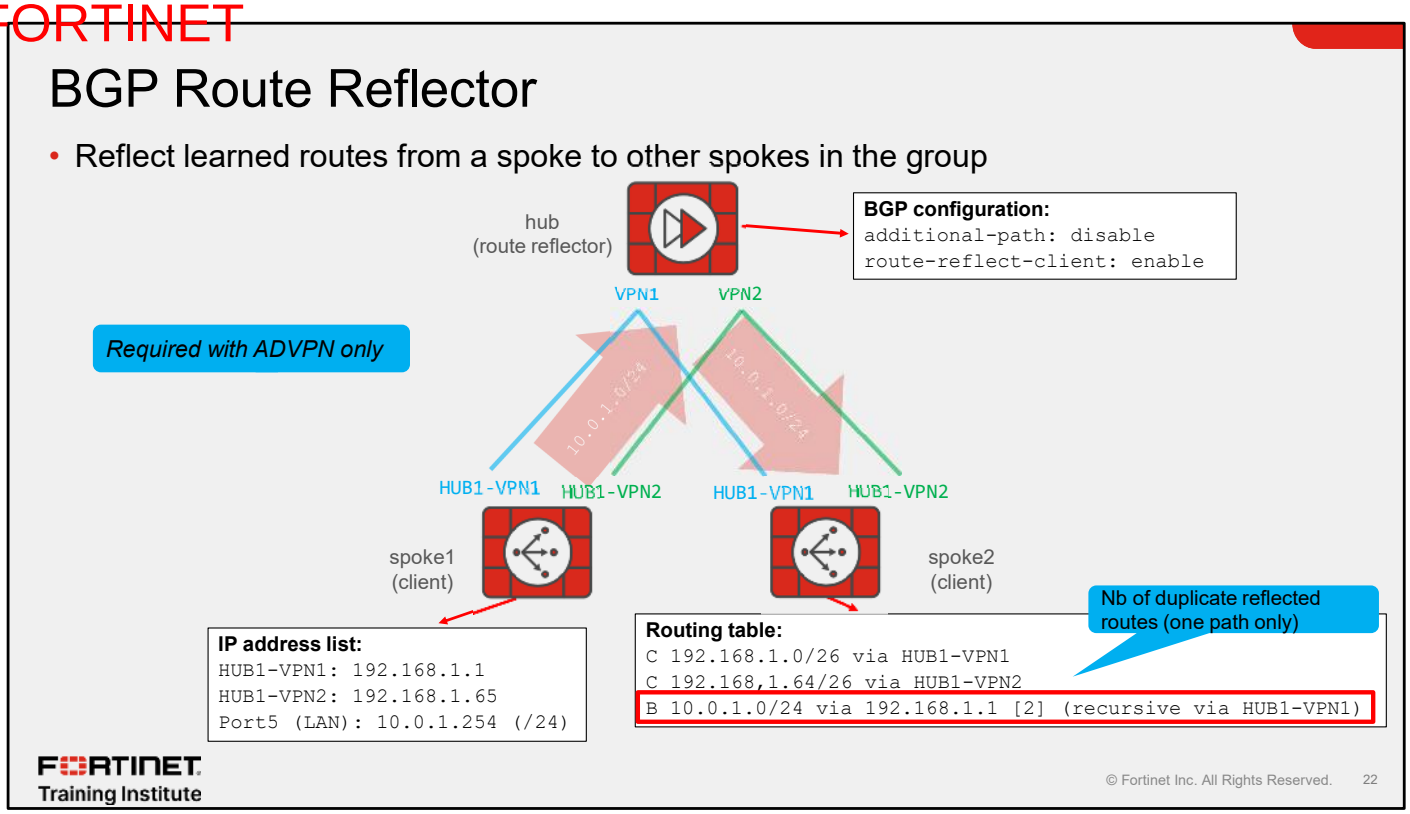
This slide shows the remaining part of the BGP configuration on the hub.

Each entry in the `neighbor-range` defines the IP address range to use for each neighbor group. For example, peers with an IP address in the `192.168.1.0/26` subnet are considered part of the `VPN1` neighbor group. Usually, the groups correspond to BGP neighbors from overlay tunnels built on the same type of underlay links (the same ISP or BGP). Neighbor groups are useful to limit the route propagation within a single neighbor group when you activate route reflection.

The section `redistribute "connected"` advertises IGP connected routes as per the route map defined. On this configuration, it's the subnets connected to port5. Although the hub routing table is not shown on this slide, `10.1.0.0/24` is the connected route from port5—the hub local subnet—which is why you configure a network entry to advertise it to the spokes. Alternatively, to `redistribute "connected", you can use config network` to indicate the interior gateway protocol (IGP) prefix to inject it into the BGP table so it is advertised to peers. IGP refers to non-BGP routes in the routing table, such as OSPF, RIP, connected, and static.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET




By default, IBGP routers do not pass on routes learned from internal neighbors to other internal neighbors. The `route-reflector-client` setting instructs FortiGate to act as a route reflector, and therefore, to pass on (or reflect) learned routes from an IBGP client (a spoke) to other IBGP clients (other spokes in all neighbor groups). If you enable ADVPN in our SD-WAN topology, you want spokes to learn the prefixes of other spokes, then you must enable `route-reflector-client` on the neighbor groups.

The diagram on this slide shows how BGP route reflector works. The hub, which acts as route reflector, reflects the `10.0.1.0/24` prefix, which is advertised by spoke1, to spoke2. The hub learns the prefix through two overlays—HUB1-VPN1 and HUB1-VPN2—each using a different next hop—`192.168.1.1` and `192.168.1.65`, respectively. That is, the hub learns the prefix through two different paths: one with next hop `192.168.1.1` and another with next hop `192.168.1.65`.

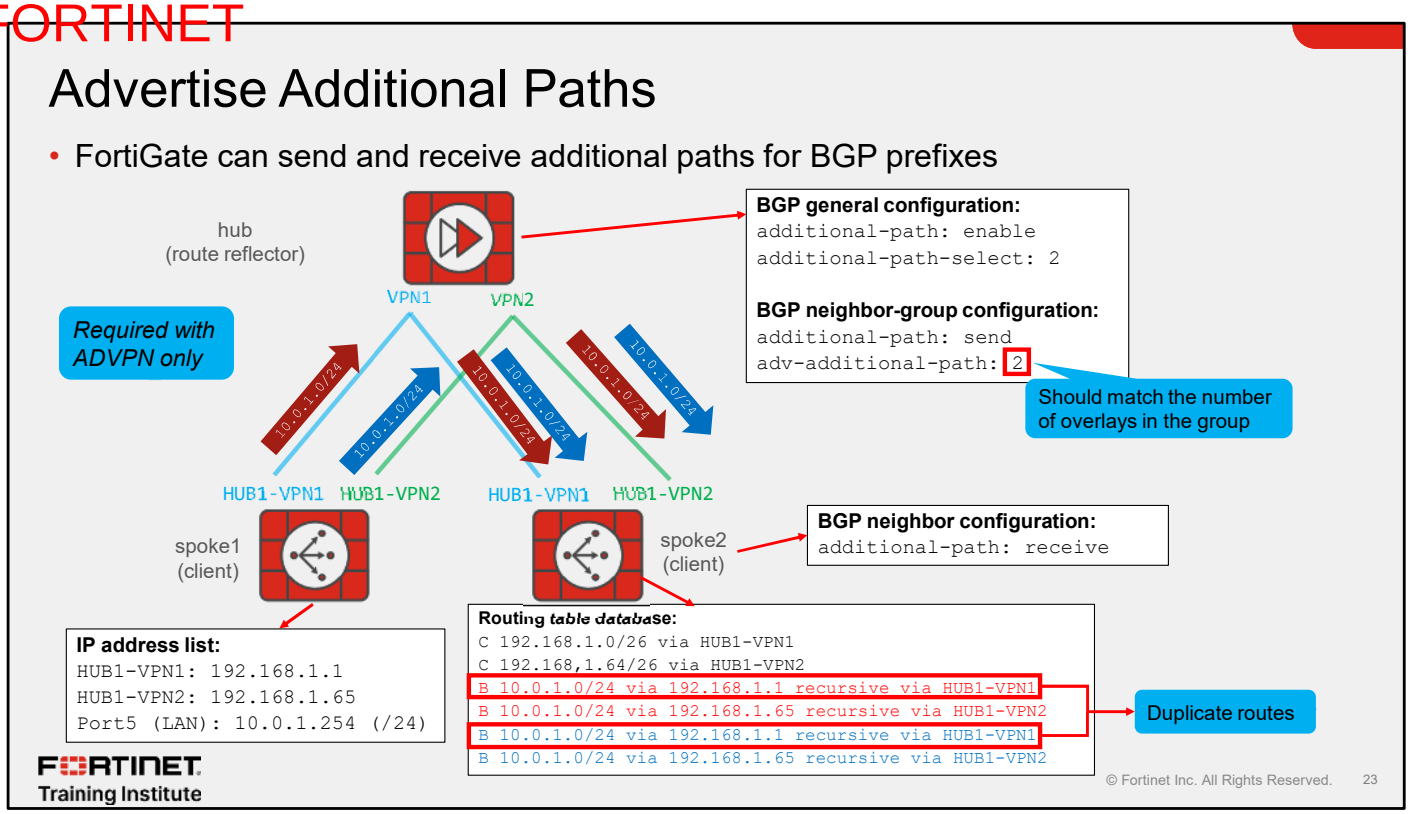
The hub then reflects the prefix to spoke2, which in turn performs a recursive lookup to determine the outgoing interface to use for the prefixes based on the next hop. The recursive lookup matches the static route for the overlay IP subnets, which is why the BGP routes show HUB1-VPN1 as the outgoing interface.

It is important to highlight the following:

- The routing table on spoke2 shows number two [2] to indicate duplicate routes for `10.0.1.0/24`. They are the result of IBGP preserving the next hop. Duplicate routes are visible on FIB and summarized on the routing table for better readability.
- The hub reflects only the path through `192.168.1.1`. It doesn't reflect the path through `192.168.1.65`. This is because the hub is not configured to advertise additional paths for prefixes (`set additional-path disable`).


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



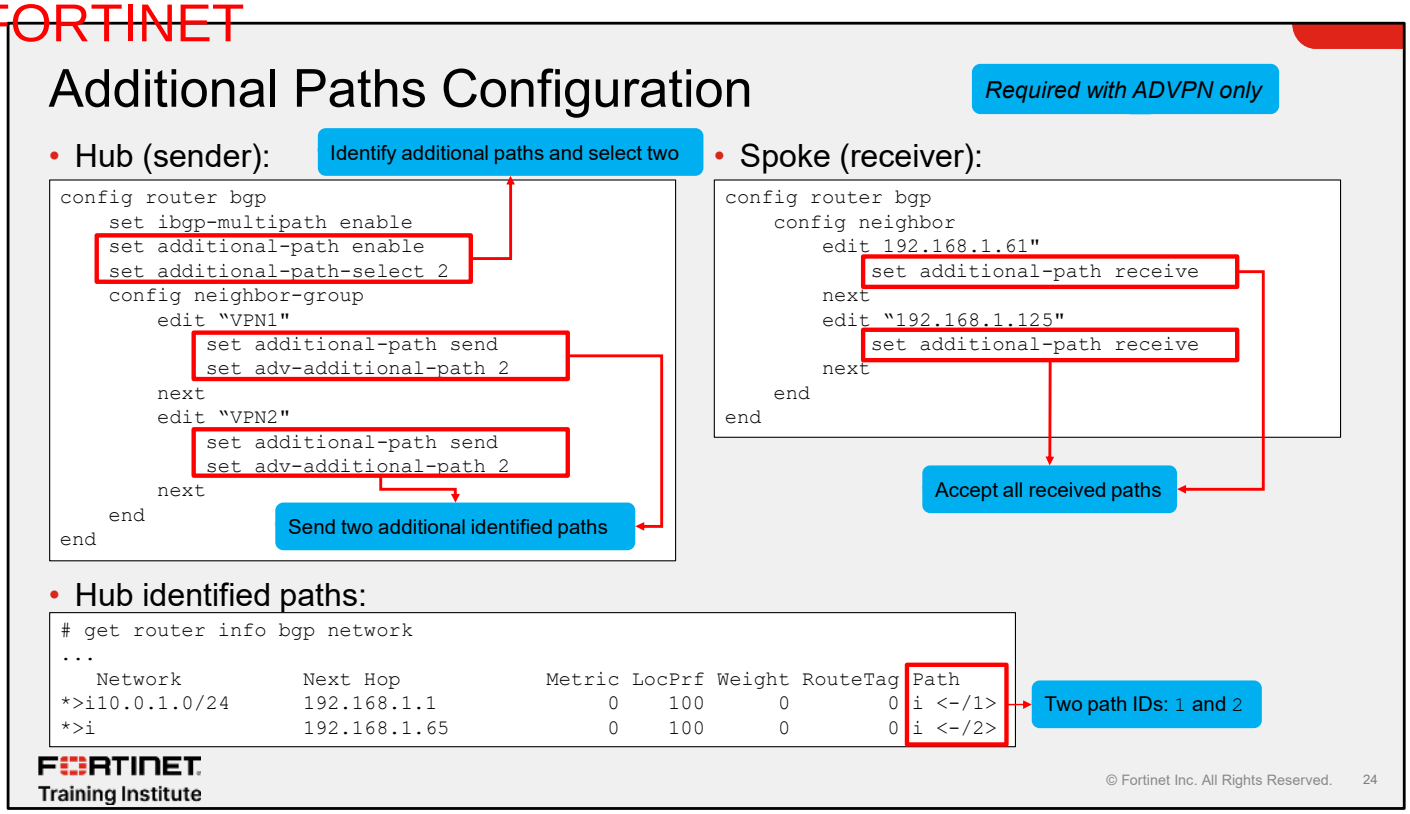

When you configure FortiGate as a BGP speaker, FortiGate advertises one path per prefix, by default. In the SD-WAN overlay deployment shown on this slide, this means that the hub, acting as the route reflector, reflects only one path for each prefix despite learning two paths from the spoke client.

For SD-WAN, it is recommended that sites learn all available paths to all possible destinations; otherwise, SD-WAN rules and members may be skipped because of the absence of a route in the FIB. For this reason, it's a best practice to allow FortiGate to advertise additional paths so peers know all available paths. You should configure the hub to advertise one path per overlay.

The diagram on this slide shows the two paths that the hub learns for `10.0.1.0/24`: one learned through HUB1-VPN1 with next hop `192.168.1.1`, and another through HUB1-VPN2 with next hop `192.168.1.65`. The hub is configured to send two additional paths, as well as to reflect prefixes learned from clients. In addition, the spoke is configured to receive any additional paths sent by the neighbor. The result is that spoke2 now receives both paths for `10.0.1.0/24` from the hub through the two overlays, for a total of four routes received. Because IBGP preserves the next-hop information, then the routing table database on spoke2 shows duplicate routes for the prefix.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




This slide shows how to configure BGP additional paths using the FortiGate CLI based on the SD-WAN overlay topology used in this lesson.

For the hub to send the additional paths, it must first identify the unique paths learned from the BGP neighbor. The hub assigns an identifier to each unique path received for a prefix. You instruct FortiGate to identify the paths by enabling `additional-path` under `config router bgp`. You can view the identifiers and paths using the `get router info bgp network` command.

Next, the hub must select two or more identified paths that it can later advertise to neighbors. You control the number of selected identified paths with the `additional-path-select` setting.

After the hub identifies all paths, and selects a number of identified paths to advertise, you must indicate the neighbors you want the hub to advertise the additional paths to and how many. You configure this using the `additional-path` and `adv-additional-path` settings under `config neighbor-group`.

The example configuration shown on this slide for the hub instructs FortiGate to identify all paths received from neighbors, and selects two of them for advertising over BGP. In addition, the hub FortiGate advertises (or sends) two selected additional paths—that is, all selected additional paths—to peers on each neighbor group. For SD-WAN topologies with BGP route reflection, you should configure the hub to path received from the spoke, that is the number of connected links between the spoke and the hub.

On the spoke, which acts as a receiver of the additional paths, you must set `additional-path` to `receive` under each neighbor entry, so the spoke FortiGate accepts all the additional paths sent by the hub.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Duplicate Routes Consolidation

- Routing table database shows all duplicate routes received on a spoke device

```
# get router info routing-table database
...
B     *> 10.0.1.0/24 [200/0] via 192.168.1.1 (recursive is directly connected, HUB1-VPN1), 01:05:02
      *>             [200/0] via 192.168.1.65 (recursive is directly connected, HUB1-VPN2), 01:05:02
      *>             [200/0] via 192.168.1.1 (recursive is directly connected, HUB1-VPN1), 01:05:02
      *>             [200/0] via 192.168.1.65 (recursive is directly connected, HUB1-VPN2), 01:05:02
```

- Duplicate routes are consolidated in the routing table

Number of duplicate routes available

```
# get router info routing-table all
...
B       10.0.1.0/24 [200/0] via 192.168.1.1 [2] (recursive is directly connected, HUB1-VPN1), 01:03:45
                    [200/0] via 192.168.1.1 [2] (recursive is directly connected, HUB1-VPN2), 01:03:45
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

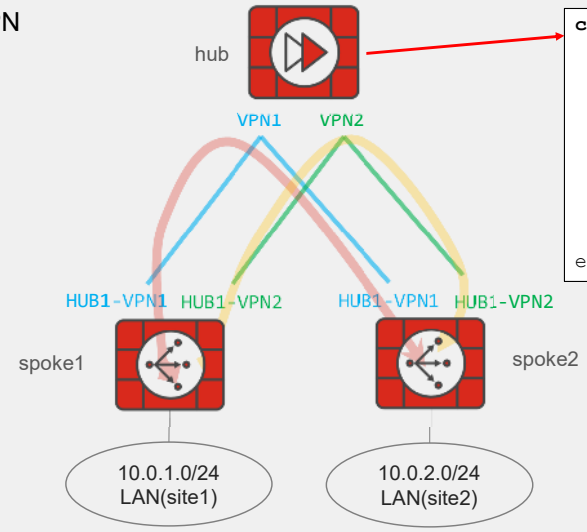
The routing table database show all duplicate routes received. On the routing table, for easier readability, FortiOS consolidates the duplicate routes and indicates the number of duplicate routes available. Note that the duplicate routes are not filtered, they are just consolidated for cosmetic purposes.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Overlay Stickiness on the Hub

- Prefer spoke-to-spoke traffic to stay within same-ISP overlays
  - Better performance
  - Useful for ADVPN




```
config router policy
    edit 1
        set input-device "VPN1"
        set output-device "VPN1"
    next
    edit 2
        set input-device "VPN2"
        set output-device "VPN2"
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

In the standard SD-WAN overlay design shown on this slide, spoke-to-spoke traffic is routed through the hub. When the hub receives the first packet of a spoke-to-spoke connection, it performs a route lookup to determine the best route and outgoing interface to forward the packet to. Based on the routing lookup results, the hub may resolve to use an overlay established over a different underlay from the one used by the incoming overlay. That is, based on our topology, if the hub receives the first packet on HUB1-VPN1, it may decide to forward it out of HUB1-VPN2.

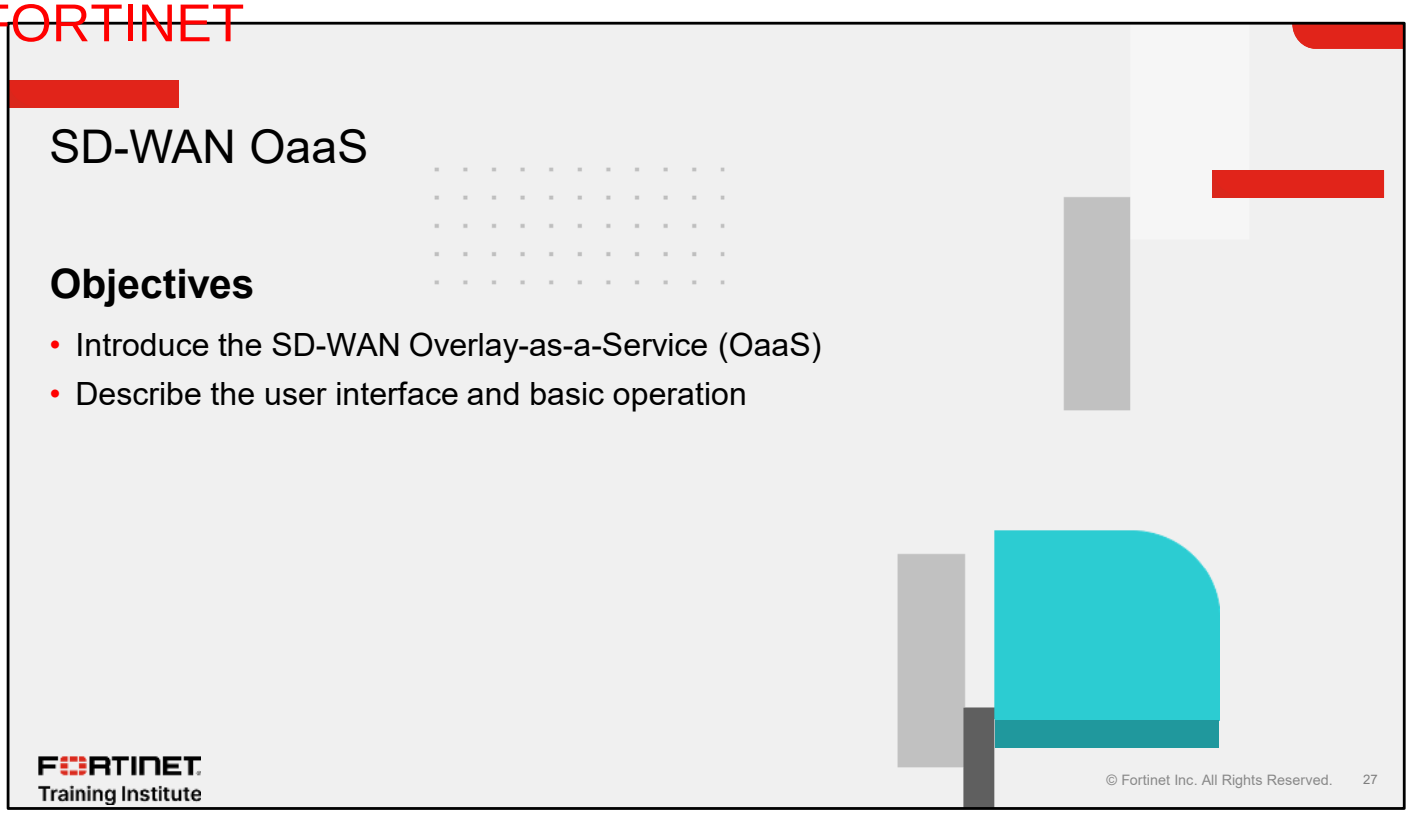
Although the connection is established, the performance isn't the best because of the added latency introduced by the cross-ISP overlay path. To instruct FortiGate to prefer to keep spoke-to-spoke traffic within same-ISP overlays, you can configure the policy routes shown on this slide.

Note that the policy routes are a preference only. That is, they are used only if the FIB contains a route for the outgoing overlay. Otherwise, they are skipped and FortiGate forwards the traffic based on the best route in the FIB.

Overlay stickiness is very important for ADVPN because it helps to prevent the spokes from trying to negotiate shortcuts over unreachable underlays. You will learn more about ADVPN and overlay stickiness in this lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

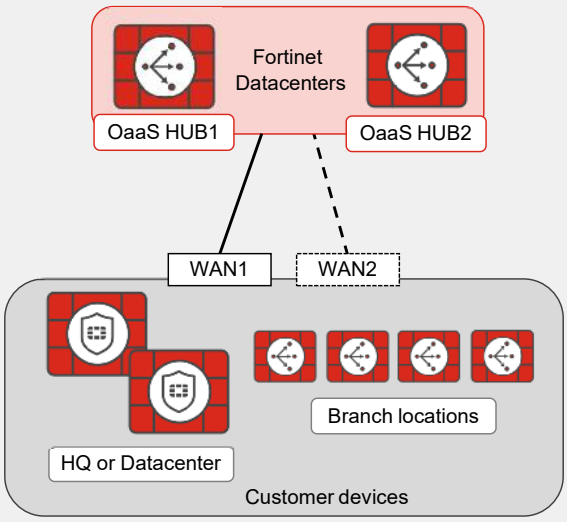
You will understand what OaaS is, the advantage of the service, and how to configure and use the service with your FortiGate devices.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## What is SD-WAN Overlay as a Service?

- Fortinet OaaS is Software-as-a-Service (SaaS) that provides on-demand secure connectivity between locations
- How does OaaS work?
  - Fortinet provides:
    - Managed hubs, with geo-redundant, dual-hub, high availability (HA) architecture
    - The OaaS orchestrator to create and install appropriate policies across multiple devices
  - Customer provides:
    - Ownership and management of the spoke devices
    - Management of the overlay connections with the OaaS web interface
- What are the benefits of OaaS?
  - Cost saving on devices, hosting, and management
  - Simplicity and fast delivery




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

Fortinet SD-WAN Overlay as a Service (OaaS) is a software service that provides on-demand secure connectivity between locations with point and click setup and monitoring. With OaaS, Fortinet provides geo-redundant, dual-hub, high availability architecture for continuous operation. Customers own and manage the local devices at branch locations or at headquarters or a datacenter, and delegates the overlay infrastructure.

The Fortinet OaaS orchestrator allows for the easy configuration and management of the overlay architecture and associated rules. The OaaS orchestrator is an intuitive web interface that allows customers to manage their network requirements—set up new connections, define policies and rules, install the configuration to multiple devices, and remove connections when they become useless.

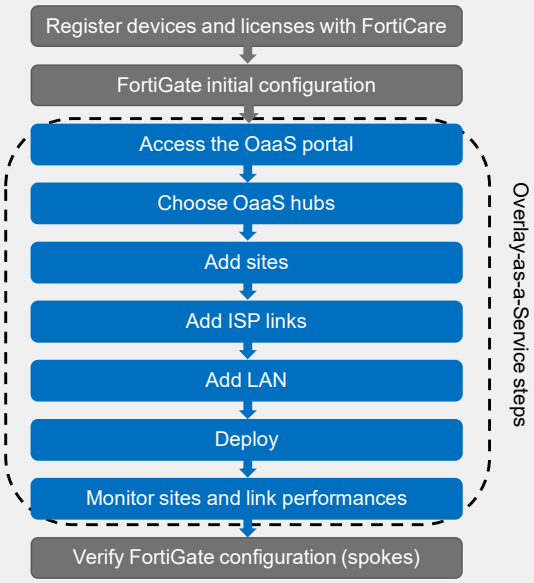
OaaS utilizes SD-WAN for intelligent path steering and BGP dynamic routing. It provides quick and easy-to-set up redundant, on-demand connectivity between locations and simplifies the conversion of legacy VPN networks to SD-WAN networks.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Initial Overlay Configuration With OaaS

- OaaS is a licensed service
  - One license for each remote device
  - Optional:
    - FortiCloud SD-WAN Network Monitor license for the bandwidth feature
- Supported topologies
  - SD-WAN with dual hub (primary and secondary)
  - SD-WAN with ADVPN
- Spokes run FortiOS 7.4.4 and later
- Spoke initial configuration
  - LAN and WAN interfaces
  - Basic routing—branches can reach the hub
  - Interfaces used for OaaS not associated with:
    - SD-WAN zone
    - Network zone
    - Firewall policy




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

OaaS is a licensed service. You must install an OaaS license for every remote site for which you want to use the service. Optionally, you can add the FortiCloud SD-WAN Network Monitor license for remote monitoring of the upload and download speed on each overlay.

You can use OaaS to deploy dual-hub SD-WAN topologies and SD-WAN topologies that allow auto-discovery VPN (ADVPN) shortcuts.

Before you connect a site to OaaS, you must connect it to the internet and register it with your FortiCare account. You must also perform the following tasks and configurations:
- Upgrade to 7.4.4 or later.
- Define LAN and WAN interfaces and their IP addresses.
- Configure routes to allow the devices to reach the OaaS hubs.
- Remove interfaces used by OaaS from SD-WAN zones, network zones, and firewall polices.

Then, on the OaaS portal, you use the GUI to define your topology and add sites with just a few steps:
- Select the location of the Fortinet-hosted OaaS hubs—select two locations for redundancy purposes.
- Define the sites with a name, a type, and a registered device serial number. For each site, you can select between branch or datacenter type. It's an information-only parameter, both behave the same way.
- Add ISP links for each site. For each site, you define a name, select an interface, and, optionally, add a cost.
- Define the LAN subnet for each site.

Once you have completed the device and link definitions, click **Apply** to deploy the service and create the overlay links that correspond to the topology that you created. OaaS installs the overlay configuration on your devices.

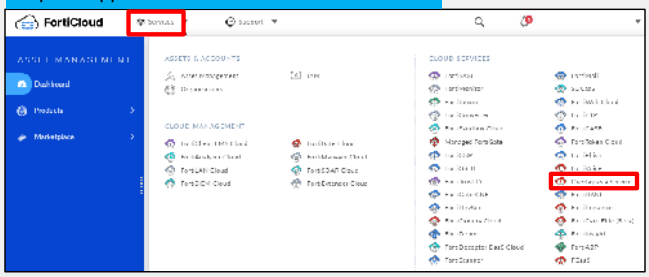

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

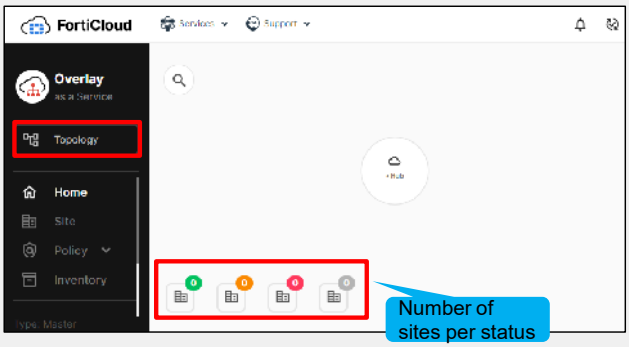
## FortiCloud OaaS Portal

- Access OaaS from the Fortinet service and support portal

https://support.fortinet.com/assets/#/dashbord




- Initial OaaS web landing page




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

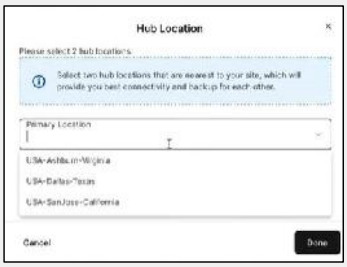
You access the OaaS portal from the Fortinet service and support portal by selecting **Services** and then **Overlay as a Service**. On the OaaS main page, if you have not yet configured a topology, you see the hub icon and 0 for each site status—**All Pass**, **Operational**, **Disconnected**, and **Unmanaged**. Select the **Topology** menu to start your topology definition.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# OaaS Web Portal Menus Overview

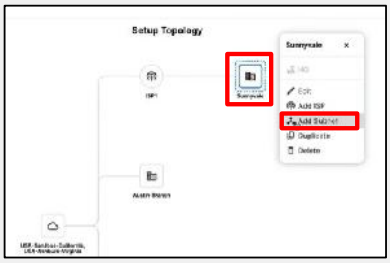
- Select primary and secondary hub devices



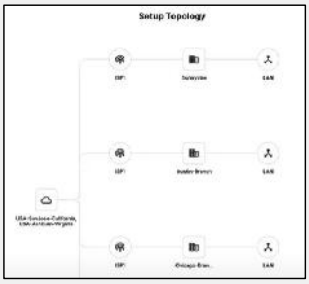

- Add company sites
  - Branches
  - Datacenters




- Define subnets and ISPs




- OaaS topology definition completed




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

To define your OaaS topology, you must first define the primary and secondary hubs. Click the hub icon, and then select the site that is the nearest to your branch site. Connecting to the nearest site provides better performances.

Once you have defined the two hubs, you add your company sites. For each site you set a name, the registered FortiGate device you want to use, and select the **Branch** or **Data Center** icon. The site type has impact on the configuration, it's for information only.

Then, for each site, you add the ISP and subnet definitions as shown in the example on this slide.

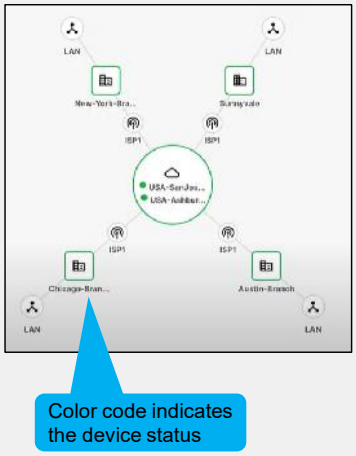
The last image on this slide shows an OaaS topology definition. You can click on any icon to review the configuration and update it.


Vouchers & Dumps are Available | WhatsApp +201224560923

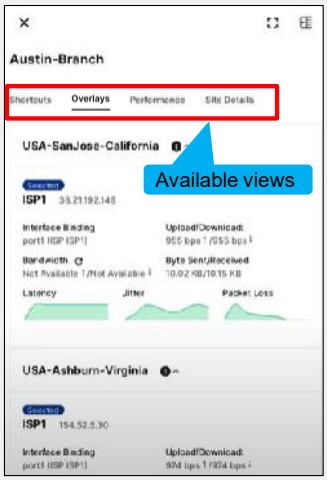
DO NOT REPRINT Brave-dumps.com
© FORTINET

# OaaS Day-to-Day Management Menus

- Home menu view status




- Click any site to monitor the device overlay status




- FortiGate GUI or CLI to manage the branches




- OaaS adds the prefix, **oaas**, to any policy or object name it creates
- Demo: OaaS configuration demo

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

This slide presents the management menus available for an active OaaS topology.

The OaaS **Home** page displays a graphical view of the devices. Colors indicates the status of each device—green indicates **All Pass**, orange indicates **Operational**, red indicates **Disconnected**, grey indicates **Unmanaged**. Click a site to display the device overlay or performance status.

OaaS updates the configuration of your branch device. OaaS adds the prefix **oaas** to any object or policy it creates. This allows you to easily identify these objects when you review the FortiGate configuration on the CLI or from the GUI. Note that OaaS creates firewall policies with wildcard address objects and services on the spoke FortiGate devices that allow all traffic. You can create new policies to provide the granularity you require to restrict overlay traffic to specific subnets or hosts.

To view a step-by-step initial OaaS configuration video, click the link shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

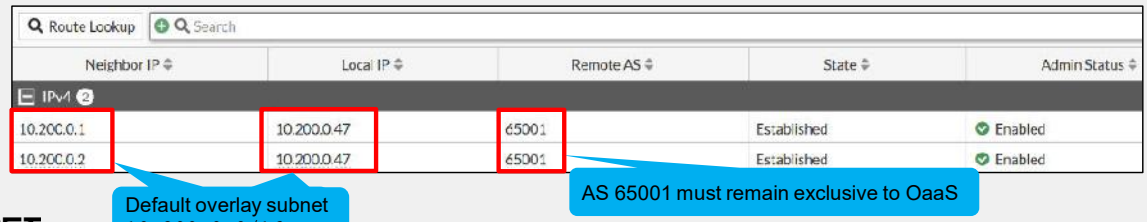
DO NOT REPRINT Brave-dumps.com
© FORTINET

## What Does OaaS Configure on Branches?

- IPsec tunnels
  - One tunnel per ISP (to the primary hub only)
- ADVPN parameters
  - Allows the establishment of shortcut tunnels between spokes




- BGP routing




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

When you deploy the configuration on branches, OaaS configures, on each branch, one IPsec tunnel interface for each ISP interface. On the cloud hubs, the corresponding remote end of the tunnel is already defined (dynamic tunnels). Note that tunnels are established with the primary hub only.

The IPsec tunnel includes the parameters required for ADVPN. This allows the establishment of shortcuts tunnels between the spokes. You will learn more about ADVPN in another lesson.

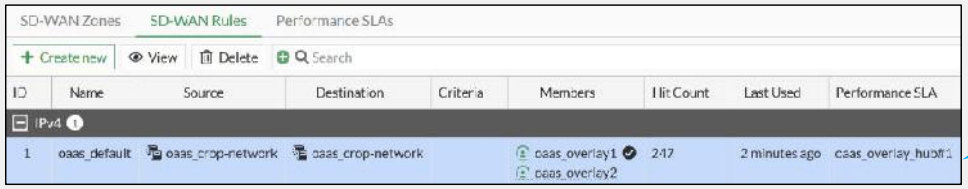
On the defined overlay topology, OaaS configure BGP routing. It use the autonomous system (AS) number 65001. You must keep this private AS number exclusively for this OaaS SD-WAN BGP configuration. OaaS reserves `10.200.0.0/16` for overlay IP addressing of all spokes, and you should not use this network in either the LAN subnets or WAN network. However, if this conflicts with your existing network configuration, you can modify the reserved subnet in the **Settings** view in the OaaS portal.


Vouchers & Dumps are Available | WhatsApp +201224560923

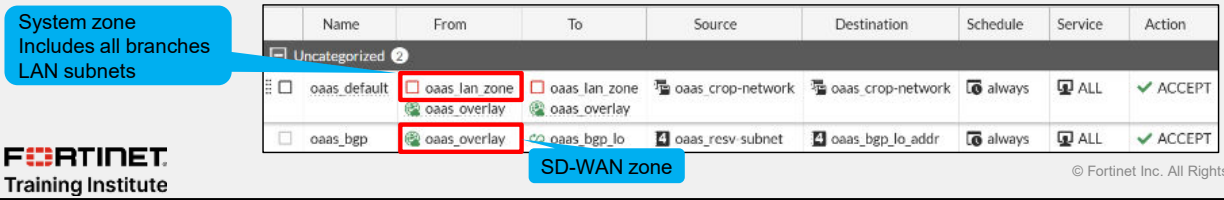
DO NOT REPRINT Brave-dumps.com
© FORTINET

## What Does OaaS Configure on Branches? (Contd)

- SD-WAN
  - Zones: One zone including all OaaS overlay interfaces
  - Rules: One default SD-WAN lowest cost (SLA) rule
  - Performance SLA: Monitor performances through each overlay and ADVPN shortcuts




- Firewall policies
  - One policy to allow traffic between the spokes LAN zones
  - One policy to allow health-check traffic to the hub and spoke loopback interfaces




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

OaaS defines SD-WAN settings on the branches. This includes:
- One zone that groups the OaaS IPsec overlay interfaces
- One performance SLA to monitor the performances through each overlay and the shortcuts established. By default, it defines the latency threshold to 100 milliseconds.
- One default SD-WAN rule—**oaas_default**. It's a lowest cost (SLA) rule that steers the traffic through the best performing overlay link, according to the latency.

OaaS defines also two firewall policies:
- One policy called **oaas_default** that allows all traffic flows between the spokes LAN subnets—grouped in a system zone **oaas_lan_zone**—and through the overlays—grouped in the SD-WAN zone **oaas_overlay**.
- One policy called **oaas_bgp** allows health-check traffic to the hub and spokes loopback interfaces.

The administrators can create additional policies to provide the granularity they require and further restricts overlay traffic to specific subnets or hosts.

OaaS will not affect any other FortiGate configuration settings and will create and modify only the configuration settings that it generated. Therefore, the FortiGate spoke administrator is free to add firewall policies and other configuration settings, as needed. When adjusting the configuration on the branches, the administrator can use the following elements created by OaaS:
- **oaas_lan_zone** (system zone)
- **oaas_overlay** (sdwan zone)
- **oaas_corp_network** (firewall addrgrp)


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe the IPsec and BGP settings required for overlays in a standard, BGP per overlay, hub-and-spoke deployment
- ✓ Configure BGP route reflectors to exchange prefixes between spokes
- ✓ Configure BGP to exchange all available paths
- ✓ Configure overlay stickiness to improve performance
- ✓ Describe OaaS, an overlay link service in the cloud hosted by Fortinet

FORTINET Training Institute

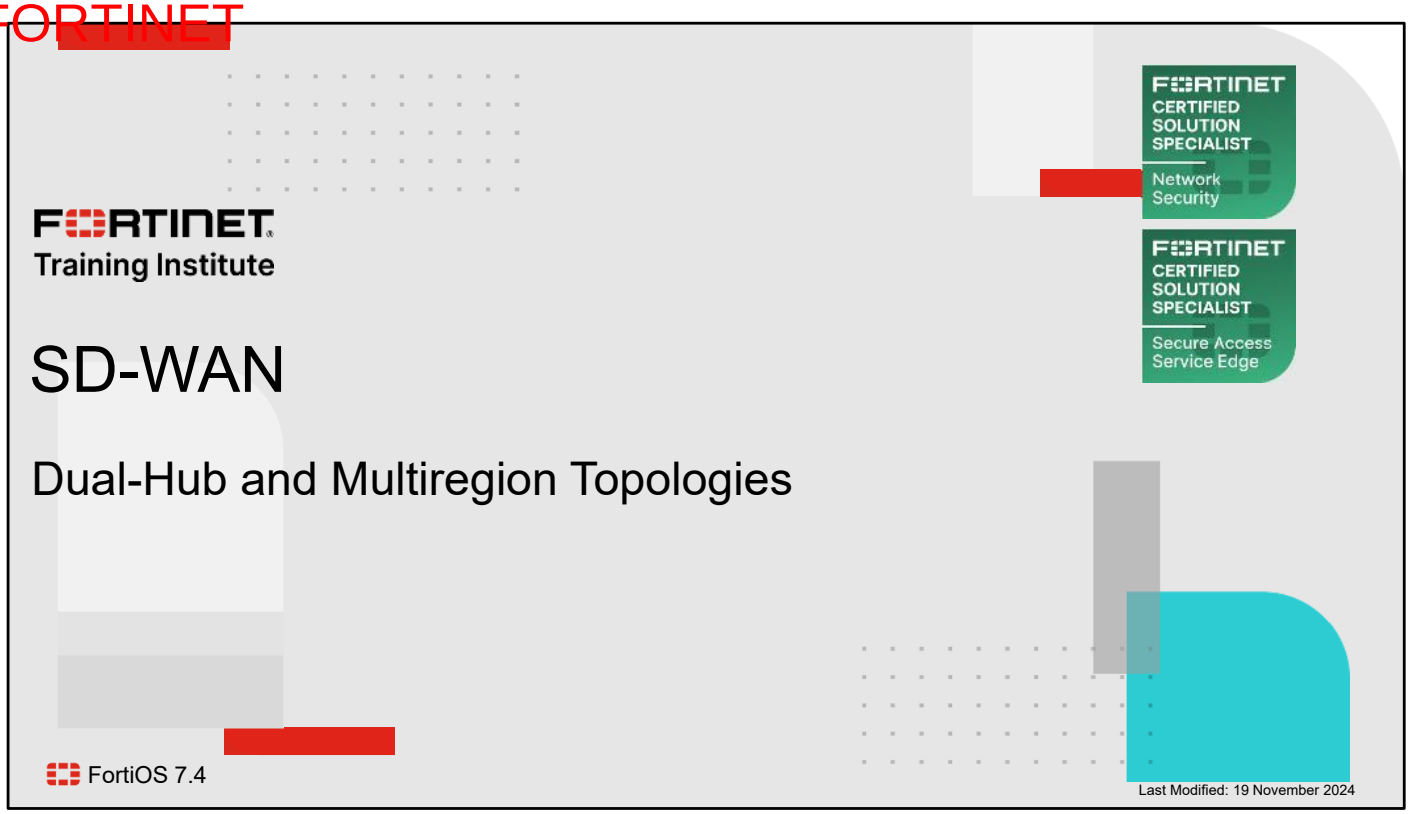
© Fortinet Inc. All Rights Reserved. 35

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure IPsec tunnels that are used as SD-WAN overlay links, and how to configure BGP routing with BGP per overlay, for SD-WAN basic hub-and-spoke topologies. You also learned how to use OaaS to deploy SD-WAN spokes with overlay links hosted in the cloud.


Vouchers & Dumps are Available | WhatsApp +201224560923

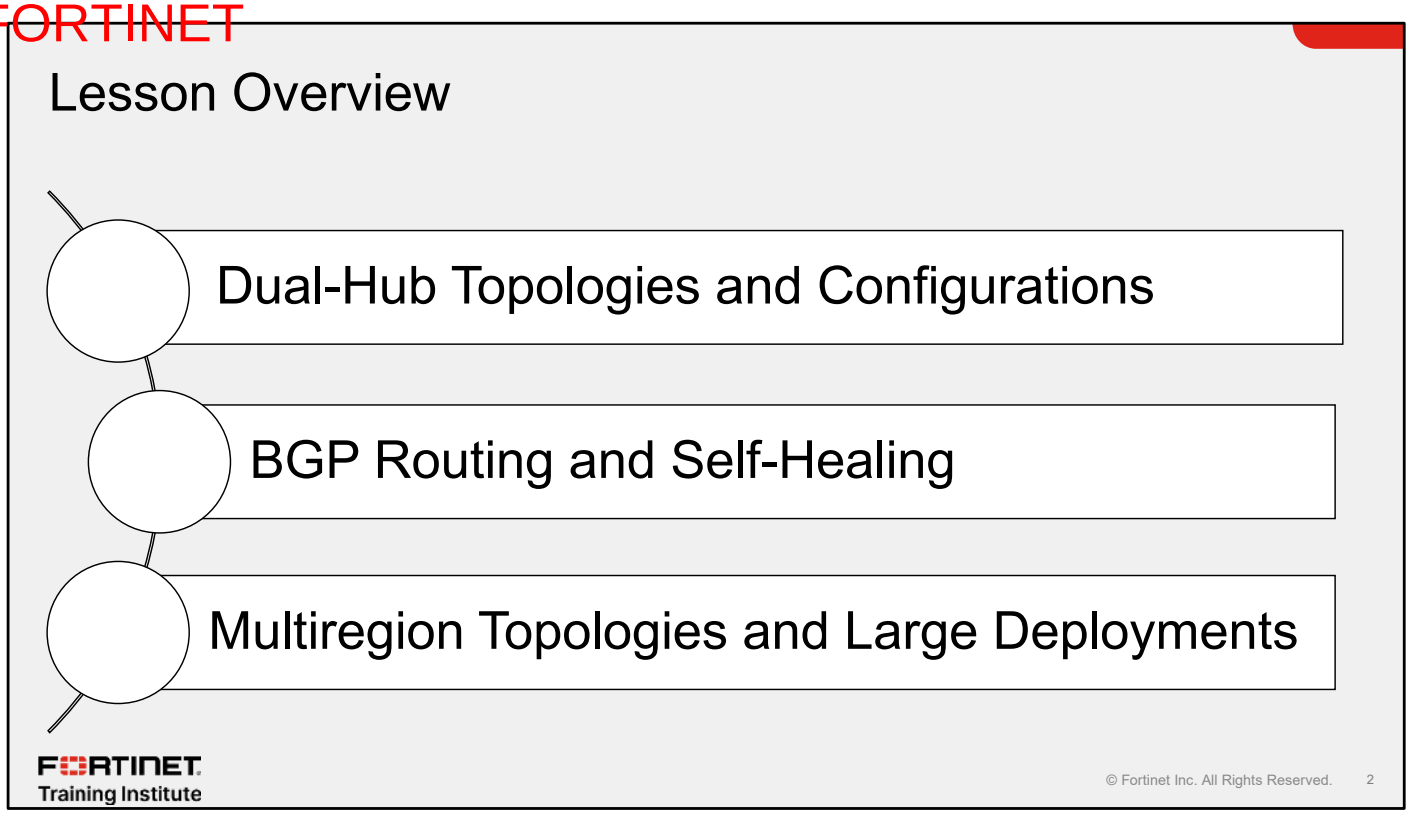
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about dual-hub and multiregion SD-WAN topologies, what is specific about those topologies, and how to configure them.


Vouchers & Dumps are Available | WhatsApp +201224560923

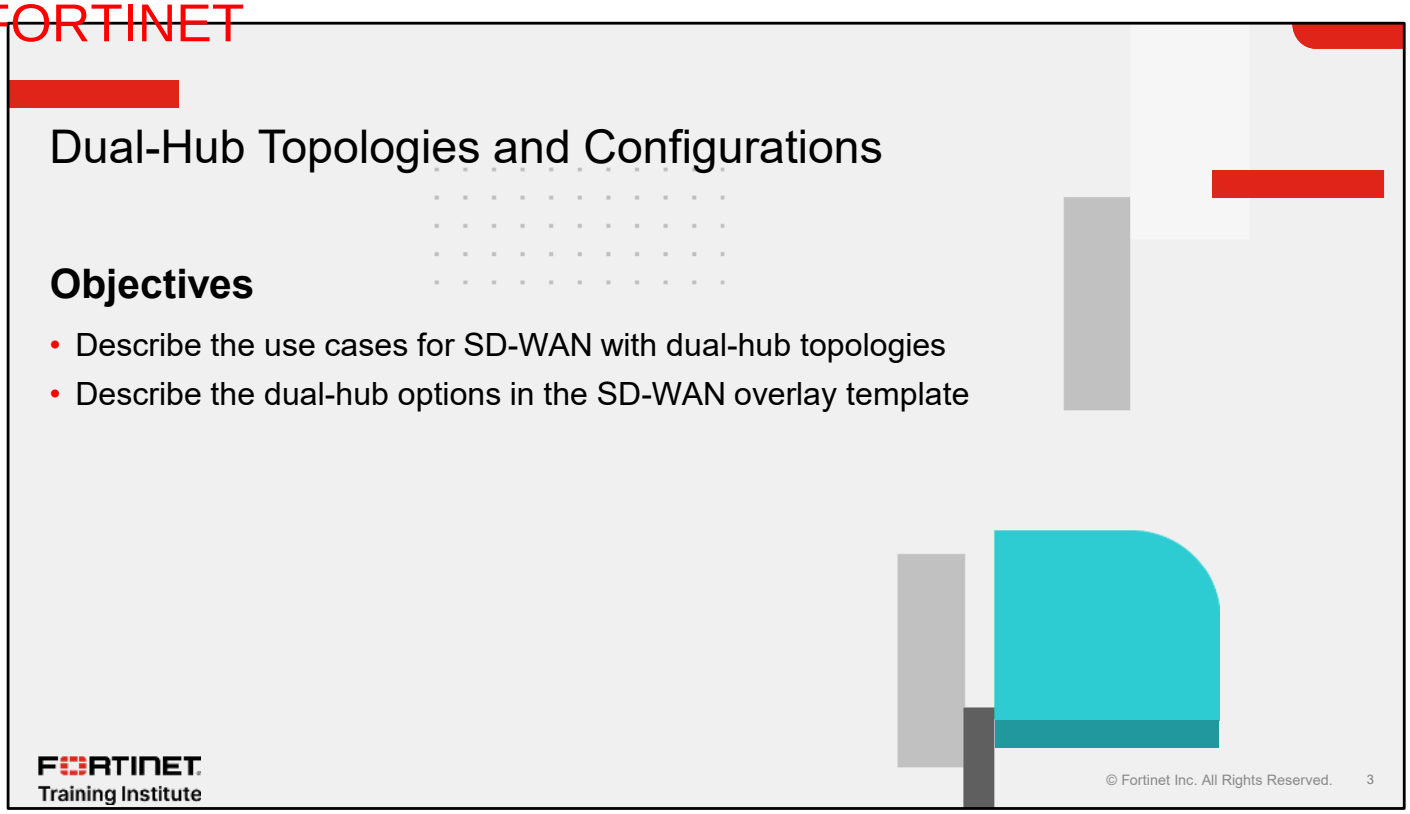
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this lesson, you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of how dual-hub SD-WAN topologies are used and the main configuration elements involved, and you will be able to configure a dual-hub topology using the FortiManager SD-WAN overlay template.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Dual-Hub Use Cases

- Dual SD-WAN attachment
  - Each site connects to two SD-WAN gateways—hubs
  - Physical or geographical redundancy
- Typical operation
  - Dial-up IPsec used for overlay
  - Each hub acts as a dial-up IPsec server
  - Overlays grouped per device and location
  - Dynamic routing
    - More scalable
    - IBGP recommended
- Auto-discovery VPN (ADVPN) possible

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

For larger deployments, you can extend the SD-WAN base design to include a second SD-WAN gateway. This second gateway can be housed in a different location to provide geo-redundancy.

In such topologies, spoke SD-WAN devices connect to two (or more) SD-WAN gateways. FortiGate steers traffic to one gateway or the other, according to the status, link health, and service-level agreement (SLA) of the devices.

For easier management and rule definition, the administrator groups overlay links for each device and location.

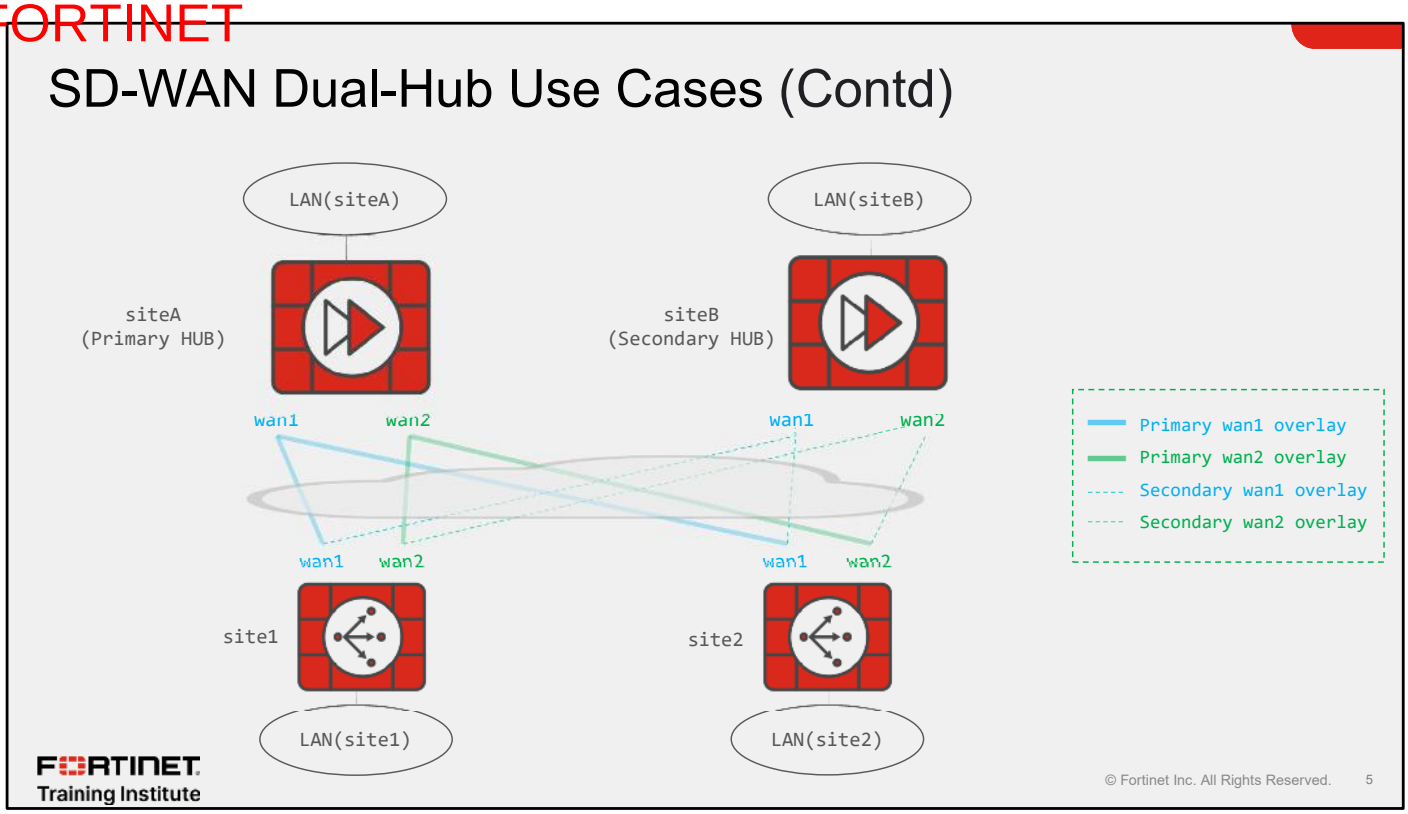
In addition to geo-redundancy, intra-site redundancy with a high availability (HA) cluster—FortiGate Clustering Protocol (FGCP) or FortiGate Support Protocol (FGSP)—remains possible.

You can combine a geo-redundant topology with ADVPN. You will learn more about configuring and using ADVPN in another lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Dual-Hub Use Cases (Contd)




This slide shows an example of a deployment that uses SD-WAN to steer traffic with hub redundancy. The hubs can be located in different building on the same campus or in different cities.

Each site has four overlays configured: two to the primary site—one on each WAN underlay link—and two to the secondary site. SD-WAN steers spoke-to-hub traffic to the primary hub, and continues to monitor the health of all overlay links. According to the rule definitions, SD-WAN triggers a fallback to the secondary hub, based on link quality or site availability.

Note that, for simplicity and ease of understanding, this slide represents the WAN links as direct connections. Note that usually the hubs and the spokes are in different locations and connect to each other through provider networks, commonly through an internet service provided (ISP), 4G/5G, or multiprotocol label switching (MPLS) links.

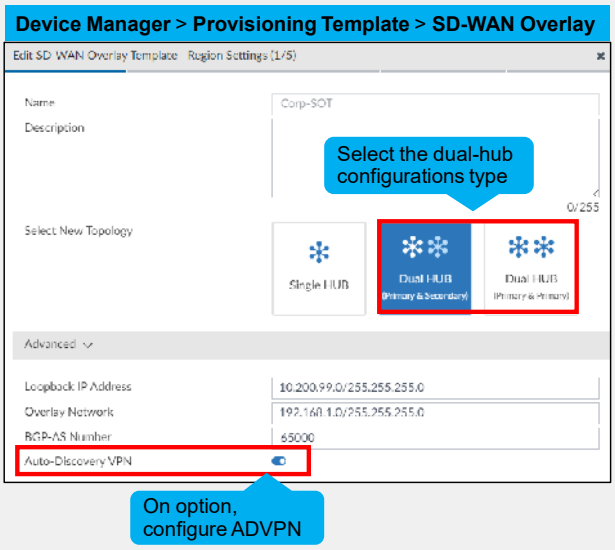


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Configure Dual-Hub With the SD-WAN Overlay Template

- Predefined settings for dual-hub topologies
  - IPsec
  - BGP with peering per overlay
  - Loopback IP address for each hub
  - SD-WAN health check on each hub
- Supports upgrades from single-hub topology
  - Easy topology upgrade
- Two options
  - **Primary & Secondary**
    - Tunnels established with both hubs
    - Secondary hub used only when performances of the primary degrades
  - **Primary & Primary**
    - Load sharing between the two hubs




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

When you use FortiManager and the SD-WAN overlay template to configure an SD-WAN topology, you can select from two dual-hub options.

The first, **Primary & Secondary**, defines an SD-WAN topology with two hubs, with one preferred over the other. Each spoke has an established IPsec tunnels with both hubs at all times. Under normal conditions, the spoke directs the traffic to the primary hub. If the performance of links to the primary hub degrades, the spoke directs traffic to the secondary hub.

The second, **Primary & Primary**, defines two hubs with similar characteristics and routing. Spokes can direct traffic to either hub, according to their SD-WAN rules and the performances of each link.

For both options, the FortiManager SD-WAN overlay template defines a dual-hub topology with BGP peering per overlay, a loopback IP address on each hub that is used for health checks, and an SD-WAN health check for each hub. It also prepares the IPsec and BGP templates for both hubs and for the spoke devices and, on the spoke SD-WAN configuration, defines one health check on each hub loopback IP address.



Vouchers & Dumps are Available | WhatsApp +201224560923

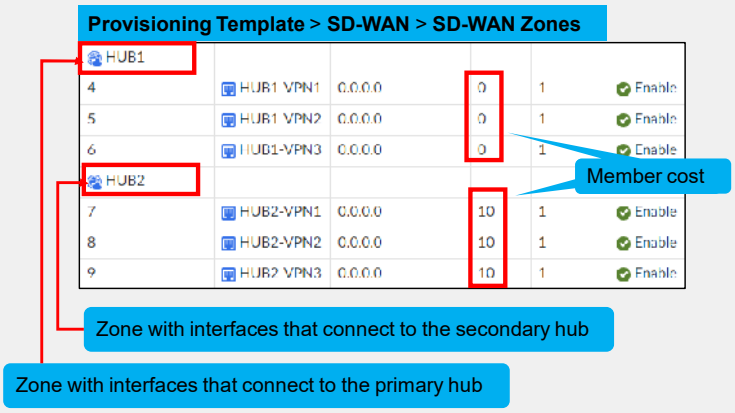
DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Member Priority to Differentiate the Hubs




- **Dual HUB (Primary & Secondary)**
  - Primary is the preferred hub
  - IPsec tunnels established with both hubs
  - Spokes direct traffic to the secondary hub if the performances of links to the primary hub degrades
- **Dual HUB (Primary & Primary)**
  - Both hubs handle traffic
  - Spokes directs the traffic to both hubs, according to the SD-WAN rules

- Similar configuration for the hubs
- On the branches:
  - Assign a higher SD-WAN member cost for interfaces to the secondary hub if it acts as **Secondary**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

With the SD-WAN overlay template, when you select **Dual HUB (Primary & Secondary)** or **Dual HUB (Primary & Primary)**, FortiManager generates similar configurations, except for one difference. In a **Dual HUB (Primary & Secondary)** deployment, on the spoke SD-WAN configuration, the secondary hub interfaces are assigned a higher cost than the primary hub interfaces.

When the configurations are defined by the template, the spoke establishes IPsec tunnels and BGP peering with both hubs, with no distinction of its status—primary or secondary. It is the spoke SD-WAN rules that steer the traffic in priority to the primary hub.

Remember the SD-WAN traffic steering rule strategies, and consider the behavior with dual-hub topologies:

- **Manual**: FortiGate prefers members according to configuration order. Then, the administrator must place the member connected to the primary hub before the members connected to the secondary hub, in each manual rule.
- **Best Quality**: FortiGate prefers the best-performing member based on the configured quality criteria. The factors that FortiGate considers are the member priority, the link-cost threshold, and the metric. As for manual rules, the administrator must place the member connected to the primary hub before the members connected to the secondary hub, in each best quality rule.
- **Lowest Cost (SLA)**: FortiGate prefers the member that meets the configured SLA target. If multiple members meet the SLA target, member cost, followed by the configuration order, are used as tiebreakers.

The SD-WAN lowest cost (SLA) strategy considers the member cost as the first discriminator if multiple members meet the SLA target. Therefore, this strategy natively directs the traffic to the primary hub, as long as its members meet the SLA target.

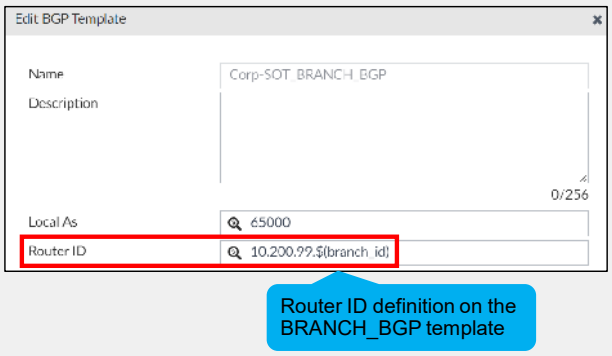


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## BGP Router ID—Scalability Limits

- Router ID for the branches defined with metadata variable




Router ID definition on the BRANCH_BGP template

- Limited to 255 branches

- Alternative
  - Use a Jinja script to define the router ID

```
Config router bgp
   set router-id {{'10.200.99.0'|ipmath(branch_id|int)}}
end
```

  - Calculation results

Increment the network value

```
Branch ID 154:     < 255      => router ID 10.200.99.154
Branch ID 256:     > 255      => router ID 10.200.100.0
Branch ID 320: 320-256=64     => router ID 10.200.100.64
```

FortiManager install preview

```
    edit "HUB2-VPN3"
        set localid "Branch320"
        unset idle-timeout
        unset auto-discovery-receiver
    next
end
config router bgp
    set router-id 10.200.100.64
end
```

Router ID

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

When you configure a router ID for the branches with FortiManager, you can build the router ID with a predefined network part and a metadata variable that corresponds to the branch ID. This simple method works well for up to 255 branches. Because the BGP protocol requires that the router ID is defined with an IP address format, you must use a different formula if your network has more branches.

The example shown on this slide shows a Jinja script that defines the router ID with a predefined network part and a calculation done on the branch ID. Using the formula `ipmath`, FortiGate increases the value of the predefined network part to provide a valid router ID for branches with a device ID above 255.

If you use the FortiManager SD-WAN overlay template, FortiManager defines the Jinja overlay script for you in a CLI script—`Corp-SOT_BRANCH_CLI`. The router ID that FortiManager calculates with the CLI script overwrites the one defined in the BGP template, if both are used.

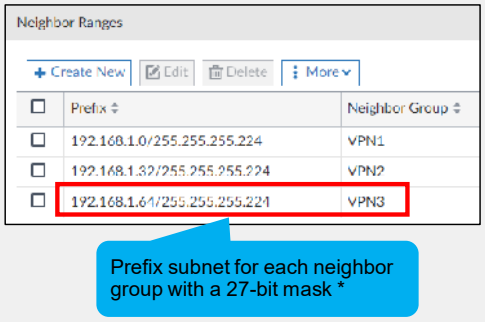


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Overlay Template—Scalability Limits

- BGP neighbor ranges on the hubs
  - One prefix range per overlay and per hub
  - Example: dual-hub topology with 3 overlays




* The number of available hosts in each subnet corresponds to the number of spokes that each design supports

- Example details:
  - Class C overlay network (24-bit mask)
  - Three overlays
    - With one hub, FortiManager subdivides the overlay network with a 26-bit mask
      - 4 available subnets
      - 61 host addresses in each*
    - With two hubs, FortiManager subdivides the overlay network with a 27-bit mask
      - 8 available subnets
      - 30 hosts addresses in each*
- Alternatives
  - Use a class A overlay network (8-bit mask)
    - Subdivide with an 11-bit mask
      - 8 available subnets
      - 2.097.150 hosts addresses in each*
  - Use a class B overlay network (8-bit mask)
    - Subdivide with a 19-bit mask
      - 8 available subnets
      - 8190 hosts addresses in each*

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

With the SD-WAN overlay template, the administrator defines a subnet for the overlay network. Then, FortiManager subdivides this subnet to attribute a range of IP addresses to each neighbor group. For dual-hub topologies, FortiManager subdivides the subnet one more time to distribute the IP addresses between both hubs—each spoke establishes BGP peering with each hub and requires an IP address from each subnet on each hub. The number of IP addresses available in each of these groups determines the number of spoke devices that the topology can support.

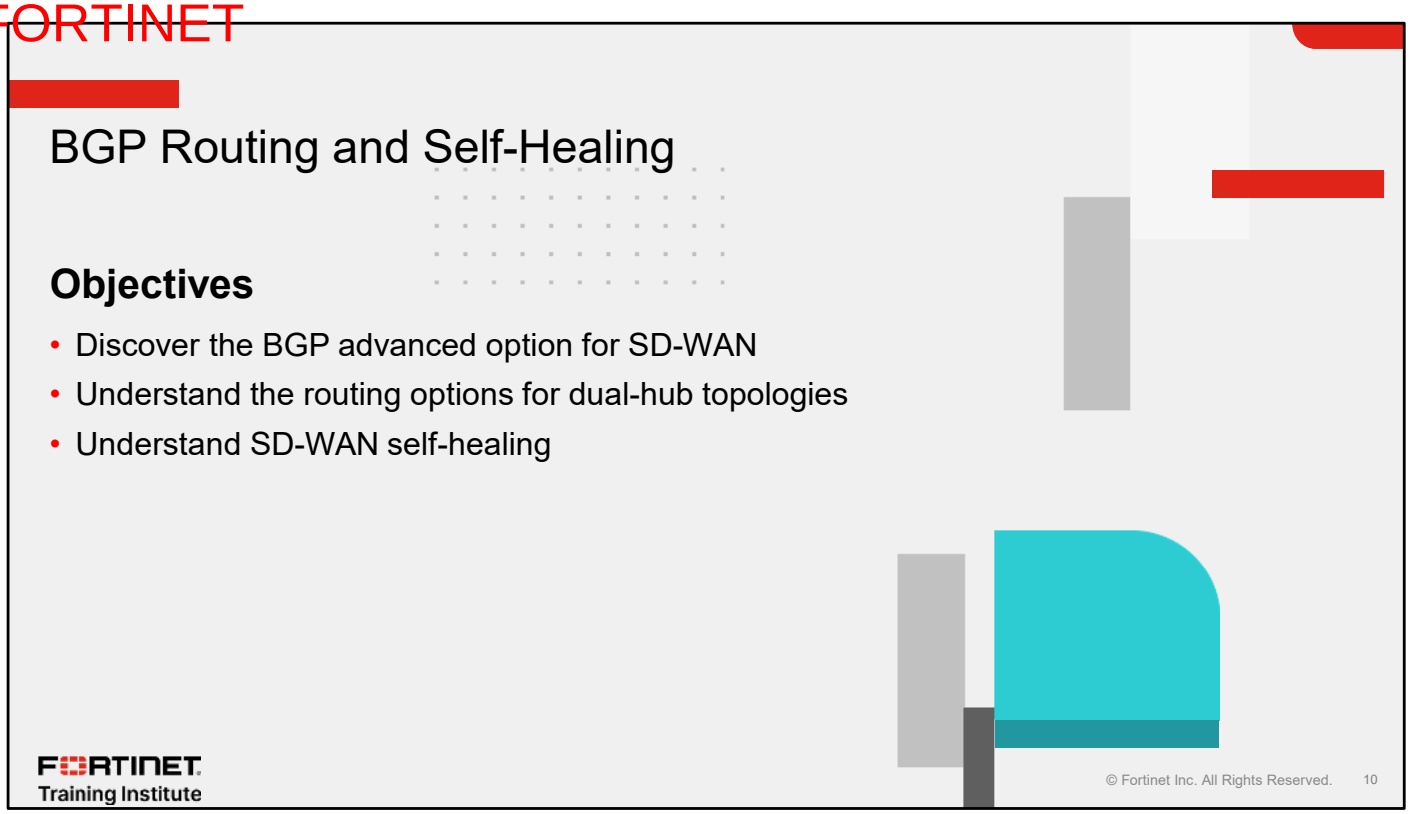
If the administrator defines a class C overlay network (24-bit mask), with one hub and three overlays, the BGP template defines three address ranges with a 26-bit mask (`255.255.255.192`). With two hubs and three overlays, the BGP template defines the address ranges with a 27-bit mask (`255.255.255.224`). That corresponds to 8 available subnets and 30 hosts addresses in each. This means that, with two hubs and three overlays, a class C overlay network can accommodate, at the maximum, 30 spoke devices.

With the same topology, a class B overlay network provides enough addresses for more 8,190 spokes, and a class A overlay network provides enough addresses for more that two million spokes. By default, the SD-WAN overlay template use the class B overlay network `10.10.0.0/16`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding BGP advanced options for SD-WAN networks, you will be able to configure BGP routing for SD-WAN in the context of dual-hub topologies.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## BGP for SD-WAN Traffic

- SD-WAN rules can use BGP routes to steer traffic:
  - iBGP
  - eBGP
- BGP options for SD-WAN
  - BGP tags
    - SD-WAN rules steer traffic to routes using the specified route tags
  - SD-WAN self-healing
  - Route mapping according to SLA status
    - `route-map-out-preferable`
    - `minimum-sla-meet-members`
  - BGP neighbor status
    - Primary–Secondary
    - Standalone

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

A key routing principles of SD-WAN is that SD-WAN requires a valid route in the forwarding information base (FIB) so the member can be used to steer traffic. The required valid route can be static or dynamic. You can combine the use of SD-WAN and the main dynamic routing protocols—OSPF and BGP. Fortinet recommends the use of BGP in the overlay, because it allows the routing and steering of SD-WAN traffic based on health-check results. In this lesson, you will learn how to use health-check results to adjust BGP routing.

You can combine SD-WAN with iBGP or eBGP. This lesson focuses only on what is specific for SD-WAN.

When using SD-WAN with BGP routing, you can:
- Configure SD-WAN rules to steer traffic to members, only if routes have a specific route tag.
- Interact with a BGP neighbor to optimize route selection—called SD-WAN self-healing.
- Use a route map that relates to the SLA status with the following parameters: `route-map-out-preferable` and `minimum-sla-meet-members`.
- Define a primary or secondary role for BGP neighbors.

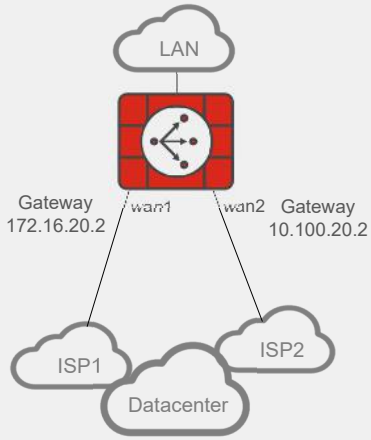
Note that you can use many BGP options for single hub topologies, but you will learn about them in this lesson because they are particularly useful for dual-hub or multiregion topologies.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## BGP Tags

- Use BGP tags in SD-WAN rules
  - Example: Use a tag to apply a service rule for traffic to the data center




Set the tag to route, received from ISP2 to the data center

Firewall address object of type `route-tag`

```
config router community-list
    edit "30:5"
      config rule
         edit 1
            set action permit
            set match "30:5"
         next
        ...
config router route-map
    edit "comm1"
      config rule
         edit 1
           set match-community "30:5"
           set set-route-tag 15
         next
        ...
config router bgp
    config neighbor
      edit 10.100.20.2
        set remote-as 65001
        set route-map-in "comm1"
        ...
config firewall address
     edit "DC_route_tag_15"
        set type route-tag
        set route-tag 15
     next
end
```

FORTINET Training Institute

12

You can use BGP route tags to determine where an SD-WAN rule steers the traffic.

In the example shown on this slide, a customer has two ISP connections: wan1 and wan2. FortiGate uses wan1 primarily for direct access to internet applications, and uses wan2 primarily for traffic to the corporate data center. The data center does not benefit from a static IP address. It receives a dynamic IP address provided by the ISP. Therefore, the administrator cannot configure SD-WAN rules based on addresses. As an alternative option, the administrator can use BGP tags.

Note that the way you configure SD-WAN to use route tags has changed in FortiOS 7.4.0. What is presented on this slide does not apply to earlier FortiOS versions. Also note that, though not presented in this lesson, you can use route tags with any size of network.

The CLI example on this slide shows how an administrator can use BGP tags in SD-WAN rules.

First, the administrator defines a `community-list` rule and a `route-map` to associate the community number received in the route advertisement with a route tag. In the example, the BGP neighbor wan2 advertises the data center network range with a community number of 30:5 and administrator associates this community number with `route-tag 15`. Then, in the FortiGate BGP router configuration, you associate the route mapping defined as `route-map-in` for the BGP neighbor.

In FortiOS 7.4, you define a firewall address object of type `route-tag`.

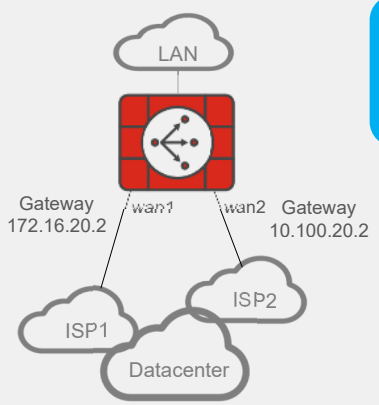


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## BGP Tags (Contd)

- Use firewall address object of type route-tag as:
  - Destination address in firewall policies
  - SD-WAN service destination




The firewall policy allows the traffic from the LAN to the SD-WAN zone underlay, if the destination corresponds to a route with the tag 15

```
config firewall policy
   edit 1
      set srcintf "LAN"
      set dstintf "underlay"
      set srcaddr "all"
      set dstaddr "DC_route_tag_15"
      set action accept
      set nat enable
      ...
   end
config system sdwan
    config service
      edit 1
        set name "DataCenter"
        set mode manual
        set priority-members 2
        set dst "DC_route_tag_15"
        next
        ...
```

Use the route-tag firewall address object as the SD-WAN rule destination

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

After you configured the route-tag firewall address object as shown in the previous slide, you can use it as destination address for firewall policies and the SD-WAN service rule.

In the example shown on this slide, the administrator defined:
- A firewall policy to allow the traffic from the `LAN` interface to the SD-WAN zone `underlay`, if the destination address corresponds to the `route-tag` address object `DC_route_tag_15`.
- An SD-WAN rule that steers the traffic that corresponds to the address object `DC_route_tag_15` through the priority member `2`. Not shown on this slide, the priority member `2` corresponds to the interface `wan2` and belongs to the SD-WAN zone `underlay`.

Note that BGP route tags do not show up in the routing table. You can use the command `get router info bgp network` to review the tag assigned to each network.

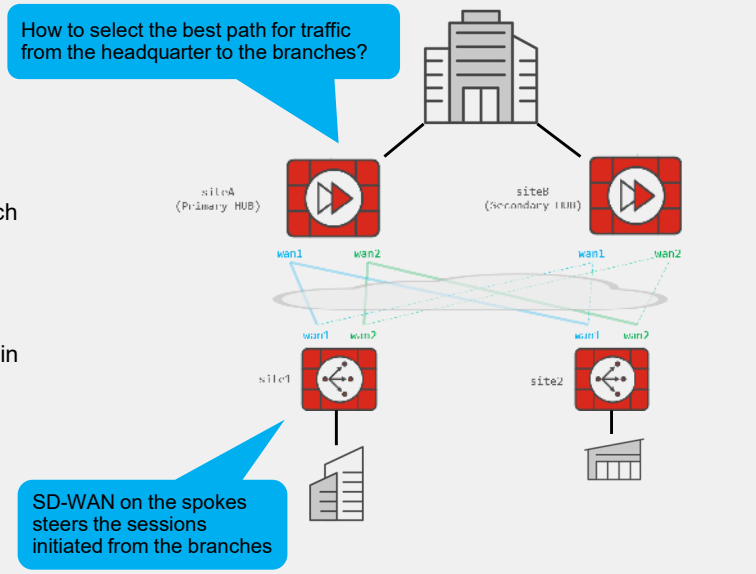


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Hub-to-Edge SD-WAN

- SD-WAN on the hub?
  - Objective: Use the best path for sessions initiated from the hub local site
  - Suboptimal:
    - Scaling issue: The hub needs to monitor the health of hundreds of overlays
    - The spokes already monitor the health of each overlay
- Alternative solutions
  - Remote health probing
    - The spoke embeds the health measurement in the probe packets
  - Advertising a preferred hub
    - Uses the BGP route maps
    - The spoke influences the route selection on the hub
    - Also known as SD-WAN self-healing




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

The term hub-to-edge SD-WAN refers to the need for intelligent steering of the traffic originating behind the hubs. It is important to highlight that this does *not* refer to the *replies* to the sessions originated by the spokes. By default, the hub FortiGate device, automatically follows a symmetrical path for the reply to sessions initiated from the spoke. The reply packets automatically prefer the same overlay on their way back from the hub.

While, in theory, you could configure SD-WAN in a classical way on the hubs, and let the hubs measure the health of all the overlay paths towards all the spokes, this design would be suboptimal for at least two reasons. First, it creates a scaling issue, a single hub should be able to measure the health of hundreds and thousands of overlays to the spokes. Secondly, it is a duplicate effort, each spoke already measures the health of the overlay paths towards its serving hubs, usually by actively sending ping probes over each overlay tunnel.

FortiGate offers a few options to effectively distribute the sessions originating from behind the hubs to the preferred overlay, without active overlay monitoring on the hub. You can configure the spokes to embed their health measurements (latency, jitter, and packet loss) into the probe packets themselves. When these probes arrive at the hubs, the hub reads the measurements and uses the results to determine the path to use. This method is called remote health probing. Alternatively, you can configure the spoke to act on the routes advertised to the hub and, this way, influence the path selection on the hub. This method is sometimes called SD-WAN self-healing.

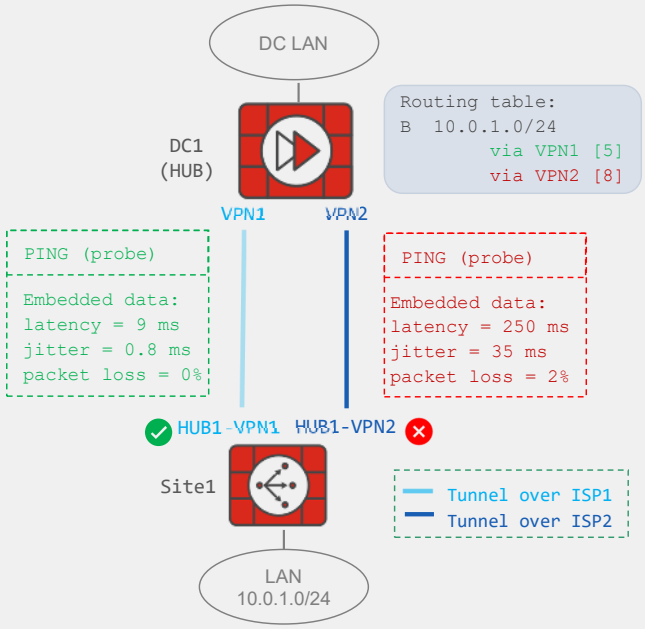


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Remote Health Probing

- Objectives
  - Inform the hub about the link health
  - Allow symmetric link selection
- Principle
  - SLA information embedded in ICMP probes
  - Hub learns from remote devices
- Limitations
  - Active probe mode
  - Health check with ping protocol
  - The hub must be a FortiGate device
  - Only one SLA criteria per hub




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

With remote health probing, the spoke embeds SD-WAN SLA information in Internet Control Message Protocol (ICMP) probes. This way, the spoke communicates the SLA status to the hub for each overlay, directly through ICMP probes. The hub can use the received SLA status information to apply priorities to the IKE routes, giving routes over overlays that are inside SLAs a lower priority value than routes over overlays that are outside of SLAs.

This method is particularly useful in combination with BGP and loopback topologies or with static routing. With BGP routing, when not on lookback topologies, you can use remote health probing or the SD-WAN neighbor feature `route-map-out-preferable` to signal the health of each overlay to the hub.

Note that to use remote health probing, you must configure active probing on the spokes and use ping as the health-check protocol. The remote health probing allows you to transmit one SLA criteria only to each hub device. Also note that, the hub must be a FortiGate device on which you configure SD-WAN with health check defined to use the information received from the spokes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Remote Health-Check Configuration—CLI

- Spoke side
  - Embed SLA measure in health check

```
config system sdwan
    config health-check
        edit "to_hub"
            set server "4.2.2.1" "4.2.2.2"
            set detect-mode active
            set protocol ping
            set embed-measured-health enable
            set members 3 4
            config sla
               edit 1
                set link-cost-factor latency
                set latency-threshold 100
            end
        next
    end
end
```

- Hub side
  - Use SLA result provided by remote device

```
config system sdwan
    config health-check
        edit "from_spoke"
            set detect-mode remote
            set sla-id-redistribute 1
            set members 1 2
            config sla
               edit 1
                set link-cost-factor latency
                set latency-threshold 100
                set priority-in-sla 10
                set priority-out-sla 20
            end
        next
    end
end
```

Matching SLA criteria on hub and spoke

Lower value for higher priority route

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

This slide shows example CLI configurations that use parameters introduced in the *Members, Zones, and Performance SLAs* lesson.

On the spoke, you activate transmission of SLA information in the ICMP probe using the command `set embed-measured-health enable`. On the hub, you use the command `set detect-mode remote` to instruct the device to get SLA information from received SLA probes. On the hub, you must also define the priority to assign to IKE routes depending on whether the corresponding overlay is in SLA or out of SLA. You do this with the commands `set priority-in-sla` and `set priority-out-sla`. The lower the priority of an interface is, the more preferrable it becomes when considered with static routing. Optionally, you can define the SLA entry that is applied to the IKE routes using the parameter `sla-id-redistribute`.

For consistency, when using the remote detect mode, you must specify the same link cost factor and metric on the spoke and the hub. In the example shown on this slide, the SLA measures latency with a threshold set to 100.

You can use the embedded SLA mechanism with static routing or BGP for each overlay topology. However, note that to use embedded SLA with BGP, you must use static IP addressing for tunnels. It is commonly used with BGP on loopback. It is not compatible with the IKE option `mode-cfg`.

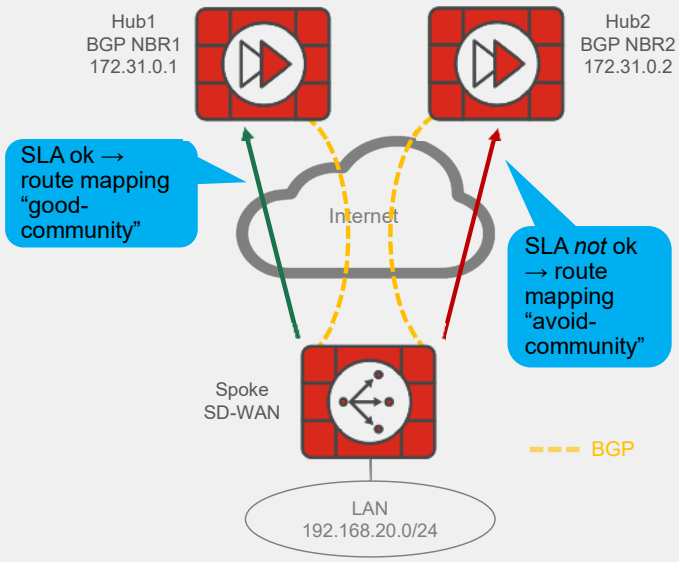


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Self-Healing With BGP

- BGP route mapping to inform BGP neighbors of link SLA status
  - BGP route-map-out adjusted from SLA status
    - `route-map-out-preferable`
      - Route mapping when SLA passed
    - `route-map-out`
      - Route mapping when SLA missed
- BGP peer
  - Non-SD-WAN device
    - Routes traffic according to standard BGP rules
    - Can be any BGP device
    - Adjusts routing from information received in BGP routing updates
  - SD-WAN device
    - Adjusts routing from information received in BGP routing updates
    - No health check needed
    - Uses rules to steer traffic from health information received




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

SD-WAN allows you to select different outbound WAN links based on performance SLAs. When a device selects a link to forward traffic, it is useful to inform BGP neighbors about this choice and allow them to adjust routing accordingly. This can limit use of bad performer links and avoid asymmetric routing. It is called SD-WAN self-healing with BGP.

On FortiGate, BGP advertisements can adapt to the SLA status of a link in the following ways:
- Apply different route maps based on SD-WAN health checks. For example, it can advertise different BGP community strings when SLAs are met or not.
- Forwards traffic based on the active BGP neighbor.

Use the following BGP parameters to adjust route maps according to SD-WAN health checks: `route-map-out` and `route-map-out-preferable`. When the SLAs are met, FortiGate advertises routes with settings defined with `route-map-out-preferable`. When SLAs are missed, it advertises routes with settings defined with `route-map-out`.

The BGP peer does not need to be compatible with SD-WAN:
- If the BGP peer is a device with standard BGP routing features only, it will adjust its routing from advertisement fields received from the SD-WAN device—usually community or route tag.
- If the BGP peer is an SD-WAN device, it does not need to run its own health check. The administrator can configure the SD-WAN service rules to match each route tag and steer traffic to the corresponding VPN overlay when the neighbor link is healthy.

Note that, because all branches advertise the same community strings and route tags, you need to configure only one set of service rules on the hub for all branches. No additional settings are needed when new branches join the network. This feature makes this solution easily scalable.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

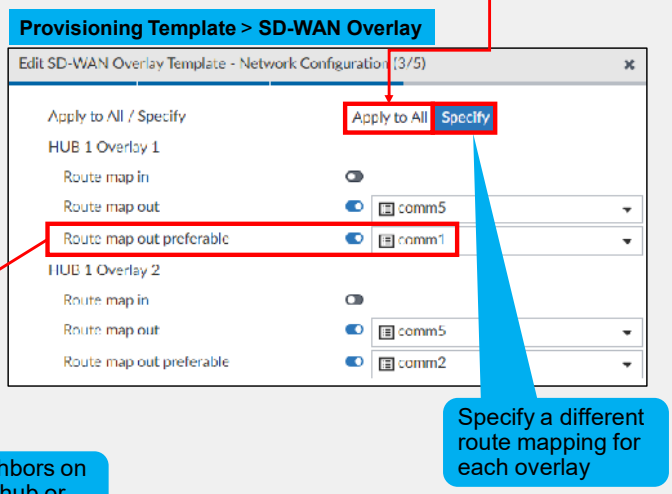
## Route Map Configuration on Spokes

- Configure a route map

```
config router route-map
    edit "comm1"
      config rule
         edit 1
            set match-ip-address "net192"
            set set-community "65000:11"
         next
       ...
```

- Configure route mapping for BGP neighbors

```
config router bgp
    config neighbor
      edit "172.31.0.1"
         set route-map-out "comm5"
         set route-map-out-preferable "comm1"
      next
      edit "172.31.0.2"
         set route-map-out "comm5"
         set route-map-out-preferable "comm2"
      next
    end
```




BGP neighbors on the same hub or on different hubs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

This slide shows the CLI configuration for route mapping based on the diagram shown on the previous slide and the equivalent route mapping configured with the FortiManager SD-WAN overlay template.

FortiGate advertises the route to local network `192.168.20.0/24` with a different community according SLA status.

First, you define the router access list `net192` for prefix `192.168.20.0/24` (not shown).
Next, you define the following route mapping:
- Use community 65000:11 for the neighbor `172.31.0.1` preferred route map (`comm1`).
- Use community 65000:21 for the neighbor `172.31.0.2` preferred route map (`comm2`).
- Use community 65000:50 if no SLAs are met (`comm5`).

For BGP neighbor configuration, use two route maps: `route-map-out-preferable` to define mapping when the SLA is met and `route-map-out` for mapping when the SLA fails.

Note that you can use the `route-map-out` and `route-map-out-preferable` to advertise different BGP communities on healthy and unhealthy links to BGP neighbors with different type of topologies.
- With single-hub topologies and BGP per overlay: This will inform the hub of the overlay to use to route the traffic to the spoke. It requires a different health check for each overlay.
- With dual-hub topologies and BGP on loopback: This will communicate different routes to each hub according to the health of the links.

Note also that, regardless of the type of topology used, you must define the SD-WAN neighbors to allow SLA differentiated route mapping.

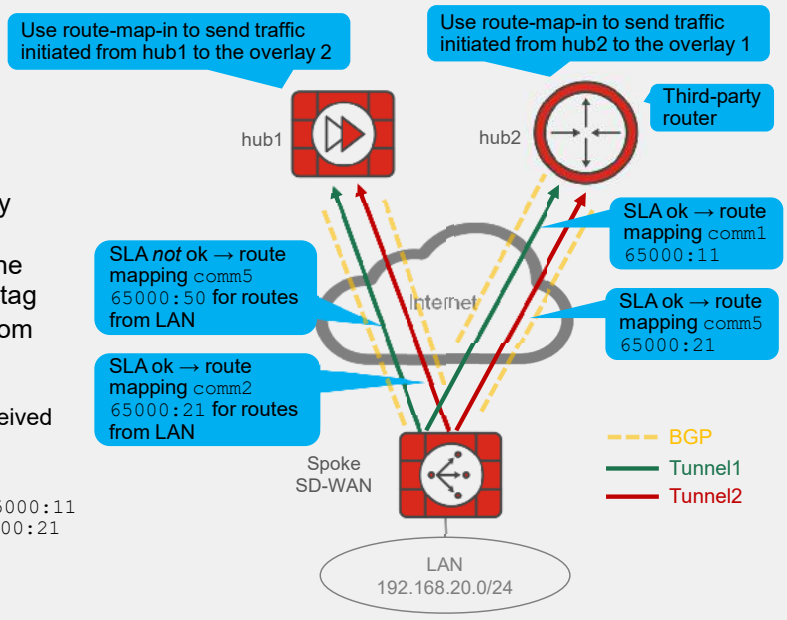


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Route Map Preferable—BGP Configuration on Hubs

- Hubs can be any BGP device
  - FortiGate with SD-WAN
  - FortiGate without SD-WAN
  - Third-party device
- Standard BGP configuration
  - Adjust routing according to the community received
  - Configure `route-map-in` to associate the community received to metric, priority, or tag
  - Use the `route-map-in` to send traffic from hub local subnets:
    - Prefer routes received with community `65000:11` or `65000:21` over routes received with community `65000:50`
    - Optionally:
      - Prefer routes received with community `65000:11` over routes received with community `65000:21`




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

When you `configure route-map-out-preferable` and `route-map-out` on an SD-WAN spoke, you can use the community to adjust the routing on the hub. Note that you don't need to configure SD-WAN on the hub to benefit from the BGP self-healing feature. In fact, the hub doesn't even need to be a FortiGate device, it can be any BGP router.

The SD-WAN spoke uses community, which is a BGP standard parameter, to inform the hub of the status of a link. The spoke associates a different community to the route advertised through a link according to the link status. It sets a "good" community if the link meets the configured SLA, and a "bad" community if it does not.

The administrator can then use the received communities to adjust the hub configuration and force it to route traffic, based on priority, to the links with the best SLAs—as measured by the spokes. BGP offers multiple options to define route priorities from the communities received. The most common are the route metric, the route priority, and the tag.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## BGP Configuration on FortiGate Hubs—Example

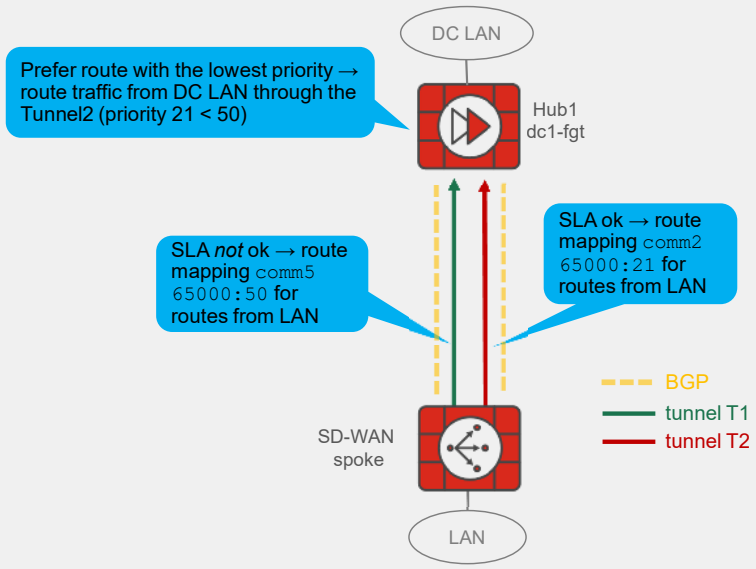
- Configure community list

```
dc1_fgt # config router community-list
    edit "comm1"
        config rule
            edit 1
                set action permit
                set match "65000:11"
            next  ...
```

- Configure route map-in

```
dc1_fgt # config router route-map
    edit "pref-1"
      config rule
         edit 1
            set match-community "comm1"
            set set-priority 11
         next   ...
```

- Route with the lowest priority is preferred
  - The hub prefers the route with priority 11 for the traffic from the DC LAN to the SD-WAN spoke
  - Second choice, the route with priority 21
  - Last choice, any route with a priority 50




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

This slides shows an example of the BGP configuration on the hub that uses BGP self-healing.

On the spoke, SD-WAN measure the link quality of the overlay tunnels `T1` and `T2`. The administrator configures `route-map-out-preferable` with the community `comm1, 65000:11` for tunnel1, the community `comm2 65000:21` for tunnel2, and `route-map-out` with the community `65000:50 for both tunnels`. The purpose of those settings are to use SD-WAN self-healing with BGP.

On the hub, you didn't configure SD-WAN but still want to select the overlay with the best measured quality to route the traffic from the DC LAN to the spoke LAN. For this, you can configure community lists that match the community received in the route advertisements received from the spoke—in this example, comm1 for 65000:11, comm2 for 65000:21, and comm5 for 65000:50. Then, you configure route mapping for the route received with the goal to associate a priority to the routes received according to their community—in this example, priority 11 for comm1, priority 21 for comm2, and priority 50 for comm5. As a result, using standard BGP techniques, the hub routes in priority the traffic through the overlay with the best quality, according to the status information it receives from the spoke.

On the diagram shown on this slide, the SLA on the tunnel `T1` is not good, so the spoke sends the community `comm5` that corresponds to the `route-map-out` setting. The tunnel `T2` is within SLA, so the spokes advertise the corresponding route with the community `comm2` that corresponds to the `route-map-out-preferable` setting. Then the hub prefers the tunnel `T2` to route the traffic to the spoke because the corresponding routes have the lowest priority.

This example uses the priority to select the preferred route on the hub. You have multiple options to take advantage of the community received from the spoke to select the best route for the traffic initiated behind the hub. The most common solutions use the route tag, the route priority, or the route metric.

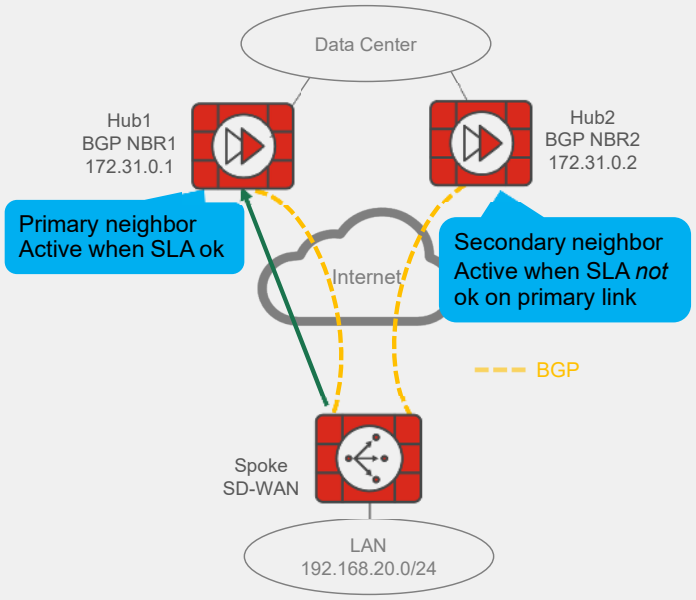


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Primary and Secondary Neighbors

- Defines hub types for a dual-hub topology:
  - Primary
    - Preferred neighbor if SLAs are met
  - Secondary
    - Active neighbor if primary SLAs are not met
  - Standalone
    - Default status (if primary/secondary not set)
    - Fallback mode if the SLAs for primary and secondary neighbor are not met




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

In a dual-hub topology, you can set one hub as active and the other as standby. The link SLAs determine which hub to use. To achieve this, you define a `primary` and a `secondary` BGP neighbor on the SD-WAN spoke device. The spoke directs the traffic to the primary hub when link SLAs are met. If SLAs are not met for the primary device, and SLAs for the secondary unit are still within threshold, the spoke adjusts the BGP routing to directs the traffic to the secondary unit.

If you don't set primary and secondary roles for SD-WAN BGP peers, the default standalone mode applies. FortiGate establishes BGP peering with both hubs without considering SD-WAN SLAs.

If you do set the primary and secondary roles, if neither the primary nor secondary neighbors are active (SLAs missed), the SD-WAN neighbor status becomes standalone. Only service rules with standalone action enabled will continue to pass traffic. This option is disabled by default.


Vouchers & Dumps are Available | WhatsApp +201224560923

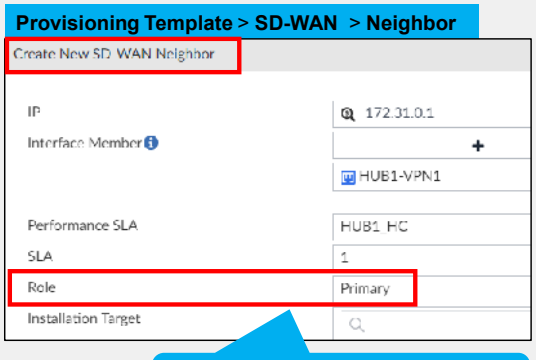
DO NOT REPRINT Brave-dumps.com
© FORTINET

# Neighbor Role Configuration

- Define the SD-WAN spoke BGP neighbors:
  - SD-WAN level config
  - Define BGP neighbors
  - Assign a role
  - Assign a health check

```
config system sdwan
    config neighbor
      edit "172.31.0.1"
         set member 1
         set role primary
         set health-check "HC1"
         set sla-id 1
      next
      edit "172.31.0.2"
         set member 2
         set role secondary
         set health-check "HC2"
         set sla-id 1
      next
    end
```

Must be different HC for each neighbor




Define the SD-WAN neighbor role within the SD-WAN template

Settings *not* configured by the SD-WAN overlay template **Dual HUB (Primary & Secondary)**



Compatible but not automatic settings

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

After you configure BGP to advertise different communities when the SLA status changes, you must define the SD-WAN neighbor role. This is how you associate the BGP neighbors and the route mapping with health checks. For each BGP neighbor of the SD-WAN spoke, you can define a role: primary, secondary, or standalone.

In the SD-WAN configuration section, you define the BGP neighbor role and the health check to determine the device role and mapping to use. If you do not explicitly set a role, FortiGate considers the neighbor as `standalone` (default role), and the BGP neighbor is active regardless of SLA status. However, because the neighbor definition associates a health check and an SLA, FortiGate uses different route maps : `route-map-out-preferable` (comm1 or comm2), if the SLA is met, and `route-map-out` (comm5), if the SLA is missed.

The examples on this slide show how you configure the SD-WAN neighbors with the FortiGate CLI and with the FortiManager SD-WAN template.

It is important to note that when you use the FortiManager SD-WAN overlay template and select **Dual HUB (Primary & Secondary)**, FortiManager prepares templates for two hubs and sets a higher priority for the SD-WAN members that connect to the secondary hub. It does *not* set differentiated roles for the BGP neighbors in the SD-WAN template.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Service Rule

- Differentiated SD-WAN service rules according the neighbor role
  - Active according to hub role: standalone, primary, secondary
  - Enable or disable rule after fallback to standalone mode

```
config system sdwan
    config service
       edit 1
          set name "Critical-DIA"
          set role secondary
          set standalone-action enable
          set src "LAN-net"
          set priority-members 1 2
       next
    end
end
```

Default role = standalone

**SD-WAN > SD-WAN Rules > Advanced Options**

| | |
|---|---|
| role | secondary |
| shortcut | |
| shortcut priority | auto |
| sla compare method | order |
| sla stickiness | |
| src-negate | |
| standalone-action | |

Allow rule after fallback to standalone role
Default = disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

After you set the primary and secondary roles for the SD-WAN neighbors, you must define the SD-WAN rules for each scenario.

For each rule, you can decide if it remains active or not in case of fallback to standalone mode. By default, the primary and secondary rules are inactive when the SLAs for both roles are not met.

In the example shown on this slide, the rule steers traffic when the secondary hub is active. Because standalone-action is enabled, the rule will continue to accept traffic when SLAs are missed for both hubs.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Neighbor Health Monitoring

- Select the metric used to monitor the neighbor
  - Based on the SLA link quality
    - One or multiple members for each neighbor

```
config system sdwan
    config neighbor
      edit "172.31.0.1"
         set member 4 5
         set mode sla
         set health-check "HC1"
         set sla-id 2
         ...
```

Default mode

- Based on the speed test status
  - Could-assisted speed tests
  - Hub-and-spoke speed tests
  - One member for each neighbor

```
config system sdwan
    config neighbor
      edit "172.31.0.1"
         set member 4
         set mode speedtest
         ...
```

Single member

Use the speedtest result for the member to determine the neighbor

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

When you define SD-WAN neighbors, you can monitor the health of the members with a health check or use the result of speed tests, if you defined a speed-test server or use cloud-assisted speed tests.

Note that you can define multiple members for each neighbor with health-check performance monitoring and only one member for each neighbor when you select the `speedtest` mode.



Vouchers & Dumps are Available | WhatsApp +201224560923

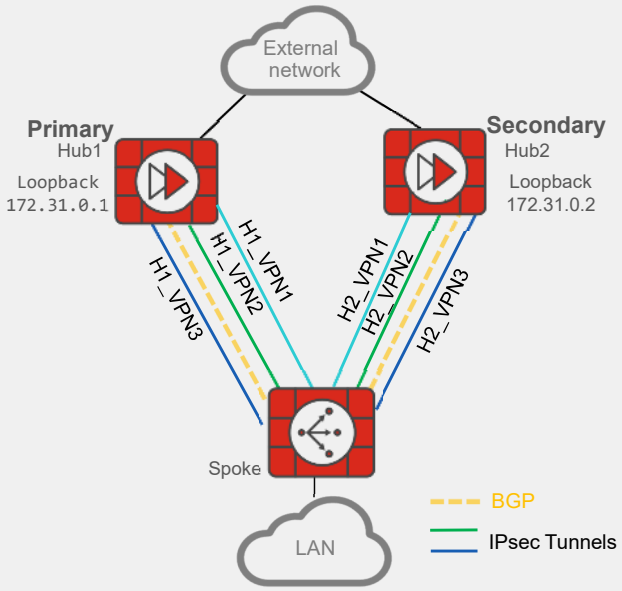
DO NOT REPRINT Brave-dumps.com
© FORTINET

## Multiple Members per SD-WAN Neighbor

- By default, a neighbor is preferable if at least one member is within the SLA
- Refine with `minimum-sla-met-members`
  - Mode `SLA` only
  - Default value:1
    - `route-map-out-preferable` used if at least one member to neighbor meet SLA

```
# config system sdwan
    config neighbor
       edit "172.31.0.1"
           set member 4 5 6
           set minimum-sla-meet-members 2
           set mode sla
           set health-check "HC1"
           set sla-id 1
       next
    end
```

Apply `route-map-out-preferable` if at least two members are within SLA




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

As you learned in this lesson, when the SD-WAN member meets the SLA threshold, FortiGate applies the route map defined in the BGP neighbor `route-map-out-preferable` option. If the SD-WAN member fails to meet the SLA, FortiGate applies the route map defined in the BGP neighbor's `route-map-out` option instead.

What happens when multiple SD-WAN members connect to the same BGP neighbor?

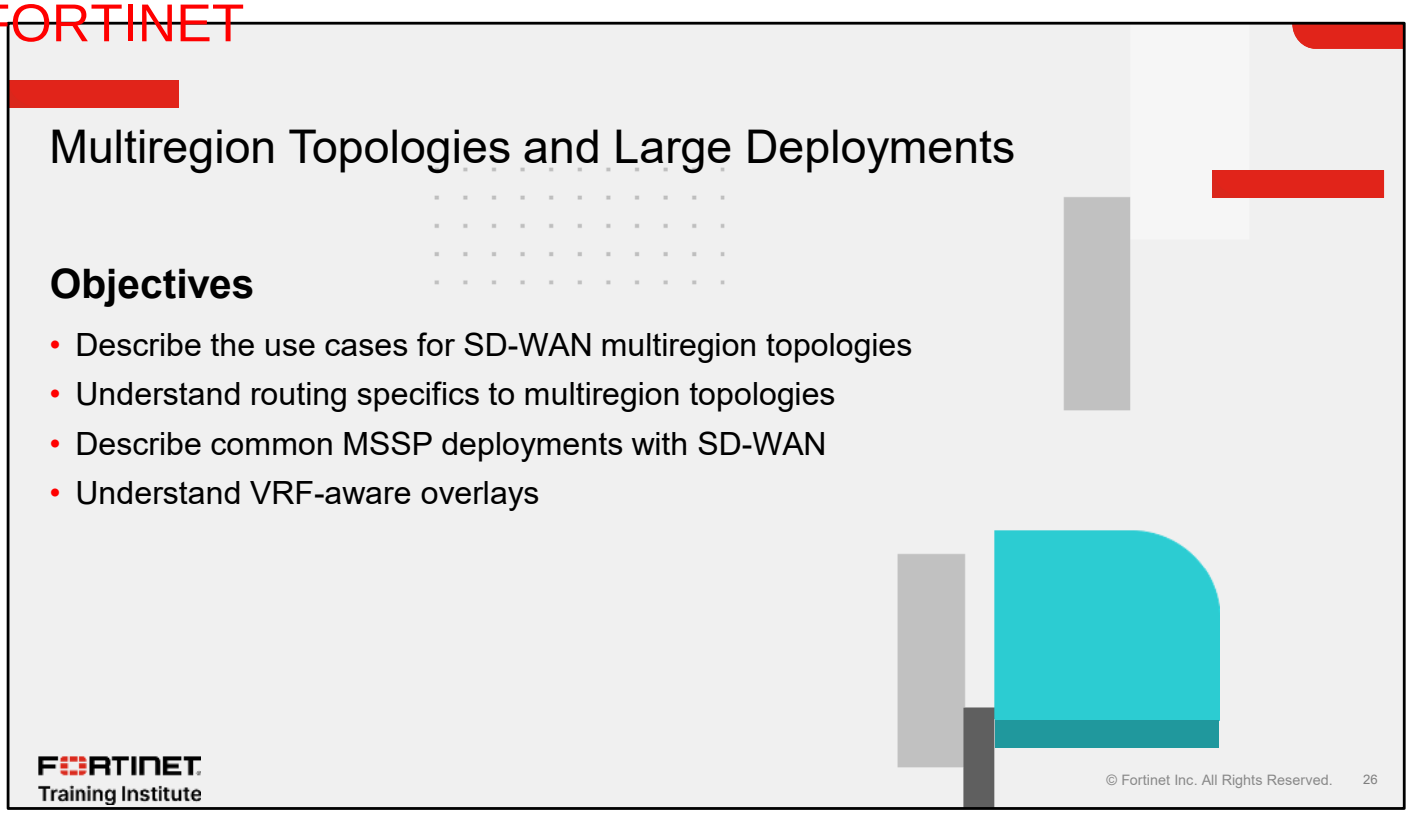
By default, FortiGate applies `route-map-out-preferable` only when at least one member connected to the BGP neighbor meets the SLA criteria. In some situations, the administrator can decide to fall back to the secondary neighbor as soon as one member that connect to the primary fails to meet the SLA or when the number of members within the SLA are not enough to ensure the bandwidth. Using the `minimum-sla-meet-members` parameter, you can refine the behavior and define the number of links that must be within the SLA to use the routing `route-map-out-preferable` for the member.

In the example shown on this slide, the administrator configured the `minimum-sla-meet-members` to `2`. Therefore, the spoke FortiGate uses the routing that corresponds to `route-map-out-preferable` for the primary neighbor as long as two members are within the SLA. Said another way, it uses `route-map-out` when only one tunnel meets the SLA.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding SD-WAN multiregion topologies and the most common use cases, you should be able to select the most appropriate topology and the options required to address you network requirements.

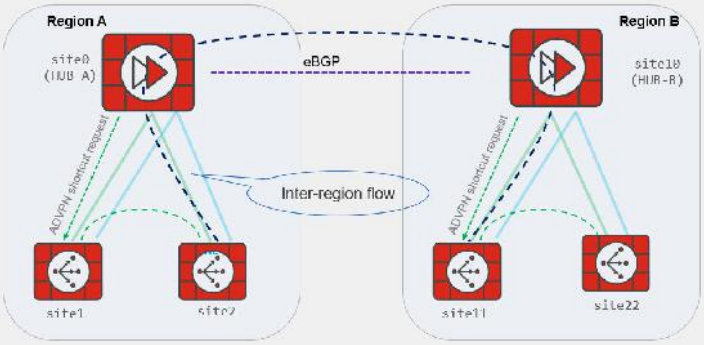


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN Use Cases—Multiregion Topologies

- Increased scalability
- Geographically expanded solution
  - High number of spokes
  - Group devices per region
  - Full-mesh connectivity between hubs
- Typical operation
  - EBGP between regional gateways
  - IBGP within regions
  - ADVPN within regions
  - Traffic across regions through regional hubs




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

As your solution expands geographically and the number of sites grows, you might decide to segment the traffic and management of devices into multiple regions to increase scalability. For each region, you can define either a single-hub or dual-hub SD-WAN topology.

In each region, branch devices connect to the regional SD-WAN gateway. Then, regional gateways are interconnected between regions in a full mesh design. When a user from one region needs to connect to a user or an application in another region, traffic goes through regional gateways.

You should consider a design like this when traffic exchanged within each region is significantly higher than traffic going through regions. Usually, regions correspond to geographical areas but, according to expected traffic flows, you might want to consider a different segmentation. It could be shops and factories, or any other logical grouping applicable to your business.

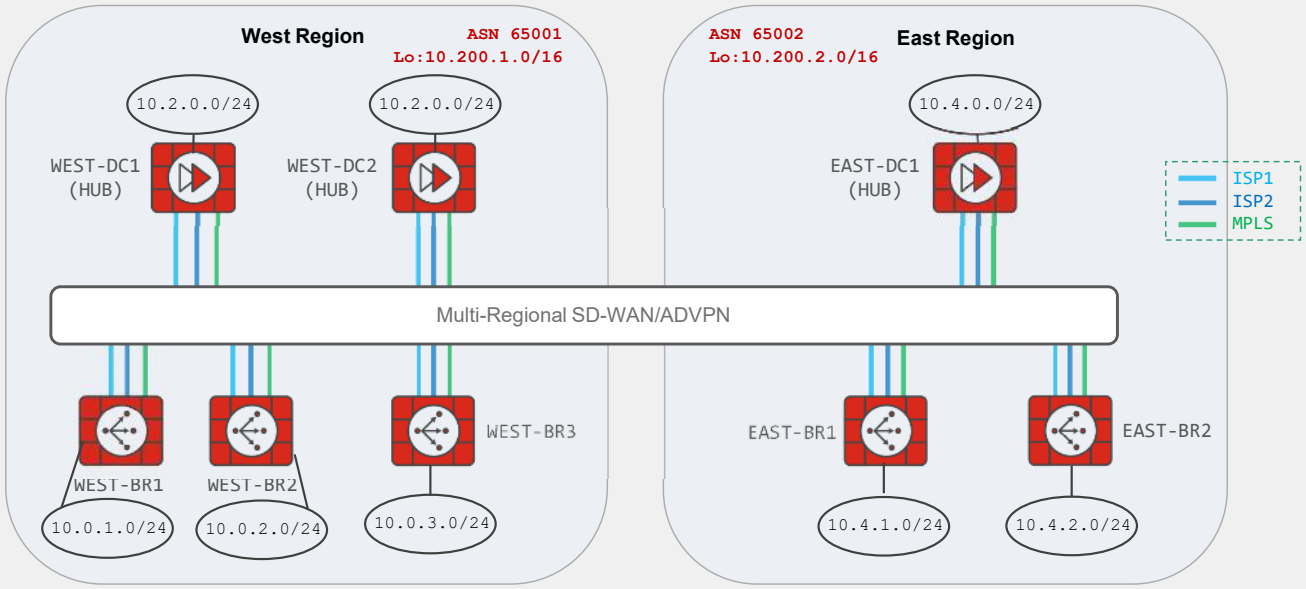
Though less common and more complex to deploy and manage, a multiregion design with IBGP as the routing protocol between the regional gateways is possible. Similarly, typical deployments allow ADVPN within each region, but FortiGate supports interregion ADVPN. To allow ADVPN between spokes in different regions, you either use IBGP as the only routing protocol, or deploy a topology with ADVPN 2.0. You will learn about ADVPN and ADVPN 2.0 configurations in another lesson.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Multiregion SD-WAN Topology—Example




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

This slide shows an example of a multiregion topology.

A region is a hub-and-spoke block. Each region has its own SD-WAN topology, which can be single or dual hub, and each hub can be standalone or high availability (HA). ADVPN shortcuts can be established between devices in each region. For redundancy reasons, Fortinet recommends topology with dual-hub regions.

In this example, external BGP (EBGP) is used between regions.

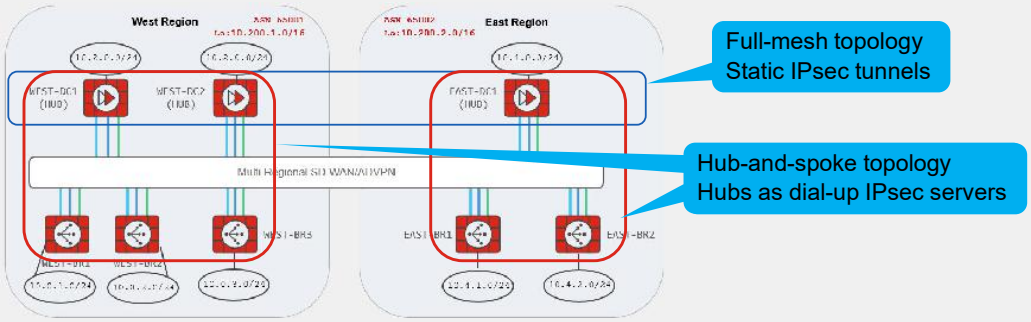
It is common for the entire SD-WAN network to consist of a single region, but large-scale deployments, with thousands of sites, you should consider a multiregion design.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# IPsec Overlays for Multiregion Topologies

- At the region level
  - Hubs act as dial-up endpoints for the spokes
  - Every spoke builds a static IPsec tunnel, over each available underlay, towards each hub
- Between the regions
  - The hubs build a full-mesh topology over each available underlay
  - Static IPsec tunnels
  - Optional: Allow interregion ADVPN shortcuts by enabling, on each hub, the forwarding of discovery requests




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

When you work with multiregion topologies, the IPsec configuration at the region level remains similar to what it would be for a single region. The hubs act as dial-up IPsec endpoints for the spokes in the region they serve. You define a separate dial-up IPsec endpoint on each available underlay. On every spoke, you define a static IPsec tunnel, over each available underlay, toward each hub.

In order to interconnect multiple regions, you configure the hubs to build a full-mesh topology between them over each available underlay. All hub-to-hub tunnels are static IPsec tunnels. Every hub builds a tunnel over each available underlay transport towards every other hub.

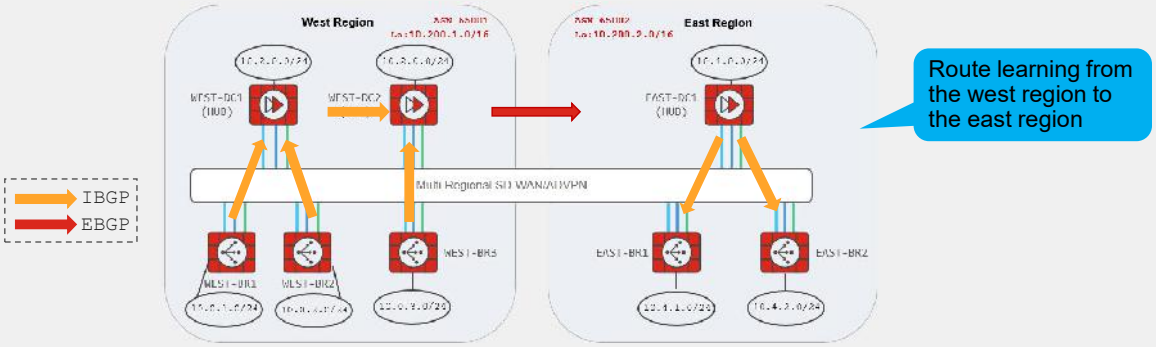
Optionally, you can enable ADVPN at the region level only to allow intraregion shortcuts. If you want to allow interregion ADVPN shortcuts, you must enable the forwarder mode on each hub.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## BGP Routing for Multiregions Topologies

- Within regions
  - IBGP
  - BGP per overlay
  - BGP on loopback
  - For ADVPN within the region
    - Each spoke learns all available paths to other spokes in the region
- Between regions
  - EBGP
  - Route summarization possible
  - Interregion ADVPN
    - Possible but not commonly used
    - Not compatible with route summarization




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

Once the overlay network is built, the devices must exchange routing information between all the SD-WAN nodes—hubs and spokes—to ensure site-to-site reachability. The recommended routing protocol for a topology like this is BGP. BGP is an industry-standard dynamic routing protocol that is famous for its flexibility and rich feature set.

The diagram shown on this slide illustrates, at a very high level, how the routing information flows from the spoke devices in the west region, through the hubs on the west and east regions, and then to the spoke on the east region.

When you plan the routing for multiregions SD-WAN topology, you should consider the following guidelines:
- Assign a single BGP autonomous system (AS) to each region.
- Every spoke advertises its LAN prefixes to the hubs using IBGP.
- Every hub acts as a BGP route reflector, readvertising the prefixes to all other spokes within the region.
- Configure EBGP peering between the hubs to exchange routing information between the regions.
- The hub in each region readvertises the routes learned to the spokes within the region.
- Additionally, the hubs advertise their own LAN prefixes, as well as any destinations learned from outside of the SD-WAN network.

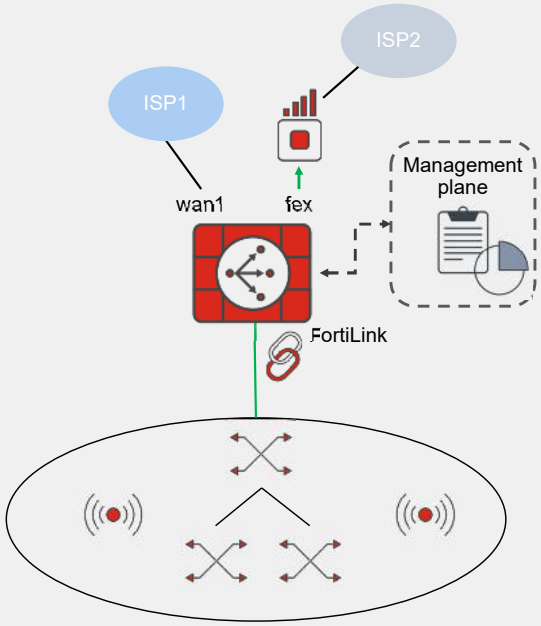
The administrator can define the level of route summarization and route redistribution according to the network requirements. However, when defining route summarization, remember that SD-WAN needs to know all available paths to a destination to select the best path to steer the traffic according the SD-WAN rules. Usually, you will not perform any summarization within each region and summarize routes exchanged between the regions, except if you want to allow interregion ADVPN, which you will learn about in another lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## What Is SD-Branch?

- An SD-Branch is an SD-WAN spoke site enriched with one or multiple extensions:
  - On the LAN side:
    - FortiSwitch
    - FortiAP
  - On the WAN side
    - FortiExtender
- The SD-WAN spoke is the local controller
  - The network sees the extensions as logical interfaces on the FortiGate
- FortiAP and FortiSwitch interfaces benefit from the capabilities of the SD-Branch
  - Security features
  - Traffic steering




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

Speaking of SD-WAN deployments, you can hear network architects talking about SD-branch, but what is SD-branch?

An SD-branch is a site with an SD-WAN spoke FortiGate device and one or multiple extensions. On the LAN side, FortiSwitch and FortiAP provide wired and wireless connectivity, respectively. They connect to their managing FortiGate using the proprietary FortiLink protocol. In this way, a wide variety of security features are extended into the LAN, such as microsegmentation, 802.1X authentication policies, and built-in NAC functionality. On the WAN side, FortiExtender supplements FortiGate WAN connectivity by adding 3G/4G/5G connectivity options. This is often used to provide a backup WAN connection.

The spoke SD-WAN FortiGate device is the local controller of all the SD-branch components deployed on that site. All these components run in *managed mode*, with their configuration fully controlled by FortiGate. The network and the management plane, FortiManager, FortiAnalyzer, or any other management tool, see the ports of the extension devices as logical interfaces of FortiGate. Consequently, the entire management plane communicates, as with a classical spoke, solely with the FortiGate devices.

This is how an SD-WAN site can easily become *an SD-branch site*, interconnected with other sites by the same overlay network and managed by the same management plane as the other SD-WAN spoke sites.

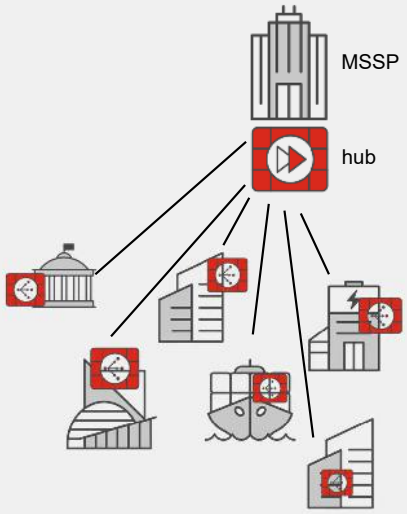


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## MSSP Deployment Blueprints

- Common questions from managed security service provider (MSSP):
  - How to efficiently provide SD-WAN as a managed service?
  - What should be deployed as the customer premises equipment (CPE)?
  - What should be deployed on the MSSP premises?
- Some answers:
  - For the edge CPEs: spoke FortiGate devices
    - Various form factors to best match the site requirements
      - How many users will the site serve?
      - How many WAN links are required and of what type?
      - What kind of security inspection is required for the traffic entering and leaving this site?
  - The hub FortiGate can be either:
    - Located in MSSP premises, with multi-tenancy
    - Located in MSSP premises, dedicated for one customer
    - Installed in customer premises




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

Customers who delegate the installation and the management of their SD-WAN network to a managed security service provider (MSSP) can select between various level of delegation. Some common questions from MSSP are:

- How do you efficiently provide SD-WAN as a managed service?
- What should you deploy as the CPE?
- What should you deploy on the MSSP premises?

To answer those questions, you should first consider the customer and site requirements. You will select the edge device form factor—entry level, mid-range, or high-range FortiGate—according to the site requirements. To do that, you will consider various factors. The main are the number of users the site serves, the number and the type of WAN links required, and the level of security inspection required for the traffic entering and leaving the site. Usually, the edge device is the spoke FortiGate device, and it is installed by the MSSP on the customer premises.

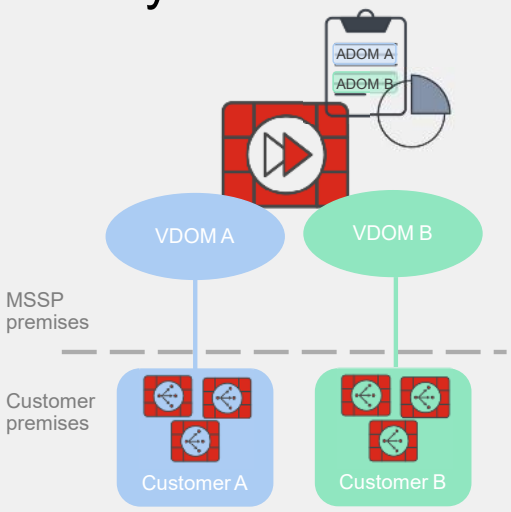
For the hub, MSSP can select between hubs located in their premises that serve one or multiple customers and hubs installed on the customer premises. You will review each option in this lesson.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Hub On MSSP Premises—Multi-tenancy

- Hub on MSSP premises
- Hub configured with VDOMs
- One VDOM for each customer
  - One SD-WAN instance per VDOM
- All customer sites are spokes
- Most customer traffic is either:
  - Spoke-to-spoke
    - Flowing through an ADVPN shortcut
  - Direct internet access (DIA)
    - From the spoke to the internet
- Reduced to no workload hosted behind the hubs on the MSSP premises
  - Traffic flow through the hub is minimal




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

One common type of deployment for MSSP is multi-tenancy hubs. The MSSP installs and manages the hubs on its own premises, and each hub serves multiple customers. In a topology like this, to enforce the independence between each customer SD-WAN network, the administrator can configure the hub with one VDOM for each customer. The MSSP installs the spoke devices on the customer premises and manages them. The MSSP administrator might provide the customer with a monitoring view or limited management access on the spoke devices.

In this blueprint, the hubs perform mainly control plane functions in the SD-WAN network. They facilitate route exchange and ADVPN operation. All types of customer sites are spokes, regardless of their size. As a result, nearly all the customer traffic is either spoke-to-spoke, flowing through ADVPN shortcuts, or direct internet access (DIA) on the spokes.

There are often no workloads hosted behind the hubs on MSSP premises, which reduces traffic flow through the hubs to the minimum. However, the hubs must forward traffic in the following cases:

- Building an ADVPN shortcut is not an option. For example, when the two spokes are not connected to any common underlay transport, such as internet and MPLS.
- The MSSP offers services, such as remote internet access (RIA) or cloud on-ramp. The role of the hubs is then to connect the customer sites to the world outside of the SD-WAN network.
- To provide connectivity to legacy customer sites that have not yet migrated to the SD-WAN network.
- If the MSSP offers services hosted on its premises. From the spoke perspective, these services are reachable only through the hub.

The hubs deployed on the MSSP premises are often called SD-WAN gateways, since they interconnect the customer SD-WAN sites and connect them to the world outside of the SD-WAN network. On the management side, MSSPs usually use ADOMs on FortiManager to ensure that each customer setup remains isolated.

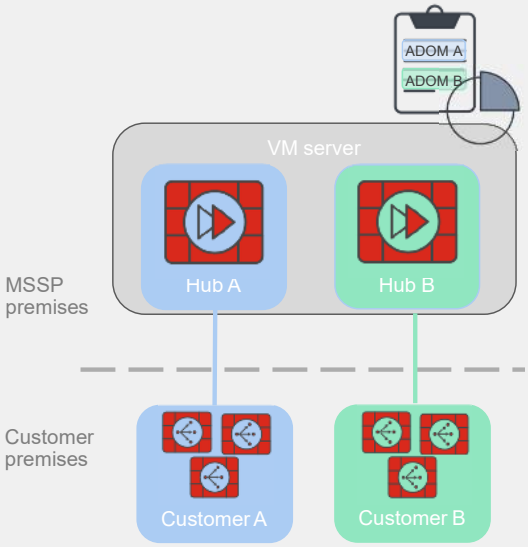


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Hub On MSSP Premises—No Multi-Tenancy

- Hub on MSSP premises
- One hub for each customer
  - Common for MSSP with cloud infrastructure
  - Usually, the hub is a FortiGate VM
- All customer sites are spokes
- Most traffic remains within the customer devices or is DIA
  - Similar to a multi-tenancy scenario




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

With the growing adoption of virtualized cloud environments, another blueprint became popular. It is similar to the blueprint described previously, but instead of managing multi-tenant hubs, the MSSP deploys and manages dedicated hubs for each customer. Indeed, when an MSSP has a telco cloud infrastructure on its premises, it becomes reasonable to delegate the multi-tenancy duties to this infrastructure. Consequently, the hubs in this blueprint are virtual, built with one FortiGate VM for each customer hub.

The spokes are still located on the customer premises and, usually, most of the traffic flows through the customer devices. The situation that requires traffic through the hub, described previously, still applies.

Finally, either FortiManager or FortiAnalyzer, or both, can be deployed with or without multi-tenancy. With dedicated products, the MSSP can provide the customers with direct access to their management products, depending on the nature of the managed service subscribed. With multi-tenancy, the MSSP defines an ADOM on FortiManager to that customer data and the setup remains isolated.



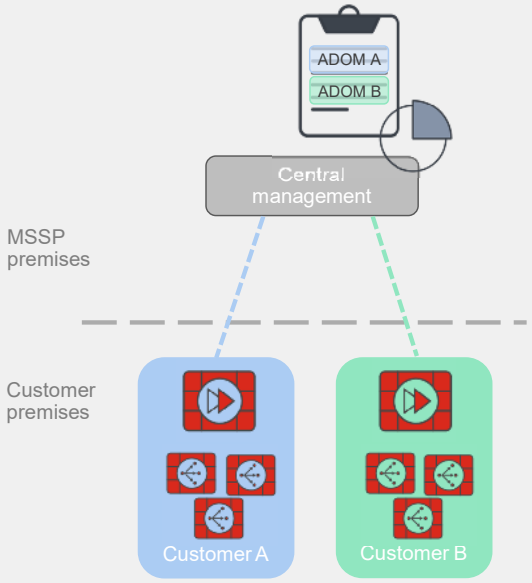
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Hub On Customer Premises

- Central management on MSSP premises
- Hub and spokes on the customer premises
- Hub in customer's central office or data center

- Traffic flow:
  - Spoke-to-hub
    - Branch sites accessing workload in the datacenter
    - RIA with centralized breakout
  - DIA on the spokes
  - Limited spoke-to-spoke traffic




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

Another popular MSSP choice is to deploy the hubs on the customer premises, such as at a central office or a data center. The traffic flow in this blueprint is quite different from the two previous scenarios described. The majority of the traffic is likely to be either spoke-to-hub—branch sites accessing workloads hosted in the data center or an RIA through a centralized breakout owned by the customer—or DIA on the spokes. In this type of topology, occasional spoke-to-spoke traffic is possible, but rare, and usually non-existent.

The MSSP is not part of the overlay network in this case. Both the control plane and the data plane are located on the customer premises. However, the MSSP can still provide the management plane as a service.

Taking the management maintenance burden away from the customer is an important benefit of the managed service. No wonder the management layer of SD-WAN solutions offered by an MSSP, including at least FortiManager and FortiAnalyzer, is almost never deployed at the customer site.

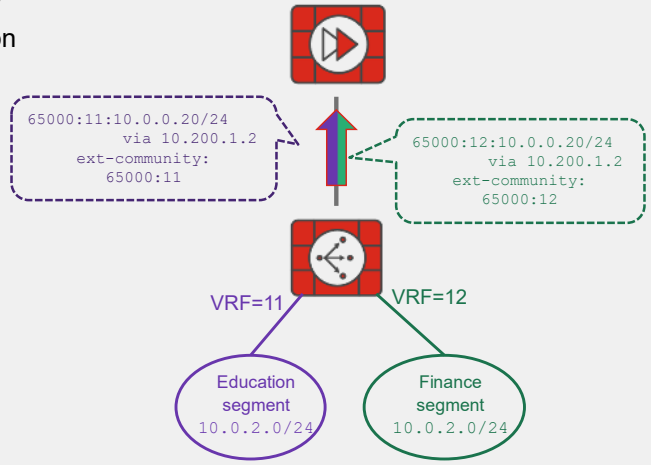


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Segmentation Over Single Overlay

- Use cases
  - Strict traffic separation between entities of a company
  - Education and finance, corporate and guest, and so on
- Segregation on a network means:
  - Separated traffic flow
  - Separated route propagation
  - Control plane segregation
    - IP addressing overlap allowed between segments
- Segregation with SD-WAN
  - Preserve the segregation on the overlay
  - Differentiated rules
- Technology in the background
  - Virtual routing and forwarding (VRF)
  - VRF creates virtual routers within on device
  - Allow multiple routing table instances on a device




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

On some customer network the need arise for strict traffic segregation. For example, the customer may want to segregate data traffic of different sensitivity, such as education and finance, guest and corporate, and so on. When customer sites have multiple segments segregated from each other, each segment can be connected to separate network equipment, such as separate switches and routers. This is called physical segmentation. Segments may also share the same equipment that supports internal segmentation, such as VRF.

On segmented networks, the devices must not only segregate the traffic flows, but also permit route propagation only *within* a segment . In other words, segmentation also means control plane segregation. It also means, for example, that IP addressing overlap is possible between different segments.

For this reason, segmentation cannot be implemented only using firewall policies. While they can provide granular segregation of traffic flows, they do not restrict route propagation and do not allow IP address overlap.

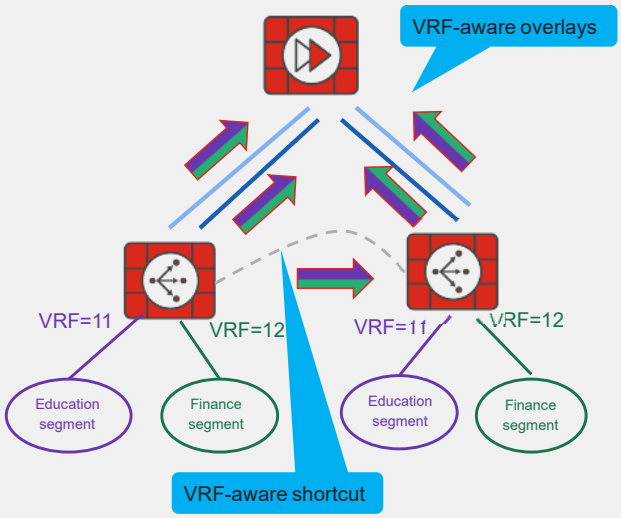


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## VRF-Aware Overlay

- FortiGate supports multiple VRFs
- On the control plane:
  - Use MP-BGP-BPNv4 to advertise VRF information with each LAN prefix
- On the data plane:
  - Traffic is tagged using vpn-id-ipip encapsulation when forwarded between SD-WAN nodes
    - Encapsulation allowed on all IPsec overlays, including ADVPN shortcuts
- FortiGate sends traffic from multiple VRFs over the same IPsec tunnel
  - ➡ VRF-aware overlays




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

A multi-VRF deployment is often referred to as a “segmentation over single overlay", because the same overlay network forwards traffic belonging to multiple segments (VRFs), while preserving their segregation across all the SD-WAN sites.

A multi-VRF deployment allows you to implement end-to-end segmentation across the entire SD-WAN network. Both routing designs described, BGP per overlay and BGP on loopback, support this functionality. FortiGate devices support multiple VRFs. Therefore, on each SD-WAN node, different customer segments are attached to different VRFs. Different VRFs effectively mean different routing tables.

On the control plane, FortiGate use MP-BGP VPNv4 to advertise VRF information, together with each LAN prefix, over the entire SD-WAN overlay network.

On the data plane, FortiGate tags the traffic using the vpn-id-ipip encapsulation, when it forwards the flows between SD-WAN nodes. FortiGate encapsulates the traffic on all the IPsec overlay tunnels, including ADVPN shortcuts. The vpn-id-ipip encapsulation is a variation of IPIP. An extra IP header is added inside the ESP payload (encrypted), encoding the VRF ID into the IP address field.

In other words, you send the traffic from multiple segments (VRFs) over the same IPsec tunnel, while tagging it with its VRF information, so that the receiving SD-WAN node can preserve the segregation.
This feature is known as VRF-aware overlays.

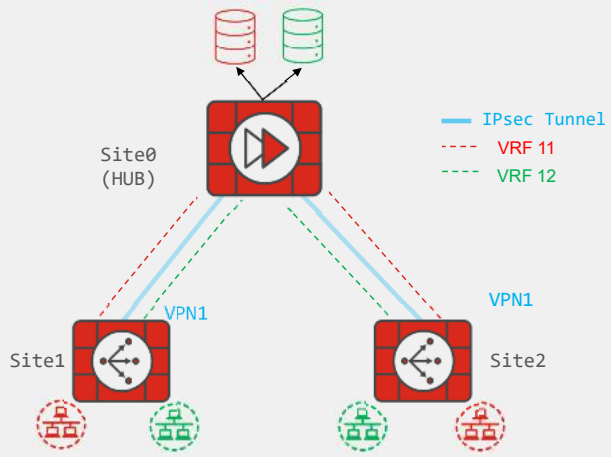


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Advanced SLA Settings—VRF-Aware Health Check

- SD-WAN on multi-VRF networks
  - Multi-VRF tunnels
  - Health check tagged with VRF ID
  - Specified source IP




- CLI configuration

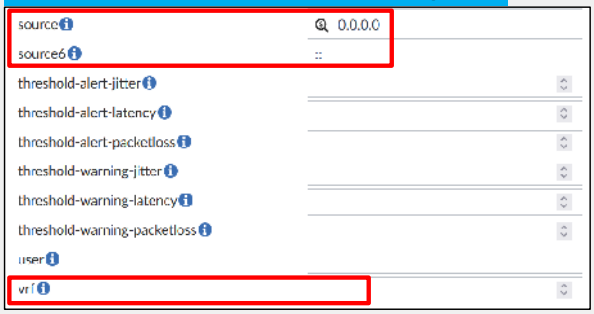
```
config system sdwan
    config health-check
        edit "Corp_HC"
            set vrf 11
            set source <address>
        next
    end
```

VRF id

Source IP address used in health check packets to the server

- GUI

**SD-WAN > Performance SLA > Advanced Options**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

For SD-WAN on a multi-VRF network, you can decide to perform health checks per VRF. The originating spoke can tag the health-check probes with the correct VRF, when transmitting to a multi-VRF tunnel. The hub will then forward the probes to the correct health-check server in the specified VRF.

You can use the advanced performance SLA options to define the VRF ID and the source IP address used to forward health-check packets to the server, as shown on this slide



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe the use cases for SD-WAN dual-hub topologies
- ✓ Discover the BGP advanced option for SD-WAN
- ✓ Understand the routing options for dual-hub topologies
- ✓ Understand SD-WAN self-healing
- ✓ Describe the use cases for SD-WAN multiregion topologies
- ✓ Describe common MSSP deployments with SD-WAN
- ✓ Understand VRF-aware overlays

FORTINET Training Institute

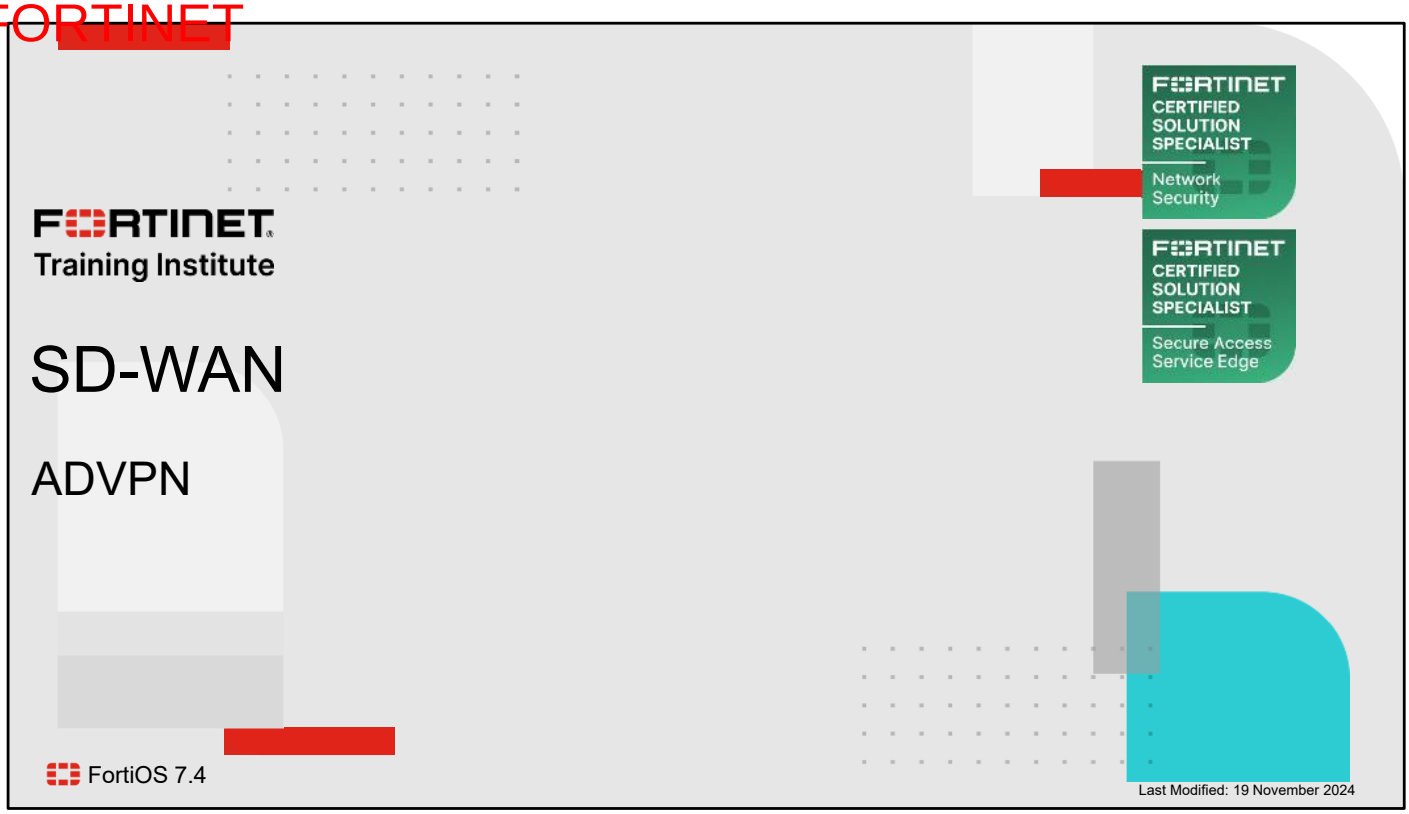
© Fortinet Inc. All Rights Reserved. 39

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about SD-WAN with dual-hub and multiregion topologies. You discovered common use cases of those topologies and learned the specific configuration requirements for each of them.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

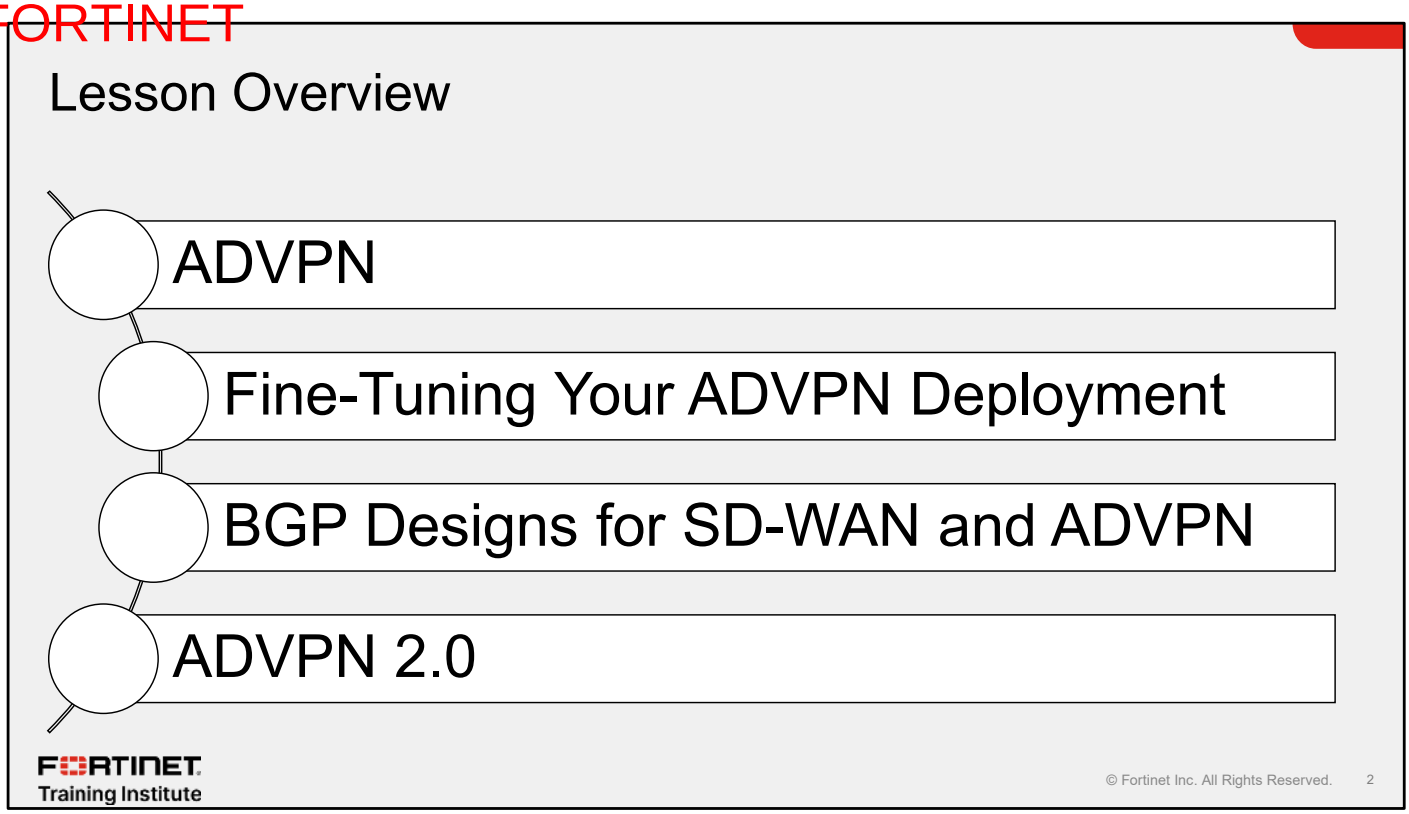



In this lesson, you will learn about auto discovery VPN (ADVPN), a proprietary framework developed by Fortinet to allow the setup of shortcut tunnels between spokes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

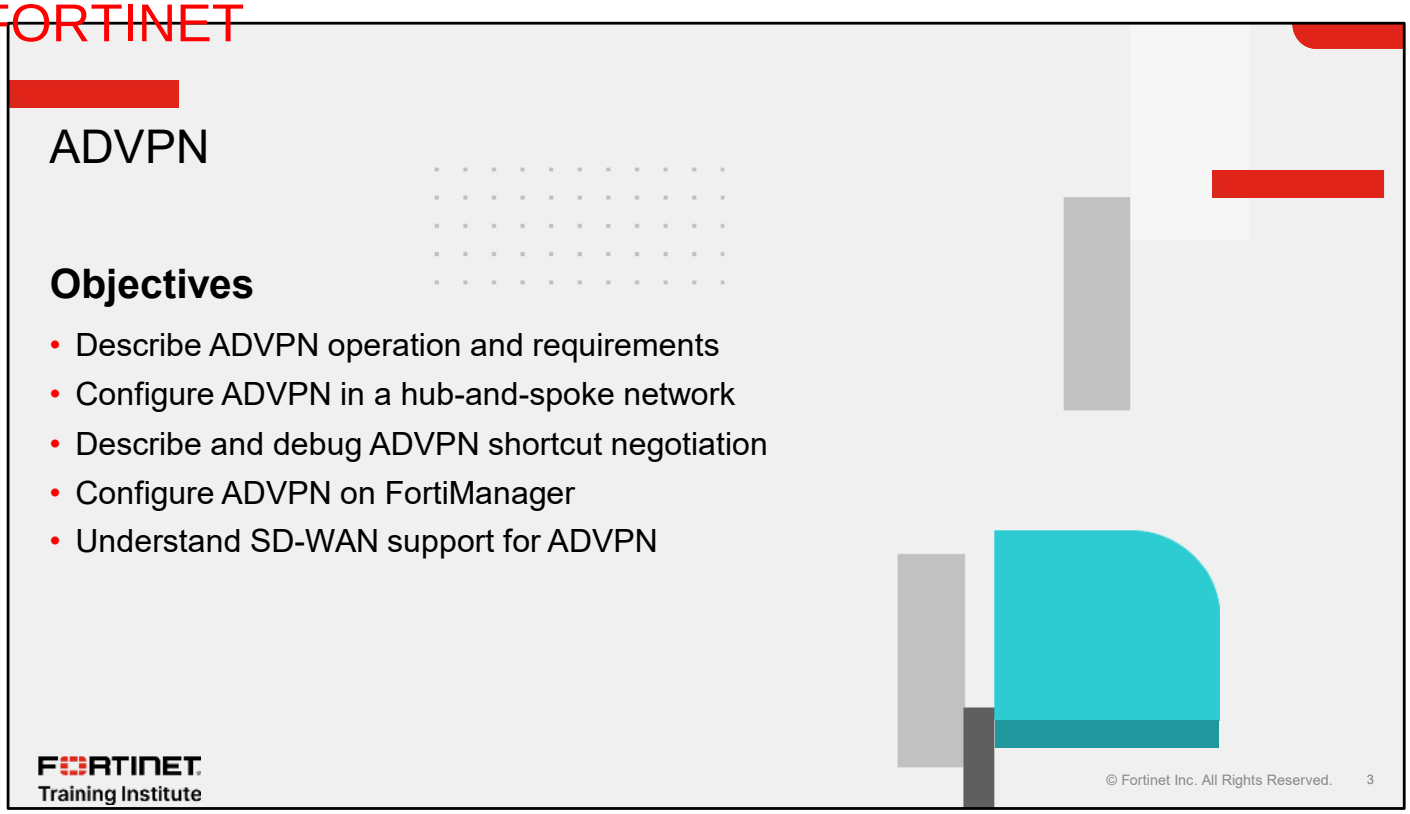



In this lesson, you will learn about the topics shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in ADVPN, you will be able to configure and troubleshoot ADVPN on a basic topology. You will also understand SD-WAN support for ADVPN.

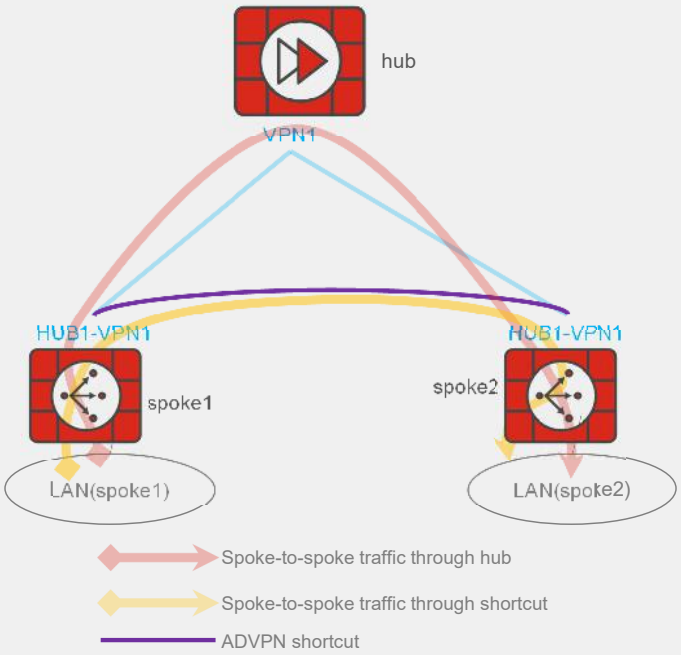


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## ADVPN Overview

- Enables direct spoke-to-spoke communication
  - Fortinet proprietary
  - Based on IKE and IPsec
  - Benefits of a full-mesh topology in a hub-and-spoke network
- Hub facilitates spokes shortcut negotiation
  - On-demand IPsec tunnels
  - Shortcuts carry spoke-to-spoke traffic
- Supported by SD-WAN
  - Automatically steers traffic through shortcuts
  - Shortcuts are monitored




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

You discovered the ADVPN terminology, its main concept and use case in the introduction lesson. Now you will learn how to configure ADVPN and implement it on top of an SD-WAN topology.

The simple hub-and-spoke topology shown on this slide is the basis for this lesson. If a device behind spoke1 wants to communicate with a device behind spoke2, the device must do so through the hub. While a hub-and-spoke topology reduces cost and configuration overhead, the fact that a spoke must communicate with other spokes through the hub increases the delay of the communication, and therefore impacts the user experience, especially if the hub and spokes are in geographically distant locations. Full-mesh topology, enables direct spoke-to-spoke communication at the expense of higher costs and increased administrative overhead. However, this is not always practical, or even feasible, especially in large networks.

ADVPN—auto discovery VPN— is a Fortinet-proprietary solution based on IKE and IPsec, that addresses the need for direct spoke-to-spoke communication in hub-and-spoke topologies by enabling the spokes to automatically negotiate on-demand IPsec tunnels—called shortcuts—between them without you having to make topology changes or many configuration changes. After a shortcut is established and routing has converged, spoke-to-spoke traffic no longer needs to flow through the hub.

SD-WAN supports ADVPN shortcuts. For this, SD-WAN automatically steers the traffic through shortcuts and monitors their health and performance. You add the parent tunnel as member, and after the shortcut is negotiated, SD-WAN automatically starts steering the traffic through the shortcut.

The topology on this slide also shows a shortcut established between spoke1 and spoke2. The result is that FortiGate routes the spoke-to-spoke traffic through the shortcuts instead of through the hub.

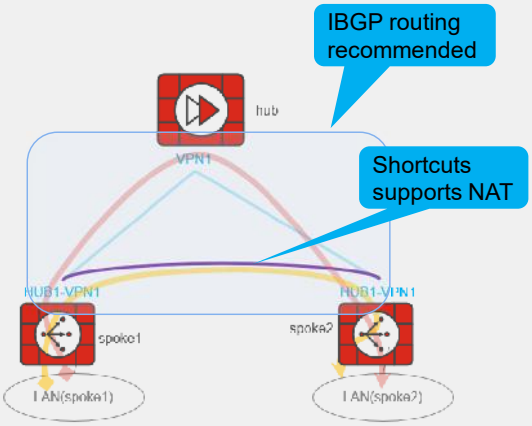


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## ADVPN Overview (Contd)

- Supports multiple hub-and-spoke architectures
- Supports NAT for on-demand tunnels
- Requires the use of a routing protocol
  - IBGP recommended for ADVPN
  - OSPF and RIPv2/RIPng are supported
  - PIM/multicast is supported
- Supports both IPv4 and IPv6




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

- ADVPN supports single or multiple hub architectures.
- NAT is supported for the on-demand tunnels.
- ADVPN requires the use of a routing protocol.
  - Currently, it supports BGP, OSPF, RIPv2/RIPng, and static routing.
  - It also supports PIM and multicast.
- Both IPv4 and IPv6 are supported.

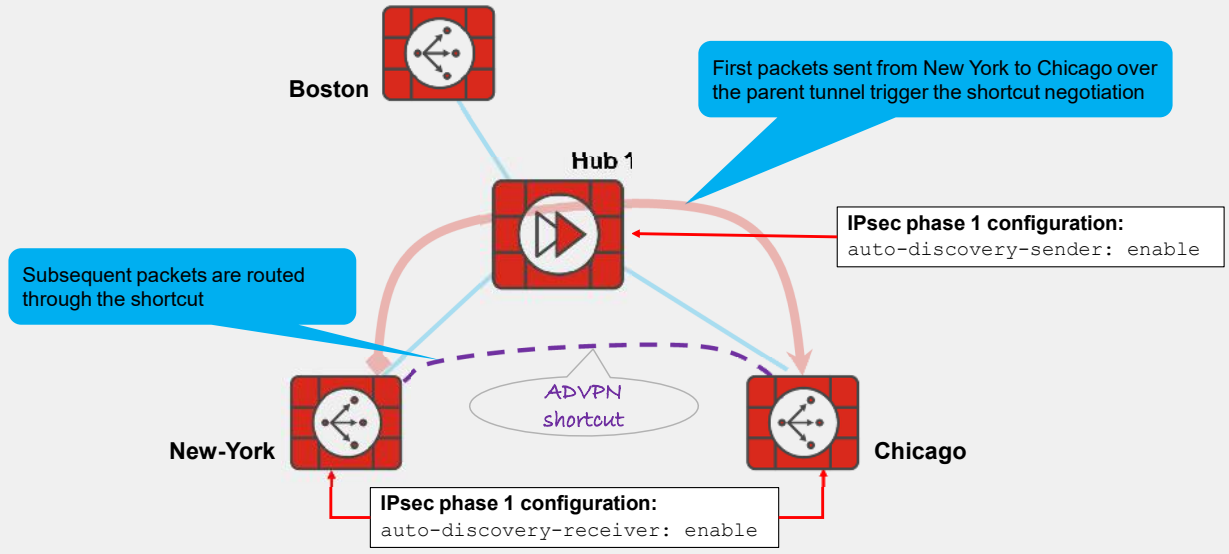
When using ADVPN, Fortinet usually recommends that you use IBGP as the routing protocol for the underlaying topologies.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## ADVPN Configuration and Example (Single Hub)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

This slide shows an example of how ADVPN works in a single hub topology. Consider the basic IPsec hub-and-spoke topology shown on this slide. Overlays that connect a spoke to a hub are called parent tunnels. Direct tunnels negotiated over parent tunnels are called shortcuts. The shortcuts between spokes are created on demand based on the IPsec phase 1 auto-discovery settings configured on each peer:

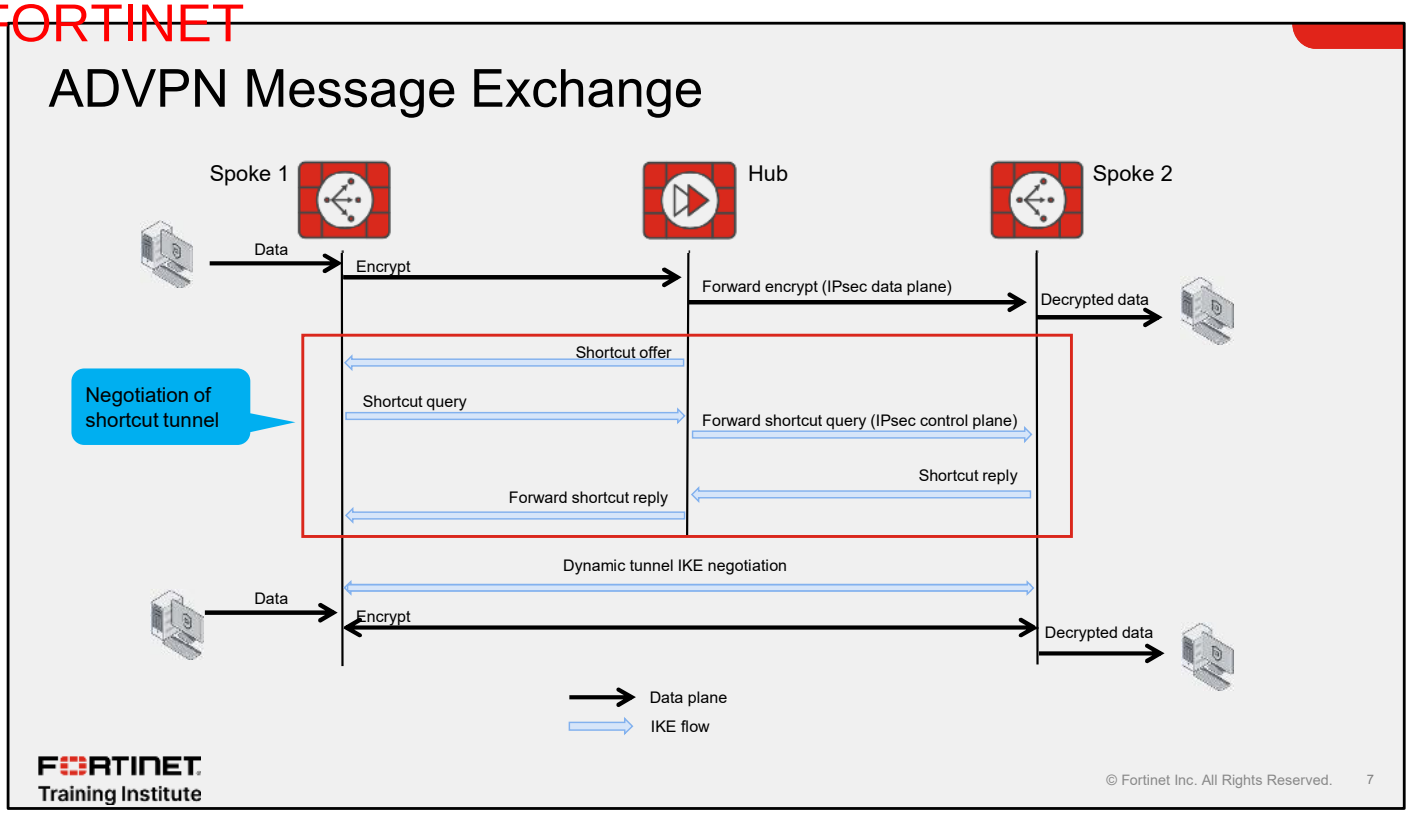
- `auto-discovery-receiver` should be enabled on the spoke overlay to inform the hubs that the spoke can negotiate shortcuts.
- `auto-discovery-sender` should be enabled on the hub overlay that connects the spoke to allow for shortcut negotiation between spokes.

Now, say that a user in New-York sends traffic to Chicago. Initially, the shortcut between New-York and Chicago has not been negotiated. So, the first packets are routed through Hub 1. When Hub 1 receives those packets, it knows that ADVPN is enabled on both spokes. So, Hub 1 sends an IKE message to New-York informing that it can try to negotiate a direct connection to Chicago. On receipt of this IKE message, New-York creates a FortiOS-specific IKE information message that contains its public IP address, its local subnet, the desired destination subnet (Chicago subnet), and an auto-generated PSK (alternatively, it can also use digital certificate authentication). This IKE message is sent to Chicago through Hub 1. When Chicago receives the IKE message from New-York, it stores the PSK and replies with another IKE information message that contains the public IP address of Chicago spoke . After the reply arrives to New-York, the shortcut is negotiated between both peers. The negotiation succeeds because Chicago is expecting a connection attempt from the public IP address of New-York spoke. You will explore this in greater detail in this lesson.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

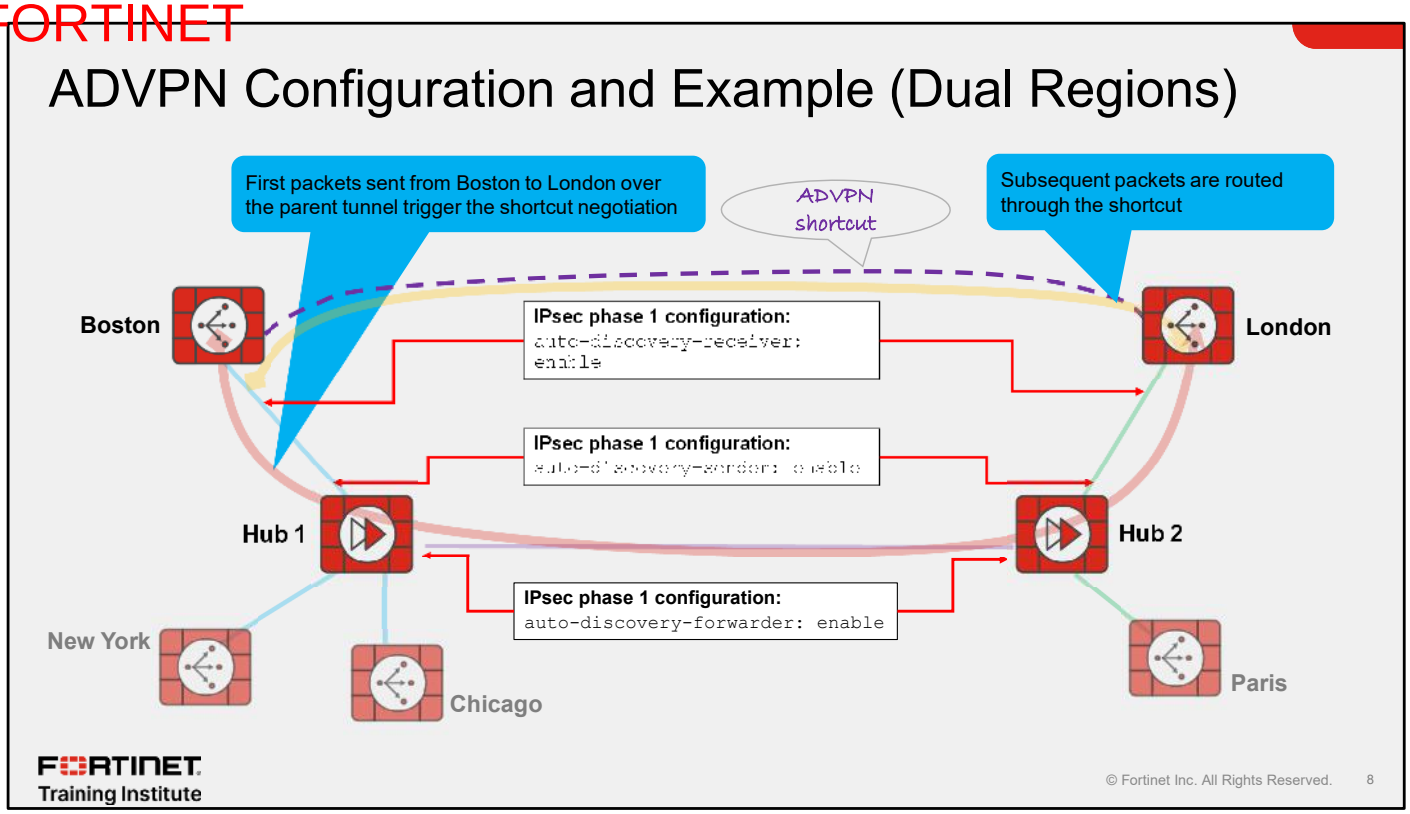



Now, you will examine the IKE messages that are exchanged when an on-demand tunnel is being negotiated:

1. The client behind Spoke 1 generates traffic for devices located on the Spoke 2 network.
2. Spoke 1 receives the packet, encrypts it, and sends it to the hub.
3. The hub receives the packet from Spoke 1 and forwards it to Spoke 2.
4. Spoke 2 receives the packet, decrypts it, and forwards it to the destination device.
5. The hub knows that a more direct tunnel option might be available from Spoke 1 to Spoke 2. The hub sends a shortcut offer message to Spoke 1.
6. Spoke 1 acknowledges the shortcut offer by sending a shortcut query to the hub.
7. The hub forwards the shortcut query message to Spoke 2.
8. Spoke 2 acknowledges the shortcut query and sends a shortcut reply to the hub.
9. The hub forwards the shortcut reply to Spoke 1.
10. Spoke 1 and Spoke 2 initiate the tunnel IKE negotiation.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




Now, consider the dual-region IPsec hub-and-spoke topology shown on this slide. It's a topology with two hubs and each spokes connect to a single hub. Consider IBGP routing between all devices shown on the diagram. In such a scenario, you must enable `auto-discovery-forwarder` on both hubs to allow ADVPN information exchange between the two hubs and permit ADVPN shortcut establishment.

- `auto-discovery-receiver` should be enabled on the spoke overlay to inform the hubs that the spoke can negotiate shortcuts.
- `auto-discovery-sender` should be enabled on the hub overlay that connects the spoke to allow for shortcut negotiation between spokes.
- `auto-discovery-forwarder` should be enabled on the hub overlay that connects to the other hub to forward ADVPN sender and receiver information between hubs.

Now, say that a user in Boston sends traffic to London. Initially, the shortcut between Boston and London has not been negotiated. So, the first packets from Boston to London are routed through Hub 1 and Hub 2. When Hub 1 receives those packets, it knows that ADVPN is enabled in all the VPNs all the way to London. So, Hub 1 sends an IKE message to Boston informing that it can try to negotiate a direct connection to London. On receipt of this IKE message, Boston creates a FortiOS-specific IKE information message that contains its public IP address, its local subnet, the desired destination subnet (London's subnet), and an auto-generated PSK (alternatively, it can also use digital certificate authentication). This IKE message is sent to London through Hub 1 and Hub 2. When London receives the IKE message from Boston, it stores the PSK and replies with another IKE information message that contains London's public IP address. After the reply arrives in Boston, the shortcut is negotiated between both peers. The negotiation succeeds because London is expecting a connection attempt from Boston's public IP address. You will explore this in greater detail in this lesson.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# SD-WAN Overlay Design—ADVPN Configuration

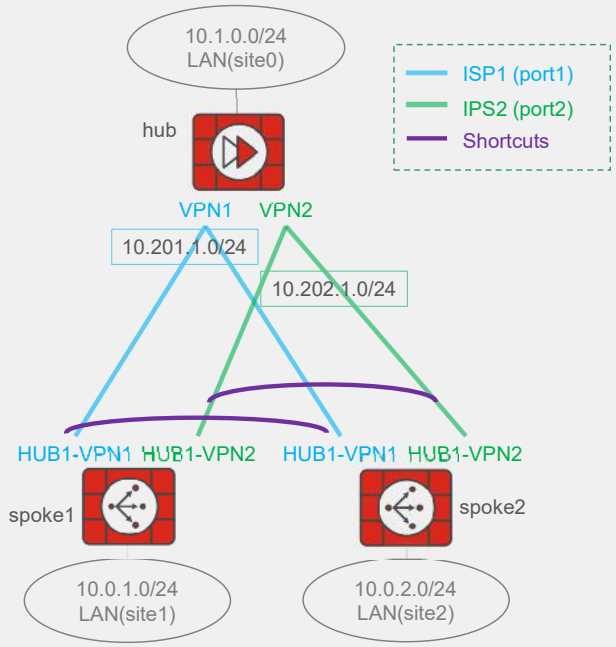
- Hub:
  - IPsec phase 1:

```
config vpn ipsec phase1-interface
    edit "VPN1"
        set net-device disable
        set auto-discovery-sender enable
    next
end
```

- Spoke:
  - IPsec phase 1 and interface:

```
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        set net-device enable
        set auto-discovery-receiver enable
    next
end
config system interface
    edit "HUB1-VPN1"
        set allowaccess ping
    next
end
```

Required for shortcut monitoring




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

The topology on this slide shows the ADVPN configuration required on our basic SD-WAN deployment.

On the hub, you must disable `net-device` and enable `auto-discover-sender` on the phase 1 configuration of each overlay.

On spokes, you must enable both `net-device` and `auto-discovery-receiver` on the phase 1 configuration of each overlay. You must also allow the interface to respond to ping packets. The reason is that SD-WAN sends ping probes to the overlay IP address of the remote spoke to monitor the shortcut performance and health. For this reason, if you don't enable ping access, then ping probes fail, and shortcuts are marked as dead.

Note that `net-device` is disabled by default, so make sure to enable it on spokes.

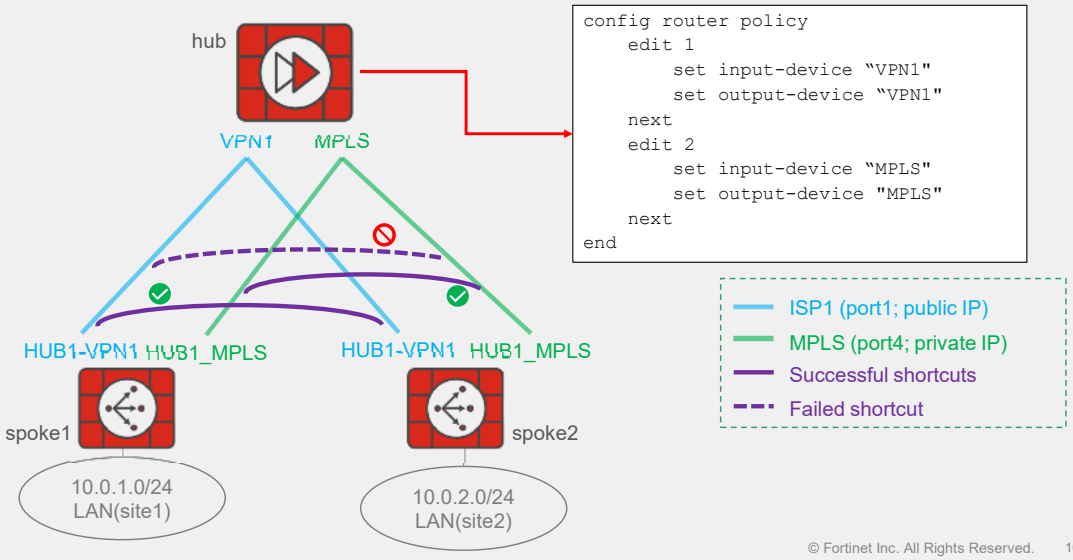


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Overlay Stickiness and ADVPN

- Prefer shortcut negotiation over same-ISP overlays
  - Prevents shortcut negotiation over unreachable underlays (for example, internet and MPLS)




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

In addition to increasing performance, overlay stickiness is also important for ADVPN because it helps to prevent the spokes from trying to negotiate shortcuts over unreachable underlays.

The topology on this slide shows two overlays, one established over ISP1 and another over MPLS. ISP1 is an internet link assigned with a public IP address. MPLS is a private link assigned with a private IP address routable only within the MPLS provider network. Same-ISP overlay shortcuts are negotiated successfully because the spokes can reach the peer IP of each other through the corresponding underlays. However, cross-ISP overlays fail to establish because the ISP1 and MPLS networks are not routable between them. That is, during shortcut negotiation, a spoke using its public IP is unable to reach the private IP of the peer, and vice-versa.

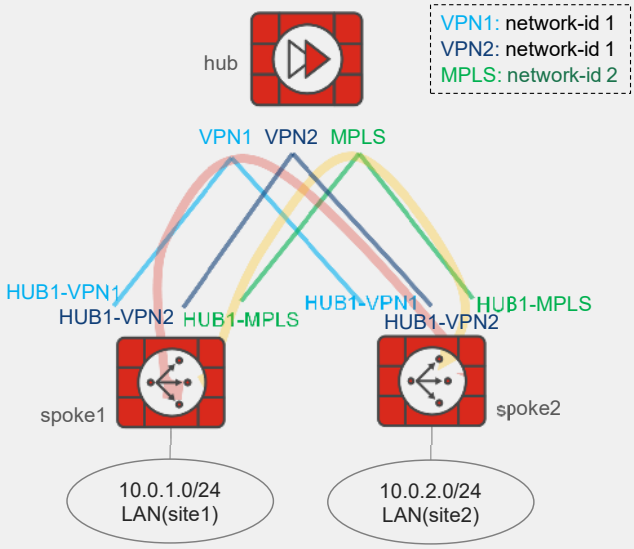


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Prevent Cross-Overlay Shortcuts With Network IDs

- Dedicated command to prevent cross overlay shortcut
- Command:
  `set auto-discovery-crossover block`
- Restricts shortcuts to overlays with the same network ID
- As an alternative or in addition to policy routes




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

As an alternative to the policy route configuration shown on the previous slide, FortiGate administrators can set the parameter `auto-discovery-crossover` to `block` on the hub to prevent cross-overlay shortcuts. When set to `block`, the FortiGate hub will not attempt to establish shortcuts between overlay interfaces with different network IDs. The administrator can use this parameter as an alternative to policy routes or keep both settings.

In the example shown on this slide, to overlays VPN1 and VPN2 share the same network ID—1—because they rely both on ISP connections. The administrator assigned the network ID 2 to the third overlay because it is built on a multiprotocol label switching (MPLS) network. The administrator configured the hub with `auto-discovery-crossover` set to `block` on the hub. With this configuration, the hub will not attempt to establish shortcuts that cannot physically be established between an overlay on an ISP networks and the overlay on the MPLS network. However, it can establish shortcuts between the overlays from both ISPs.

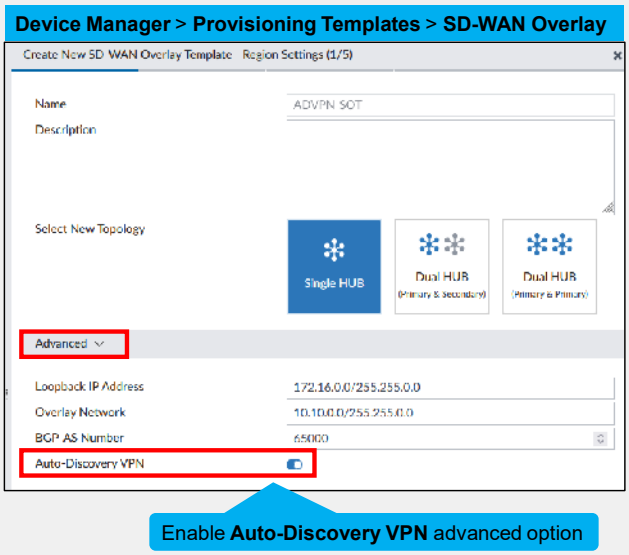


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## ADVPN and FortiManager—SD-WAN Overlay Template

- ADVPN option on SD-WAN overlay template
- Hub
  - IPsec template
    - `add-route` option is disabled
    - `net-device` option is disabled
    - `auto-discovery-sender` option is enabled
  - BGP templates
    - `additional-path` option is enabled
- Spoke
  - IPsec template
    - `add-route` option is disabled
    - `net-device` option is enabled
    - `auto-discovery-receiver` option is enabled
  - BGP templates
    - `recursive-next-hop` option is enabled
    - `additional-path` option is enabled




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

The SD-WAN overlay template on FortiManager allows you to configure ADVPN with a single stitch selector. When you select **Auto-Discovery VPN** on the overlay template, FortiManager configures the IPsec and BGP templates with the necessary parameters to configure ADVPN on the hub and spokes using Fortinet-recommended settings.

For BGP templates, FortiManager defines `additional-path enable` for the hub, and `recursive-next-hop enable` for the spoke .

For IPsec templates, FortiManager enables `auto-discovery-sender` on the hub, `auto-discovery-receiver` on the spoke, and adjusts a few other parameters, as shown this slide.

Note that you must keep the `add-route` option disabled if you use a dynamic routing protocol. This ensures that the IKE protocol does not add additional routes to the spokes and hubs, and that FortiGate keeps only the route configured by the dynamic routing protocol.

Later in this lesson, you will learn about ADVPN 2.0. By opposition to ADVPN 2.0, what you learned in the previous slides is sometimes called ADVPN 1.0. Note that when you use the SD-WAN overlay template to configure ADVPN on your SD-WAN topologies, with FortiManager versions 7.4 and earlier, it defines ADVPN 1.0.

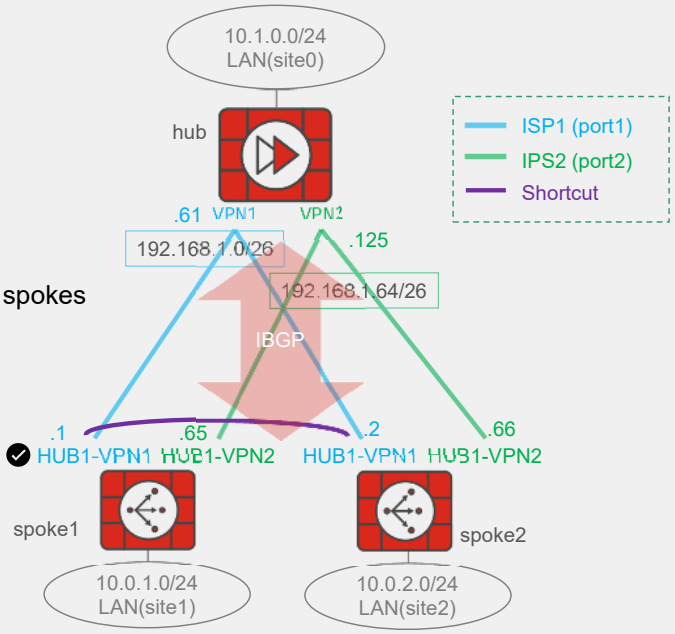


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Summary for Basic SD-WAN + ADVPN Deployment

- Hub
  - `net-device: disable`
  - Route reflector enabled (IBGP)
  - Overlay stickiness configured (policy route)
  - `auto-discovery-sender: enable`
- Spokes
  - Overlays are members of SD-WAN
  - Manual SD-WAN rule ID 1 steers traffic between spokes
  - Performance SLA
  - `net-device: enable`
  - `auto-discovery-receiver: enable`
  - `allowaccess: ping`
  - `mode-cfg: enable`




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

This slide shows the topology used for testing SD-WAN and ADVPN. It's essentially the same basic topology used before, except that the slide indicates the IP addresses assigned to each overlay on the spokes using IKE mode config, and a summary of the configuration applied on the hub and spokes.

The next slides show how the FortiOS routing table, the diagnostic output for SD-WAN rules, and the performance SLA change when a shortcut is established between the spokes after an endpoint behind spoke1 generates traffic to spoke2. Note that the preferred member on spoke1 is HUB1-VPN1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Before Shortcut Is Established—Spoke1

- Routing table and IPsec tunnel summary:

```
# get router info routing-table all
...
B       10.0.2.0/24 [200/0] via 192.168.1.2 [2] (recursive is directly connected, HUB1-VPN1), 2d20h18m, [1/0]
                    [200/0] via 192.168.1.66 [2] (recursive is directly connected, HUB1-VPN2), 2d20h18m, [1/0]
S       192.168.1.61/32 [15/0] via HUB1-VPN1 tunnel 100.64.1.1, [1/0]
# get vpn ipsec tunnel summary
'HUB1-VPN1' 100.64.1.1:0  selectors(total,up): 1/1  rx(pkt,err): 111933/0  tx(pkt,err): 603908/14
'HUB1-VPN2' 100.64.1.9:0  selectors(total,up): 1/1  rx(pkt,err): 121167/0  tx(pkt,err): 627331/11
```

Recursive lookup for next hop 10.201.1.2 is HUB1-VPN1

Installed by iked because of IKE mode config

- SD-WAN service and performance SLA:

```
# diagnose sys sdwan service4 3
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(2):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, selected
    2: Seq_num(5 HUB1-VPN2), alive, selected
...
# diagnose sys sdwan health-check status HUB1_HC
Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(1.544), jitter(0.299) [...] sla_map=0x1
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.431), jitter(0.276) [...] sla_map=0x1
```

Preferred member

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

This slide shows the routing table, IPsec tunnel summary, and relevant SD-WAN diagnostic outputs before the shortcut is established.

Note that the recursive lookup for the next hop of the first IBGP route resolves to HUB1-VPN1. This is because there is a static route to 192.168.1.61/32 that FortiOS adds on spoke1 as a result of the IKE mode config feature, which is enabled.

When FortiGate establishes the tunnel, with IKE mode-config enabled, it install a static route to hub overlay IP address (192.168.1.61/32) with a priority of 15. 15 is the default priority for any static route that IKE mode-config defines.

Note also that the SD-WAN rule is configured in manual mode, and the preferred member is HUB1-VPN1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Bringing Up Shortcut—Spoke1

- Sniffer:

```
#  diagnose sniffer packet any "host 10.0.2.101 and icmp" 4 | grep HUB1-VPN1
...
10.974856 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
10.977462 HUB1-VPN1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
11.975091 HUB1-VPN1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
11.976266 HUB1-VPN1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
12.976186 HUB1-VPN1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
12.977304 HUB1-VPN1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

Shortcut established

- Routing table and IPsec tunnel summary:

```
# get router info routing-table all
...
B       10.0.2.0/24 [200/0] via 192.168.1.2 [2] (recursive is directly connected, HUB1-VPN1_0), 00:06:35
                    [200/0] via 192.168.1.66 [2] (recursive is directly connected, HUB1-VPN2), 00:06:35
C       192.168.1.0/26 is directly connected, HUB1-VPN1
C       192.168.1.2/32 is directly connected, HUB1-VPN1_0
# get vpn ipsec tunnel summary
'HUB1-VPN1_0' 203.0.113.1:0  selectors(total,up): 2/2  rx(pkt,err): 3/0  tx(pkt,err): 3/2
'HUB1-VPN1' 100.64.1.1:0  selectors(total,up): 1/1  rx(pkt,err): 3425/0  tx(pkt,err): 3426/0
'HUB1-VPN2' 100.64.1.9:0  selectors(total,up): 1/1  rx(pkt,err): 3424/0  tx(pkt,err): 3425/0
```

Recursive lookup for next hop 192.168.1.2 is now HUB1-VPN1_0

Installed by iked because of ADVPN

Spoke2 IP (port1)

Shortcut is up

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

When an endpoint with address 10.0.1.101 generates traffic to 10.0.2.101, spoke1 initially steers traffic through the parent overlay HUB1-VPN1. At the same time, the negotiation of the shortcut between spoke1 and spoke2 begins. After the shortcut is established, spoke1 starts routing the traffic through the shortcut (HUB1-VPN1_0).

The routing table on spoke1 also reflects the successful shortcut negotiation. FortiOS installs a static route through the shortcut to reach the overlay IP address of the remote spoke. The result is that the next hop of the IBGP routes to 10.0.2.0/24 now recursively resolves to the shortcut, instead of to the parent tunnel. Note that the IKE mode config connected route to 192.168.1.0/26 through the parent tunnel is still there. It is just that the new static route to 192.168.1.2/32 is better (more specific).

In addition, the IPsec tunnel summary output also shows the new shortcut. Note that the shortcut name is composed by the parent tunnel name followed by an underscore and a number.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Bringing Up Shortcut—Spoke1 (Contd)

- SD-WAN service and performance SLA:

```
# diagnose sys sdwan service4 3
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Member sub interface(4):
    2: seq_num(4), interface(HUB1-VPN1):
      1: HUB1-VPN1_0(28)
  Members(3):
    1: Seq_num(4 HUB1-VPN1_0 HUB1), alive, selected
    2: Seq_num(4 HUB1-VPN1 HUB1), alive, selected
    4: Seq_num(5 HUB1-VPN2 HUB1), alive, selected
...

# diagnose sys sdwan health-check status
Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(1.613), jitter(0.327), ..., sla_map=0x1
Seq(4 HUB1-VPN1_0): state(alive), packet-loss(0.000%) latency(1.358), jitter(0.292),..., sla_map=0x1
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.500), jitter(0.287), ..., sla_map=0x1

# diagnose sniffer packet HUB1-VPN1_0 "" 4
...
0.770110 HUB1-VPN1_0 - 192.168.1.1 -> 192.168.1.2: icmp: echo request
0.771631 HUB1-VPN1_0 - 192.168.1.2 -> 192.168.1.1: icmp: echo reply
```

Shortcut listed as subinterface

Shortcut becomes preferred member

10 seconds after shortcut is established, FortiGate starts monitoring the shortcut using ping and targeting remote overlay IP (192.168.1.2)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

After the shortcut is established, FortiGate lists the shortcut as a subinterface in the SD-WAN rule diagnostic output. FortiGate also starts monitoring the shortcut using ping as protocol and targeting the overlay IP of the remote spoke (192.168.1.2), 10 seconds after the shortcut is established.

Note that FortiGate moves the shortcut to the top of the list, so it takes precedence over the parent tunnel.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Debugging Shortcut Negotiation

- Specify multiple IP addresses to filter the IKE real-time debug
  - Useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations

```
diagnose debug console timestamp enable
diagnose vpn ike log filter clear
diagnose vpn ike log filter mrem-addr4 <ip.of.hub> <ip.of.spoke>
diagnose debug application ike -1
diagnose debug enable
```

Filter on multiple IPv4 destination address (mrem-addr6 for IPv6 address)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

Enable debug of IKE to debug ADVPN shortcut negotiation, as shown on this slide. In the IKE log filter, you can specify multiple IP addresses to print debug messages for. This is very useful when debugging ADVPN shortcuts and spoke-to-spoke ADVPN negotiation issues.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Shortcut Debug—shortcut-offer

- Hub output—hub sends shortcut offer to spoke1:

```
ike V=root:0: shortcut VPN1_0:192.2.0.1:0 to VPN1_1:203.0.113.1:0 for 10.0.1.101->10.0.2.101 0
ike 0 ike_ui_admin_caps_trigger sport 2048, dport 0, proto 1, iif 20
ike V=root:0 send shortcut-offer to VPN1_0
ike V=root:0:VPN1_0:46: sending NOTIFY msg
ike V=root:0:VPN1_0:13:46: send informational
```

- Spoke1 output—spoke1 receives shortcut offer from hub, and then sends shortcut query to hub:

```
ike V=root:0:HUB1-VPN1:8: received informational request
ike V=root:0:HUB1-VPN1:8: processing notify type SHORTCUT_OFFER
ike V=root:0:HUB1-VPN1: ikev2_process_shortcut_offer sport 2048, dport 0, proto 1, iif 20
ike V=root:0:HUB1-VPN1: shortcut-offer 10.0.1.101->10.0.2.101 0 psk 64 ppk 0 ver 2 mode 0, peer-addr
203.0.113.1:0
ike V=root:0 looking up shortcut by addr 10.0.2.101, resp-name:, name HUB1-VPN1, peer-addr 203.0.113.1:0
ike V=root:0:HUB1-VPN1: send shortcut-query 2456748025368782036 47381fce98c67ded/0000000000000000 192.2.0.1
10.0.1.101->10.0.2.101 0 psk 64 ttl 32 nat 0 ver 2 mode 0 network-id 1
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

This slide shows an example of the real-time debug output displayed by IKE during a shortcut negotiation triggered after spoke1 communicates with spoke2 over the parent tunnel.

The shortcut negotiation starts on the hub. On the hub, the tunnel to spoke1 is `VPN1_0`, and its remote gateway is `192.2.0.1`. The tunnel to spoke2 is `VPN1_1`, and its remote gateway is `203.0.113.1`. The hub identifies that a shortcut can be negotiated between the two spokes for traffic sourced from `10.0.1.101` and destined to `10.0.2.101`. For this reason, the hub sends a shortcut offer to spoke1 to initiate the shortcut negotiation.

Spoke1 then receives the shortcut offer from the hub, to which it replies with a shortcut query.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Shortcut Debug—`forward shortcut-query`

- Hub output—hub receives shortcut query from spoke1 and forwards it to spoke2:

```
ike V=root:0:VPN1_0:13: received informational request
ike V=root:0:VPN1_0:13: processing notify type SHORTCUT_QUERY
ike V=root:0:VPN1_0: recv shortcut-query 13079782794578682520 3457fd9837d92f61/0000000000000000 192.2.0.1
10.0.1.101:2048->10.0.2.101:0 0 psk 64 ppk 0 ttl 32 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:VPN1: iif 20 10.0.1.101->10.0.2.101 0 route lookup oif 20 VPN1 gwy 192.168.1.2
ike V=root:0: shared dev tunnel lookup, tun-id=192.168.1.2
ike V=root:0:VPN1_1: forward shortcut-query 13079782794578682520 3457fd9837d92f61/0000000000000000
192.2.0.1 10.0.1.101->10.0.2.101 0 psk 64 ppk 0 ttl 31 ver 2 mode 0, ext-mapping 192.2.0.1:0, network-id 1
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

The hub receives the shortcut query from spoke1 and forwards it to spoke2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Shortcut Debug—Spoke2—shortcut-reply

- Spoke2—spoke2 receives shortcut query from hub, and then sends shortcut reply to hub:

```
ike V=root:0:HUB1-VPN1:13: received informational request
ike V=root:0:HUB1-VPN1:13: processing notify type SHORTCUT_QUERY
ike V=root:0:HUB1-VPN1: recv shortcut-query 9828560659066150666 5a1b8a251891a87b/0000000000000000 192.2.0.1
10.0.1.101:2048->10.0.2.101:0 0 psk 64 ppk 0 ttl 31 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:HUB1-VPN1: iif 20 10.0.1.101->10.0.2.101 0 route lookup oif 7 port5 gwy 0.0.0.0
ike V=root:0:HUB1-VPN1: shortcut-query received from 192.2.0.1:500, local-nat=no, peer-nat=no
ike V=root:0:HUB1-VPN1: send shortcut-reply 9828560659066150666 5a1b8a251891a87b/8255ccf4af12fb8f
203.0.113.1 to 10.0.1.101 0 psk 64 ppk 0 ver 2 mode 0 network-id 1/1
```

- Hub output—hub receives shortcut reply from spoke2 and forwards it to spoke1:

```
ike V=root:0:VPN1_1:14: received informational request
ike V=root:0:VPN1_1:14: processing notify type SHORTCUT_REPLY
ike V=root:0:VPN1_1: recv shortcut-reply 13079782794578682520 3457fd9837d92f61/810cdbceaa157463 203.0.113.1
to 10.0.1.101 0 psk 64 ppk 0 ver 2 mode 0 ext-mapping 0.0.0.0:0, network-id 1/1
ike V=root:0:VPN1: iif 20 10.0.2.101->10.0.1.101 0 route lookup oif 20 VPN1 gwy 192.168.1.1
ike V=root:0: shared dev tunnel lookup, tun-id=192.168.1.1
ike V=root:0:VPN1_0: forward shortcut-reply 13079782794578682520 3457fd9837d92f61/810cdbceaa157463
203.0.113.1 to 10.0.1.101 0 psk 64 ppk 0 ttl 31 ver 2 mode 0 ext-mapping 203.0.113.1:0
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

Spoke2 receives the shortcut query from the hub, to which it responds with a shortcut reply. The hub then receives the shortcut reply from spoke2 and forwards it to spoke1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Shortcut Debug—Shortcut Established

- Spoke1 output—spoke1 receives shortcut reply from hub, and then initiates tunnel negotiation with spoke2:

```
ike V=root:0:HUB1-VPN1:8: received informational request
ike V=root:0:HUB1-VPN1:8: processing notify type SHORTCUT_REPLY
ike V=root:0:HUB1-VPN1: recv shortcut-reply 7710043960895744004 352120eba5982918/f3ee894fe131e22b
203.0.113.1 to 10.0.1.101 0 psk 64 ppk 0 ver 2 mode 0 ext-mapping 203.0.113.1:0, network-id 1/1
ike V=root:0:HUB1-VPN1: iif 20 10.0.2.101->10.0.1.101 0 route lookup oif 7 port5 gwy 0.0.0.0
ike V=root:0:HUB1-VPN1: shortcut-reply received from 203.0.113.1:500, local-nat=no, peer-nat=no
ike V=root:0:HUB1-VPN1:HUB1-VPN1: created connection: 0x103367d0 3 192.2.0.1->203.0.113.1:500.
ike V=root:0:HUB1-VPN1: adding new dynamic tunnel for 203.0.113.1:500
ike V=root:0:HUB1-VPN1_0: tunnel created tun_id 203.0.113.1/::203.0.113.1 remote_location 0.0.0.0
ike V=root:0:HUB1-VPN1_0: added new dynamic tunnel for 203.0.113.1:500
ike V=root:0:HUB1-VPN1_0: shortcut selector added new 1 a203
```

- Spoke1 output—shortcut `HUB1-VPN1_0` is established:

```
ike V=root:0:HUB1-VPN1_0:22:HUB1-VPN1:71: sending SNMP tunnel UP trap
ike V=root:0:HUB1-VPN1_0: tunnel up event
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

Spoke1 receives the shortcut reply from the hub, and then starts the IKE negotiation to bring up the shortcut tunnel. Shortly after, the shortcut (`HUB1-VPN1_0`) is established.

Note that for this example, the name of the spoke1 tunnel on the hub is the same as the shortcut tunnel on spoke1. However, the tunnels are different. That is, on the hub, HUB1-VPN1_0 is the child tunnel that connects the hub to spoke1, and that results from configuring the hub as the IPsec dial-up server. On spoke1, HUB1-VPN1_0 is the shortcut negotiated with spoke2. Both the child dial-up and shortcut tunnels use the same name convention.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Identify Shortcuts on Log Messages

- Log messages field **advpnsc**
  - Shortcut tunnel: `advpnsc=1`
  - Other tunnels: `advpnsc=0`
- Filter ADVPN shortcut log messages on FortiGate
  - `execute log filter category event`
  - `execute log filter field advpnsc 1`

```
branch1_fgt # exec log filter category event
branch1_fgt # exec log filter field advpnsc 1
branch1_fgt # exec log display
23 logs found.
10 logs returned.

10: date=2024-09-20 time=09:37:57
eventtime=1726850277059859240 tz="-0700"
logid="0101037127" type="event" subtype="vpn"
level="notice" vd="root" logdesc="Progress IPsec ...]
vpntunnel="HUB1-VPN1_0" status="success" init="local"
exch="AUTH" dir="inbound" role="initiator"
result="DONE" version="IKEv2" fctuid="N/A" advpnsc=1
```

ADVPN shortcut flag

Shortcut tunnel name

- On FortiAnalyzer
  - Column **AD-VPN Shortcut**

**Log View > Event > VPN**

branch1_fgt | Last 30 Minutes | 09:23:04 - 09:53:04

advpnsc="1"

ADVPN shortcut filter

| # | Action | Message | VPN tunnel | AD-VPN Shortcut |
|---|---|---|---|---|
| 1 | tunnel-stats | IPsec tunnel statistics | HUB1-VPN1_0 | 1 |
| 2 | tunnel-stats | IPsec tunnel statistics | HUB1-VPN1_0 | 1 |
| 3 | negotiate | progress IPsec phase 2 | HUB1 VPN1_0 | 1 |
| 4 | phase2-up | IPsec phase 2 status chan | HUB1-VPN1_0 | 1 |
| 5 | install sa | install IPsec SA | HUB1-VPN1 0 | 1 |

ADVPN shortcut flag

Activate AD-VPN Shortcut column to view the flags

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

When reviewing VPN log messages, the field `advpnsc` will help you identify the shortcut VPN tunnels. FortiGate will set `advpnsc` value `1` for any log messages related to shortcut tunnels; for any other tunnel, the `advpnsc` value is set to `0`.

When viewing the log on FortiAnalyzer, you can display the column **AD-VPN Shortcut** to view the `advpnsc` flag.

This slide shows examples of log display, filtered to see only ADVPN-related messages on the FortiGate CLI and on the FortiAnalyzer GUI.

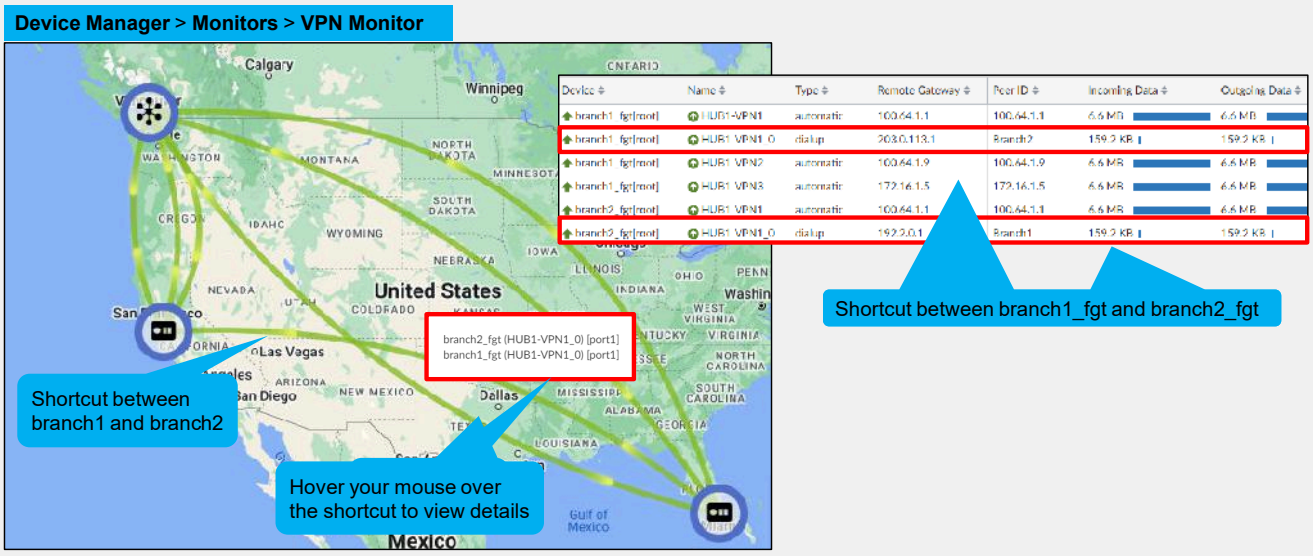


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Monitor ADVPN Shortcuts on FortiManager

- FortiManager **VPN Monitor** page displays the shortcut tunnels




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

On this slide you can see an example of the **VPN Monitor** page available on FortiManager. On the map view, you can see a graphical representation of active shortcuts. You can hover your mouse over any tunnel, including shortcuts, to see details. On the table view, you can see details about each tunnel and each shortcut, with bandwidth usage statistics for each of them.

Note that the table view displays two lines for each tunnel and each shortcuts. Each line represents one end of the tunnel.

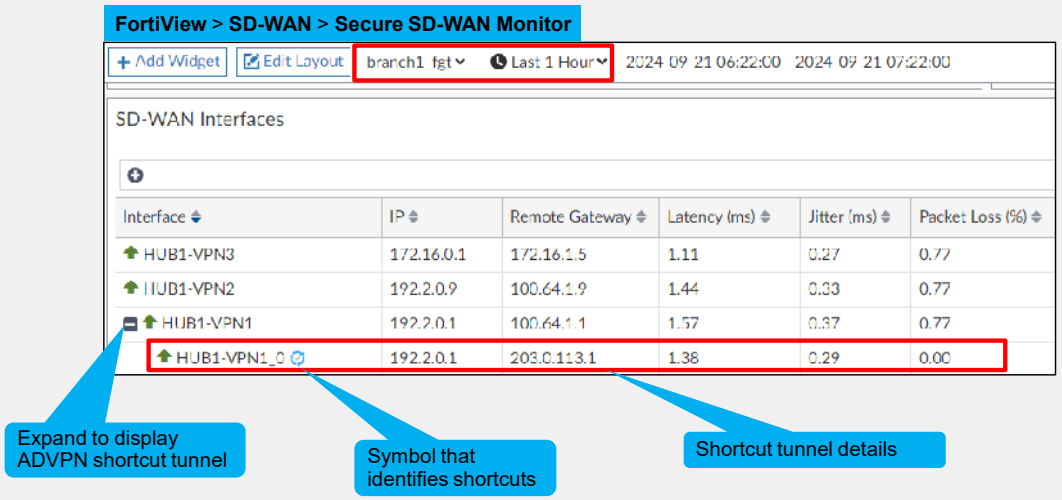


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Monitor ADVPN Shortcuts on FortiAnalyzer

- FortiView **Secure SD-WAN Monitor** page displays ADVPN shortcut information




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

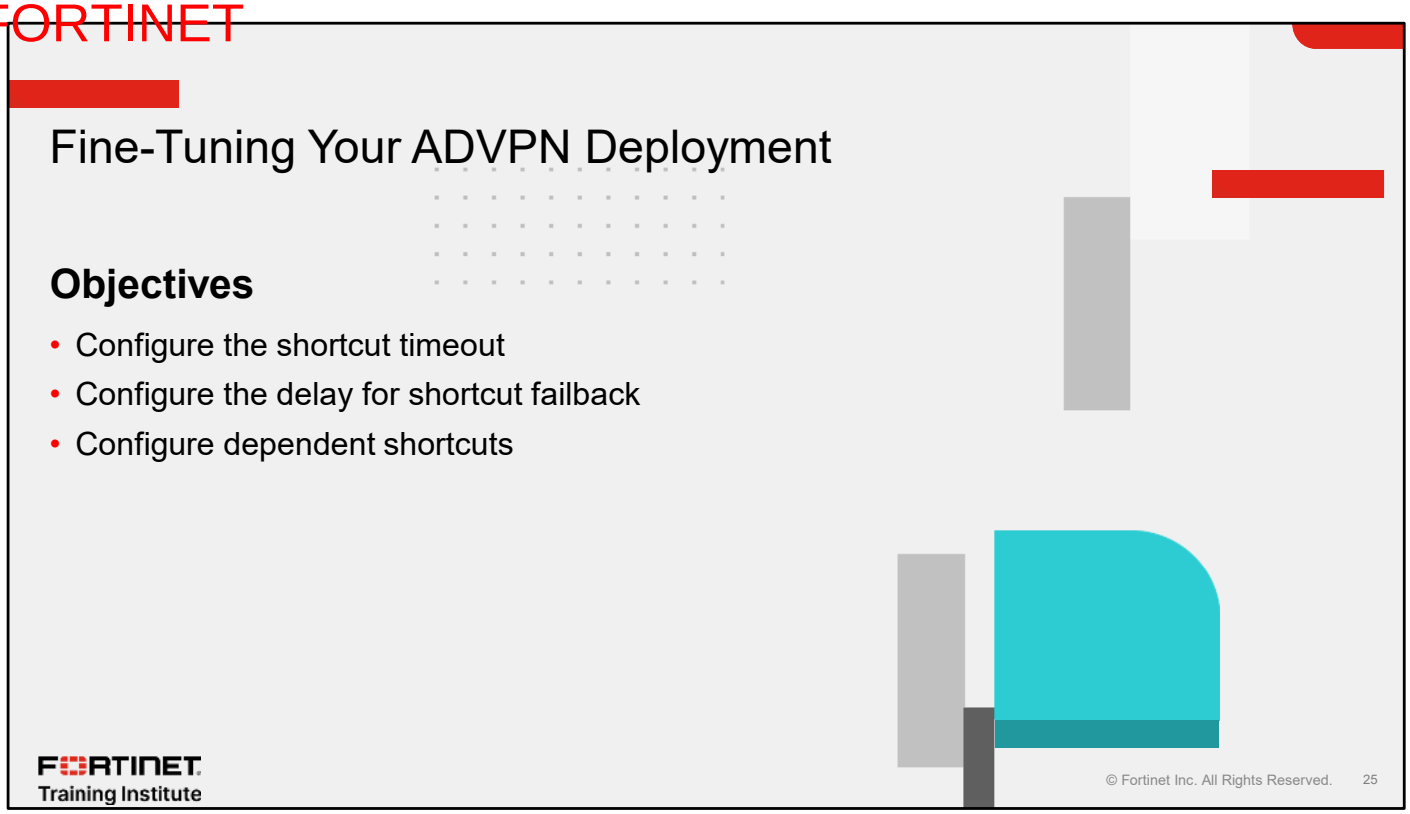
On this slide you can see an example of the **SD-WAN Interface** widget available on the **Secure SD-WAN Monitor** page. It displays bandwidth and performance information for SD-WAN interfaces. For some tunnel interfaces, you will see an expand button near the interface name, which indicates that one or more ADVPN shortcuts are established from this tunnel. Expand the display to see details for ADVPN shortcut tunnels.

Note that for VPN tunnels, the **IP** and **Remote Gateway** columns display the local IP address and remote gateway IP address of the VPN tunnel.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in fine-tuning your ADVPN deployment, you will be able to configure the network to save resources, speed up routing convergence, and improve the user experience for sensitive applications.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Timing Out Idle Shortcuts

- By default, shortcuts inherit lifetime settings of parents
  - Idle shortcuts may remain up for a long time
    - Waste of resources
- Set an idle timeout to shortcuts to save resources
  - FortiGate brings down shortcuts with no user traffic for a set period of time
    - Health check traffic doesn't count

- Spoke configuration:

```
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        set idle-timeout enable
        set idle-timeoutinterval 5
    next
end
```

- IKE debug upon timeout:

```
ike V=root:0:HUB1-VPN1_0: connection idle time-out
ike V=root:0:HUB1-VPN1_0: going to be deleted
ike V=root:0:HUB1-VPN1_0: flushing
...
ike V=root:0:HUB1-VPN1_0: sending SNMP tunnel DOWN trap
for HUB1-VPN1
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

By default, shortcuts inherit their lifetime from their parent tunnels. That is, if the lifetime of a parent tunnel is 1800 seconds, then its shortcuts also use the same lifetime.

Usually, the lifetime of an IPsec tunnel is set for a few hours, which means that idle shortcuts remain up for the same period of time unless they are manually flushed or are detected dead by DPD, which can lead to unnecessary resource utilization on spokes.

To reduce resource utilization, you can configure an idle timeout for shortcuts. This way, FortiGate brings down a shortcut if it hasn't been used for forwarding user traffic in a certain period of time. Note that health check traffic is not considered user traffic and, therefore, it doesn't prevent an idle tunnel from timing out.

This slide shows how to set an idle timeout for shortcuts. The example configuration sets an idle timeout of five minutes. This slide also shows some of the relevant messages seen in the IKE debug when a shortcut times out.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Making Shortcuts Lifetime Dependents of Parents

- By default, lifetime of a shortcut is independent of the parent tunel lifetime
  - Shortcuts remain up if parent goes down
    - Waste of resources
    - Slows down routing convergence
- Bring down shortcuts immediately after parent goes down (default = `independent`):

```
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        set auto-discovery-shortcuts dependent
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

By default, shortcuts are not brought down if the parent tunnel goes down. That is, the lifetime of a shortcut is independent of its parent tunnel.

To save resources and obtain a faster routing convergence, you can instruct FortiGate to bring down a shortcut immediately after its parent tunnel goes down by configuring the `auto-discovery-shortcuts` to `dependent`, as shown on this slide. By default, the setting is set to `independent`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Delaying Failback to Recovered Shortcut

- Delay use of recovered members
  - Including shortcuts
- Wait until `hold-down-time` has passed
  - More accurate monitoring
  - Prevent impact to:
    - Sensitive applications during brownout conditions and SLA changes
    - CPU usage caused by session re-evaluation
- Highly recommended for SD-WAN + ADVPN + lowest cost (SLA) rules deployments

- Example configuration (default = `0`):

```
config system sdwan
    config service
        edit 1
            set hold-down-time 20
        next
    end
end
```

- SD-WAN rule status:

```
# diagnose sys sdwan service4 1

Service(1): Address Mode(IPV4) flags=0x200 use-
shortcut-sla use-shortcut
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1-
>65535):dst(1->65535), Mode(sla), sla-compare-order
Hold down time(20) seconds, Hold start 84259 second,
now 84270
...
```

Value decrease when timer active (SLA recovered for higher priority member)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

When you use lowest cost (SLA) rules, FortiGate uses the lowest cost member that meets the configured SLA target. If a member doesn't meet the SLA target, it is considered out of SLA and therefore, placed at the bottom of the outgoing interface list.

Links that are impacted by brownout conditions—that is, the link is up but its quality is degraded—may switch in and out of SLA states in short periods of time. This may result in poor user experience for sensitive applications such as voice or video, as well as high CPU utilization caused by frequent session re-evaluation.

To prevent immediate failback to a recovered member, including recovered shortcuts, you can configure the `hold-down-time` setting on an SD-WAN rule. The result is that FortiGate waits a set number of seconds before moving a recovered member back to its original place in the outgoing interface list. This way, FortiGate can monitor the member more accurately and ensure it meets the required SLA target for a certain amount of time before it starts to steer traffic to it.

This slide shows an example configuration of the `hold-down-time` setting, which is set to 20 seconds. The setting applies to all members configured in the rule, including ADVPN shortcuts. Configuring a value of at least 20 seconds on SD-WAN and ADVPN deployments using lowest cost (SLA) rules is highly recommended.

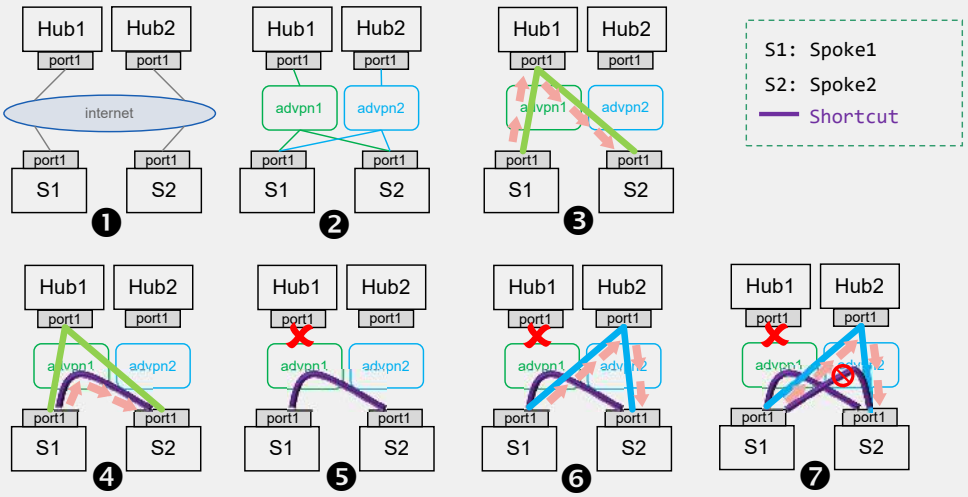
Note that the setting affects only the lowest cost (SLA) and best quality rules. The `hold-down-time` default value is `0`, which means there is no failback delay. When you set it to a value higher than 0, the service SD-WAN rule status reflects the change, as shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Multiple Shortcuts Over the Same Pair of Gateways




- Lifetime of shortcuts are independent of parent tunnels (default setting)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

Consider the dual-hub topology shown on this slide, which shows two hubs and two spokes.

1. All devices have one internet underlay on port1.
2. The spokes have dual IPsec overlays, one to each hub. ADVPN is enabled on the overlays.
3. Traffic from spoke1 to spoke2 initially flows through the parent tunnel to hub1 and a shortcut negotiation starts.
4. A shortcut between spoke1 and spoke2 is established, and spoke-to-spoke traffic starts to flow through the shortcut.
5. On hub1, internet access is lost, which results in the parent tunnel between hub1 and spoke1 going down. The shortcut, however, remains up because its lifetime is independent of the parent tunnel (default behavior).
6. Routing information on spoke1 is updated, and now spoke2 is reachable through hub2, which triggers a session re-evaluation. Traffic from spoke1 to spoke2 starts flowing through hub2, and a shortcut negotiation over hub2 starts. At this point, the first shortcut negotiated over hub1 is still up.
7. Shortcut negotiation over hub2 fails because there is already a shortcut established between the same pair of gateways. That is, the local and remote gateway IP addresses are the same.

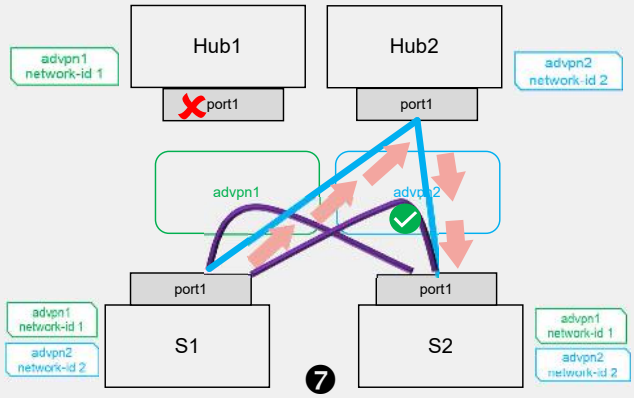


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Multiple Shortcuts With Network IDs

- Assign different network IDs to overlays to allow multiple shortcuts between two spokes




- Example configuration:

```
config vpn ipsec phase1-interface
    edit "advpn1"
        set ike-version 2
        set network-overlay enable
        set network-id 1
    next
    edit "advpn2"
        set ike-version 2
        set network-overlay enable
        set network-id 2
    next
end
```

By default, the SD-WAN overlay template defines one `network-id` per overlay

- Supported by IKEv2 only
- Can be used for gateway lookup
  - Multiple IPsec dial-up VPNs on the same local gateway

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

To allow the spokes to establish shortcuts between the same pair of local and remote gateway IP addresses, set a network ID on each overlay, as shown on this slide. The network ID feature is supported by IKEv2 only.

When you set a different network ID for each overlay, both shortcuts, the one negotiated over hub1 and the one negotiated over hub2, can be established at the same time.

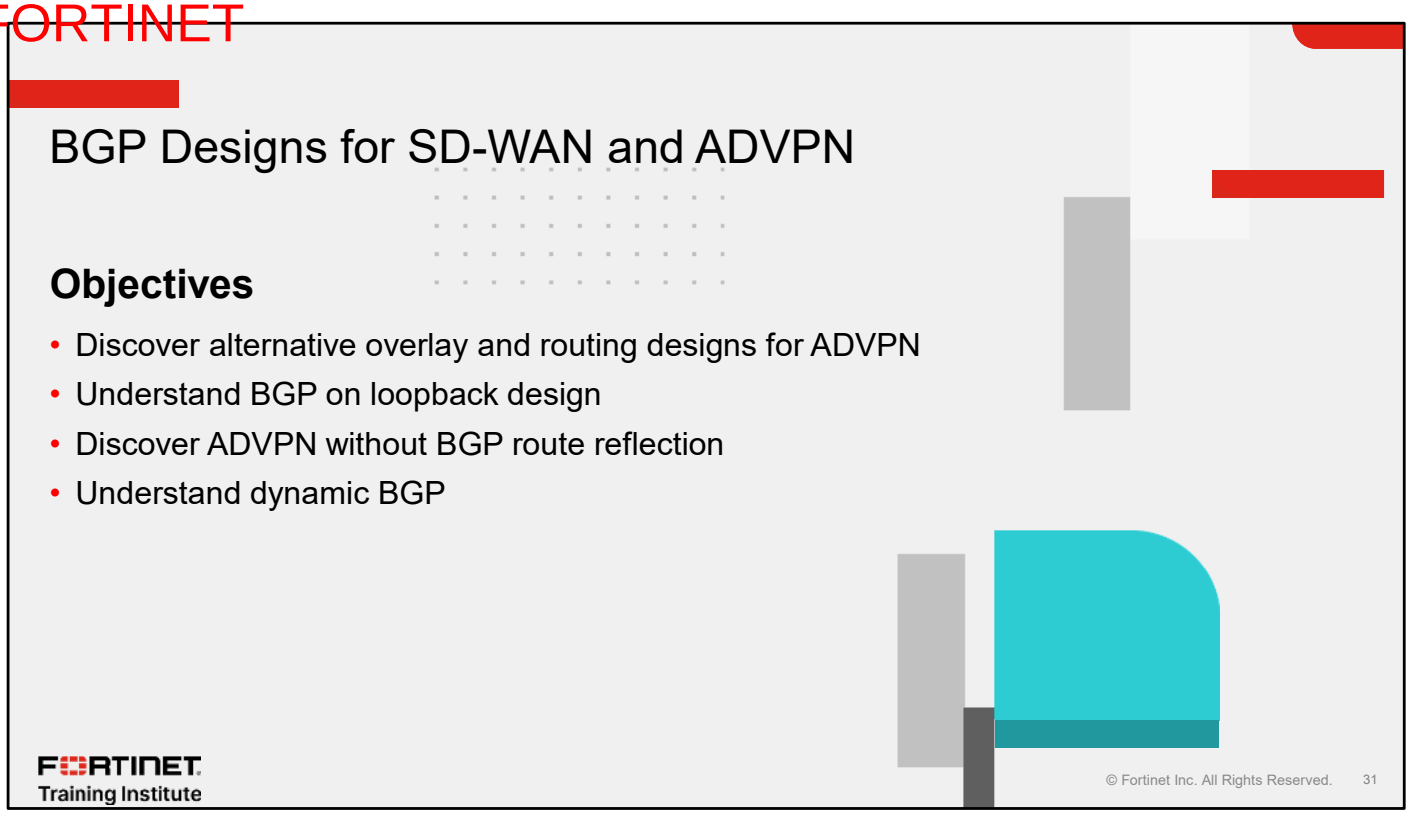
The network ID is also useful for gateway lookup, when you configure multiple dial-up VPNs that terminate on the same local IP address, and you want users to connect to a particular VPN. Because the network ID is in the first packet of the initiator, it can be used to identify the correct phase 1 gateway configuration to match.

Note that you need to enable `network-overlay` to configure `network-id`. When you use the SD-WAN overlay template to define your overlay tunnels, it enables `network-overlay` and defines a different network ID per overlay, for each phase 1 interface.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the overlay design options for ADVPN and the advantages and disadvantages of each of them, you will be able to select and configure the best option for your network.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Routing Overlay Designs for SD-WAN and ADVPN

- Original design
  - Routing protocol: BGP
  - One BGP peer for each overlay
  - Route reflector on the hub
  - Prefix redistribution
- Advantages
  - Easy to configure
  - Simple to understand
- Disadvantages
  - Not suitable for large topologies with thousands of branches
  - High load on the hub for a large design
  - The routing table grows exponentially when the number of branches increases
- Available designs increased with FortiOS versions
  - Multiple options available
  - Accommodate various customer requirements
- Examples
  - BGP on loopback interfaces
  - IPsec selector with static routing
  - BGP without route reflection and IPsec selector
  - Dynamic BGP
- Advantages
  - Improves scalability
  - Suitable for large networks
  - Removes the requirement for route reflection or limits its impact
  - Some compatible with OSPF and static routing

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

When Fortinet introduced ADVPN, you could configure it with only the BGP routing protocol on the overlay, BGP neighbor relationship established for each overlay tunnel, route reflection, and prefix redistribution enabled on the hub. This design is well understood and easy to configure. However, it has some drawbacks and limitations; notably, it does not scale well when the number of branches increases. In large-scale networks, the BGP route reflection approach can lead to high CPU usage on the hub FortiGate device, due to the significant processing required to reflect routes to the spokes. Additionally, the spoke FortiGate devices must learn many unnecessary routes, which could impact network efficiency.

In later FortiOS versions, Fortinet introduced design alternatives to offer solutions for scenarios where a large number of spokes and routes are involved. Though ADVPN with route reflection is still common in the field, administrators can now select from multiple design options. All of these options improve the scalability and the overall performance of the solution, and remove the requirement for route reflection, or limit its impact.

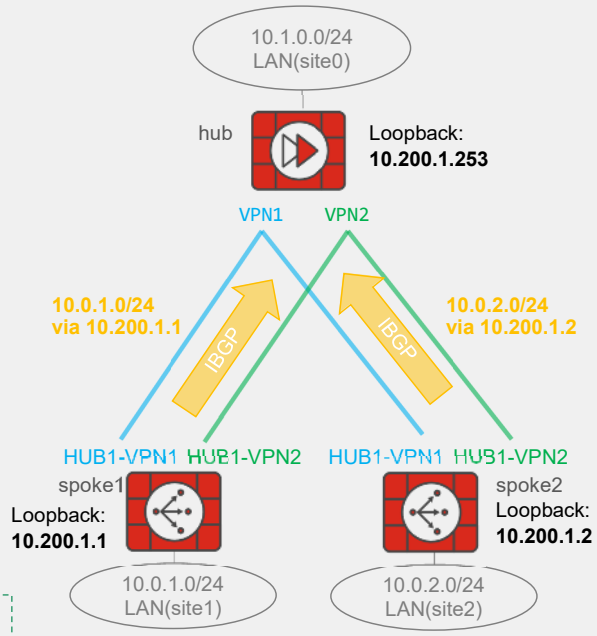


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## BGP on Loopback

- Each branch establishes a single IBGP session with the hub
- IBGP sessions between loopback interfaces on the branch and on the hub
- Routes recursively resolved through all available overlays
- Advantages
  - One peering between the hub and the spokes, regardless the number of overlays
  - Improved scalability
  - Simplified configuration
- Limitation
  - Reduced support for hub-to-edge SD-WAN




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

With BGP on loopback, each branch establishes a single IBGP session with the hub, compared to one IBGP session for each overlay with the historical design.

At the configuration level, you define a loopback IP address on each device, and use those addresses to define the BGP peering between the hub and the spokes. FortiGate terminates the IBGP session on the loopback interface on both sides, but still resolves the routes recursively, through all available overlays. FortiGate generates and propagates a single BGP route for each LAN prefix.

Compared to the traditional BGP per overlay design, the BGP on loopback design improves scalability and simplifies configuration. This is particularly true on the hubs, since they must reflect a much smaller number of routes between a much smaller number of IBGP peers. Note that BGP route reflection is a "square problem" (O(n^2)): the number of routes to reflect equals the number of routes multiplied by the number of peers. Therefore, reducing both these numbers significantly improves the scalability of the route reflector. Additionally, since only a single BGP route is generated for each LAN prefix, BGP add-path functionality is no longer required. Thus, the hubs do not inflate the number of routes, neither when reflecting them between the spoke devices, nor when advertising them to other regions.

While BGP on loopback greatly increases scalability, it also reduces the possibility for hub-side steering, or SD-WAN on the hub. BGP on loopback is not compatible with the use of route-tags or with the configuration of route priority. However, you can use SD-WAN with remote SLA to influence the path selection on the hub.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Configure ADVPN With BGP on Loopback—Hub

- Hub configuration
  - IPsec

```
config vpn ipsec phase1-interface
    edit "VPN1"
        ...
        set ike-version 2
        set net-device disable
        set exchange-ip-addr4 10.200.1.253
        set add-route disable
        set auto-discovery-sender enable
```

Hub loopback IP address
Configure the same IP address for `exchange-ip-addr4` for each tunnel

  - Firewall policy

```
config firewall policy
    edit x
        set name "loopback"
        set srcintf "VPN1" "VPN2"
        set dstintf "loopback"
        set action accept
```

Allow traffic from the IPsec tunnels to the loopback IP address

- BGP routing

```
config router bgp
    ...
    set ibgp-multipath enable
    set recursive-next-hop enable
      config neighbor-group
        edit "advpn"
            ...
            set next-hop-self enable
            set interface "loopback"
            set update-source "loopback"
        ...
      config neighbor-range
         edit 1
           set prefix 10.200.1.0 255.255.255.0
           set neighbor-group "advpn"
         ...
      config network
         edit 1
           set prefix 10.200.1.0 255.255.255.0
      ...
```

`10.200.1.0/24` is the loopback subnet for the hub and for the spokes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

To configure ADVPN with BGP on loopback on the hub, configure the loopback IP address as `exchange-ip-adr4` for the phase1 of each IPsec interface. Then, because VPN tunnels don't have their own IP addresses, define a firewall policy to allow traffic from the VPN interfaces to the loopback IP address. You need this policy to allow the BGP traffic.

The BGP configuration itself is similar to standard ADVPN with IBGP configuration. You must enable `recursive-next-hop`, and for each neighbor group, you must enable `next-hop-self`. The `interface` and `update-source` settings point to the loopback IP address instead of each VPN interface IP address.

In the example shown on this slide, the network `10.200.1.0/24` is the loopback subnet for the hub and all spokes. The hub needs to distribute this network, because the spokes use this network for next-hop resolution.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Configure ADVPN With BGP on Loopback—Spoke

- Spoke1 configuration
  - IPsec

```
config vpn ipsec phase1-interface
    edit "VPN1"
        ...
        set ike-version 2
        set net-device enable
        set exchange-ip-addr4 10.200.1.1
        set add-route disable
        set auto-discovery-receiver enable
```

Spoke loopback IP address
Configure the same IP address for `exchange-ip-addr4` for each tunnel

  - Firewall policy

```
config firewall policy
    edit x
        set name "loopback"
        set srcintf "VPN1" "VPN2"
        set dstintf "loopback"
        set action accept
```

Allow traffic from the IPsec tunnels to the loopback IP address

- BGP routing

```
config router route-map
        edit "set-tag-hub1"
            config rule
                edit 1
                    set set-tag 1    ...
config router bgp
        set ibgp-multipath enable
        set recursive-next-hop enable
        set tag-resolve-mode merge
            config neighbor
                edit "10.200.1.253"
                    set interface "loopback"
                    set route-map-in "set-tag-hub1"
                    set update-source "loopback"
                    set additional-path both
                ...
            config network
                edit 1
                    set prefix 10.0.1.0/24
                next
                edit 2
                    set prefix 10.200.1.1/32
...
```

Set a different tag for routes received from each hub

Required on the spokes

Spoke1 LAN subnet

Local loopback only

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

The example on this slide shows the configuration of spoke1. The configuration on the other spoke devices is similar, except for the IP addresses.

Note the following two BGP settings that are important to correctly resolve next-hop, and for the correct routing through ADVPN shortcuts:

- `set recursive-next-hop enable` allows the resolution of the next-hop through another BGP route.
- `set tag-resolve-mode merge` allows the resolution of the next-hop with the best-match route, and with the route with the same tag, at the same time. You need this setting to keep the route to the hub in the routing table after ADVPN has established shortcuts. This parameter also helps to manage some degraded routing conditions, such as when the connectivity between the spoke and the two hubs remains active but one hub has lost connectivity to the destination subnet.

At the same time, it is necessary to mark routes with tags in the incoming direction, with a different tag for routes received from each hub. This is the purpose of the parameter `set-tag` in the `route-map` configuration.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## ADVPN With Phase2 Selector

- Historical alternative ADVPN design, often called ADVPN without route reflection
- Compatible with static, OSPF, or BGP routing—BGP recommended and the most used
- Routing over shortcuts managed by IPsec
- Each site announces its protected subnet during IPsec negotiation

- Advantages and limitations

| | Phase 2 selector | Route Reflection |
|---|---|---|
| Routing (overlay / LAN) | Static / BGP / OSPF | BGP |
| Route reflector on hub | No | Yes |
| BGP route aggregation | Yes | No |
| Prefixes redistribution | No | Yes |
| Definition of local networks on IPsec phase2 | Yes | No |
| VRF-aware overlay | Not compatible | Compatible |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

FortiGate can use BGP route reflection to allow routing through ADVPN tunnels, but what about ADVPN on a network with static routing?
Prior to FortiOS 7.2.0, it was not possible to use ADVPN without BGP routing. Now, FortiGate can take advantage of Phase 2 selectors to allow ADVPN without route reflection which makes ADVPN compatible with static routing.

Instead of BGP route reflection, routing over ADVPN shortcuts is managed by IPsec. When phase2 selectors are used, each site announces its protected subnets during IPsec negotiation for tunnel establishment.

Route reflection and the phase2 selector both allow routing through ADVPN shortcuts. Each has its own advantage and limitations. The main factors that you should consider when selecting an option are summarized in the table shown on this slide.

With BGP routing, two options are possible. Note that phase 2 selector allows BGP route aggregation, which simplifies the routing table. On hubs, it reduces the BGP daemon process load and can help improving scalability on large ADVPN networks. The phase 2 selector option also allows a simplified BGP configuration (no `route-reflection`, no `add-path`), but it adds configuration requirements on IPsec phase 2: The administrator must define each local network.

Note that ADVPN with static or OSPF routing is not commonly used. Fortinet recommends that you limit the use of such designs to small networks where branches number in the hundreds, but no higher.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Configure ADVPN with Phase2 Selector—Hub

- Hub configuration
  - IPsec

```
config vpn ipsec phase1-interface
    edit "VPN1"
        ...
        set ike-version 2
        set net-device disable
        set auto-discovery-sender enable
    next
end
```

- Routing options
  - Static routing
  - OSPF
  - BGP
  - For BGP routing

```
config router bgp
    ...
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-select 3
    config neighbor-group
        edit "VPN1"
            ...
            set additional-path send
            set adv-additional-path 3
            set route-reflector-client disable
        next
```

Keep advertisement of additional path for SD-WAN

Disable route reflection (default setting)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

To use ADVPN with phase2 selector, IPsec configuration on the hub is similar to one you will do for ADVPN with route-reflector. On the phase1, you need to enable ADVPN `auto-discovery-sender` and should keep `net-device` to disable. There are no specific setting required for the phase2 on the hub.

You should make sure that required routing for the overlay is correctly configured. It can be static, OSPF or BGP. If you use BGP routing and SD-WAN, you should allow additional path advertisement to allow SD-WAN to learn all possible paths and correctly steer the traffic. Keep the parameter `route-reflector-client` disabled (default setting).



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Configure ADVPN with Phase2 Selector—Spoke

- Spoke configuration
  - IPsec

```
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
         ...
         set ike-version 2
         set net-device enable
         set add-route enable
         set mode-cfg enable
         set auto-discovery-receiver enable
         set mode-cfg-allow-client-selector enable
         ...
    next
config vpn ipsec phase2-interface
    edit "HUB1-VPN1"
         ...
         set src-addr-type name
         set dst-addr-type name
         set src-name "LAN_Net"
         set dst-name "all"
    next
...
```

Allow mode-cfg client to use custom selectors

Select `name` to define src/dst addresses as address object
Select `subnet` for direct configuration as subnet

Local subnet or user defined subnet or subnet group

Both selectors must be of same type (`name` or `subnet`)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

To use phase2 selectors to inject IKE routes on ADVPN shortcuts tunnel you must adjust IPsec configuration on the spokes as shown on this slide.

On IPsec phase1, you must enable configuration method (`mode-cfg enable`) and allow addition of routes per the destination selector (`add-route enable`). You must also enable the parameter `mode-cfg-allow-client-selector` to allow the configuration of custom selector at phase2 level.

On the phase2, you will define local subnets that will be injected on tunnel and tunnel shortcut establishment. You can define the local subnet directly as a subnet or as firewall address object. On configuration example shown on this slide, the source subnet is defined with firewall address group LAN_net. This type of configuration with address object is required when you want to define multiple subnets as phase2 source.

ADVPN shortcuts establishment follow the same steps with Phase2 selectors and route-reflection—shortcut offer, shortcut query, shortcut reply. For troubleshooting and to review shortcut tunnel establishment you can use the commands seen earlier in this lessons.

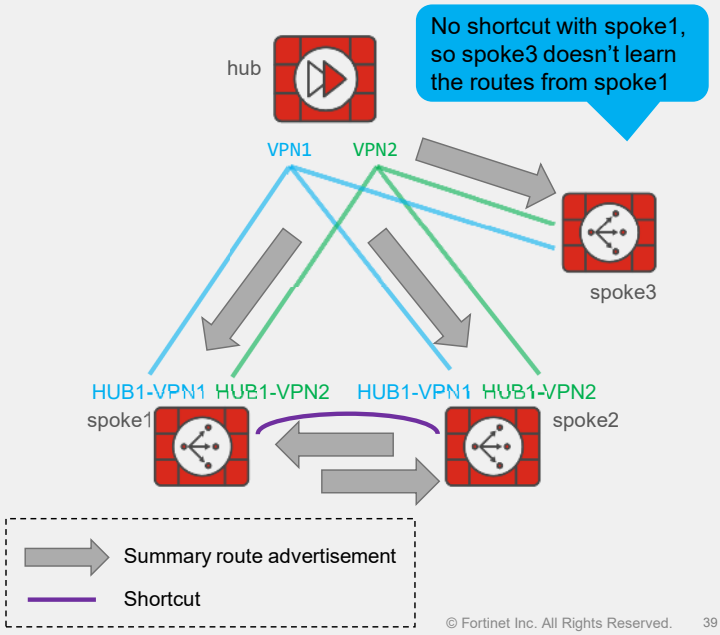


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Dynamic BGP With ADVPN

- Active dynamic BGP neighbor triggered by ADVPN shortcuts
- Spokes establish BGP neighbor relationship with the hub
  - The hub learns the summary route from each spoke
- Spokes establish BGP neighbor relationship only if they establish ADVPN shortcut
  - Each spoke learns routes from its BGP neighbors only
- Compatible with BGP per overlay and BGP on loopback
- Compatible with IPv4 and IPv6




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

Dynamic BGP is an alternative solution that works in conjunction with ADVPN. It involves establishing active dynamic BGP neighbor connections triggered by ADVPN shortcuts. With this method, the spoke FortiGate devices form BGP neighbor relationships with other spokes only after they establish the shortcut tunnel between them. As a result, the spokes learn routes solely from their BGP neighbors—the devices with which they exchange traffic—reducing unnecessary route learning and reducing CPU usage on the hub.

You can configure dynamic BGP on top of a BGP per overlay or BGP on loopback design, and it is compatible with IPv4 and IPv6.

Dynamic BGP removes the requirement for route reflection on the hub. The hub learns only the summary route from each spoke. Initially, each spoke knows the route to the hub and the subnets it can reach through the hub. When a host behind spoke1 tries to connect to a host behind spoke2, spoke1 first reaches the hub based on its routing table. The hub determines that the destination is reachable and initiates the establishment of an ADVPN shortcut tunnel between the two spokes. Then, once the spokes complete the shortcut establishment, they actively initiate a BGP connection to each other over the shortcut, and then they exchange their routing information. On both spokes, BGP will resolve the route to its spoke neighbor through the shortcut, and update the routing table accordingly.

On the example show on this slide, the three spokes advertised their summary route to the hub. Spoke1 established an ADVPN shortcut with spoke2, and then both devices exchanged their routing advertisement. Spoke3 did not exchange traffic directly with spoke1 or spoke3 and therefore did not establish a shortcut with them, nor exchange its routing details with them.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Configure ADVPN With Dynamic BGP

- Hub configuration
  - IPsec
    - Usual settings for ADVPN
    - `set auto-discovery-sender enable`
  - BGP
    - Define `neighbor-group` and `neighbor-range`
    - Disable route reflection globally or for each neighbor group
- Spoke configuration
  - IPsec
    - Usual settings for ADVPN
    - `auto-discovery-receiver enable`
  - BGP
    - Each spoke for a BGP neighbor relationship with the hub
    - Define `neighbor-group` and `neighbor-range`
    - Configure `set passive disable` to ensure that spokes can initiate a dynamic BGP connection

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

To configure ADVPN with dynamic BGP, you must define the following parameters:

- On the hub:
  - At the IPsec phase 1 interface level, define the usual ADVPN settings to enable `auto-discovery-sender` and, if required, to enable `auto-discovery-forwarder`.
  - At the BGP level, define `neighbor-group` and `neighbor-range`. Disable route reflection globally, with the parameter `client-to-client-reflection disable`, or for each involved neighbor group, with the parameter `route-reflector-client disable`.
- On each spoke:
  - At the IPsec phase 1 interface level, define the usual ADVPN setting to enable `auto-discovery-receiver`.
  - At the BGP level, configure neighbor peering with the hub, define `neighbor-group` and `neighbor-range`, and configure `set passive disable` to ensure that spokes can initiate a dynamic BGP connection with the other spokes after the ADVPN tunnel comes up.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN and ADVPN Designs Summary

- This table summarize the feature combinations that you can use for routing with ADVPN

| Hub—Branch routing | BGP per overlay | | | BGP on loopback | | |
|---|---|---|---|---|---|---|
| Branch-Branch ADVPN shortcut routing | BGP next-hop convergence | IPsec phase 2 selectors | Dynamic BGP | BGP next-hop convergence | IPsec phase 2 selectors | Dynamic BGP |
| BGP add-path | Required | No | No | No | No | No |
| Route reflector on hub | Required | No | No | Required | No | No |
| BGP aggregation | Not possible | Yes | Yes | Not possible | Yes | Yes |
| Prefixes redistribution | Yes | No | Yes | Yes | No | Yes |
| VRF-aware overlays | Yes | No | Yes | Yes | No | Yes |
| FortiSASE integration | Yes | No | No | Yes | No | Yes |
| Main advantage | Simplicity | Reduced routing table | Good scalability | Reduced routing table | Reduced routing table | Good scalability |
| Main disadvantage or limitation | Limited scalability | Limited scalability | Introduced with FortiOS 7.4.1 | Limits the hub-side steering (No steering by route tag or BGP with route priority) | | Introduced with FortiOS 7.4.1 |

FORTINET Training Institute

Original design

© Fortinet Inc. All Rights Reserved. 41

The table shown on this slide summarizes the design options available for SD-WAN and ADVPN with FortiOS version 7.4.4. It groups the options available under two main sections that correspond to the two main routing designs available for the overlay network: *BGP per overlay* and *BGP on loopback*.

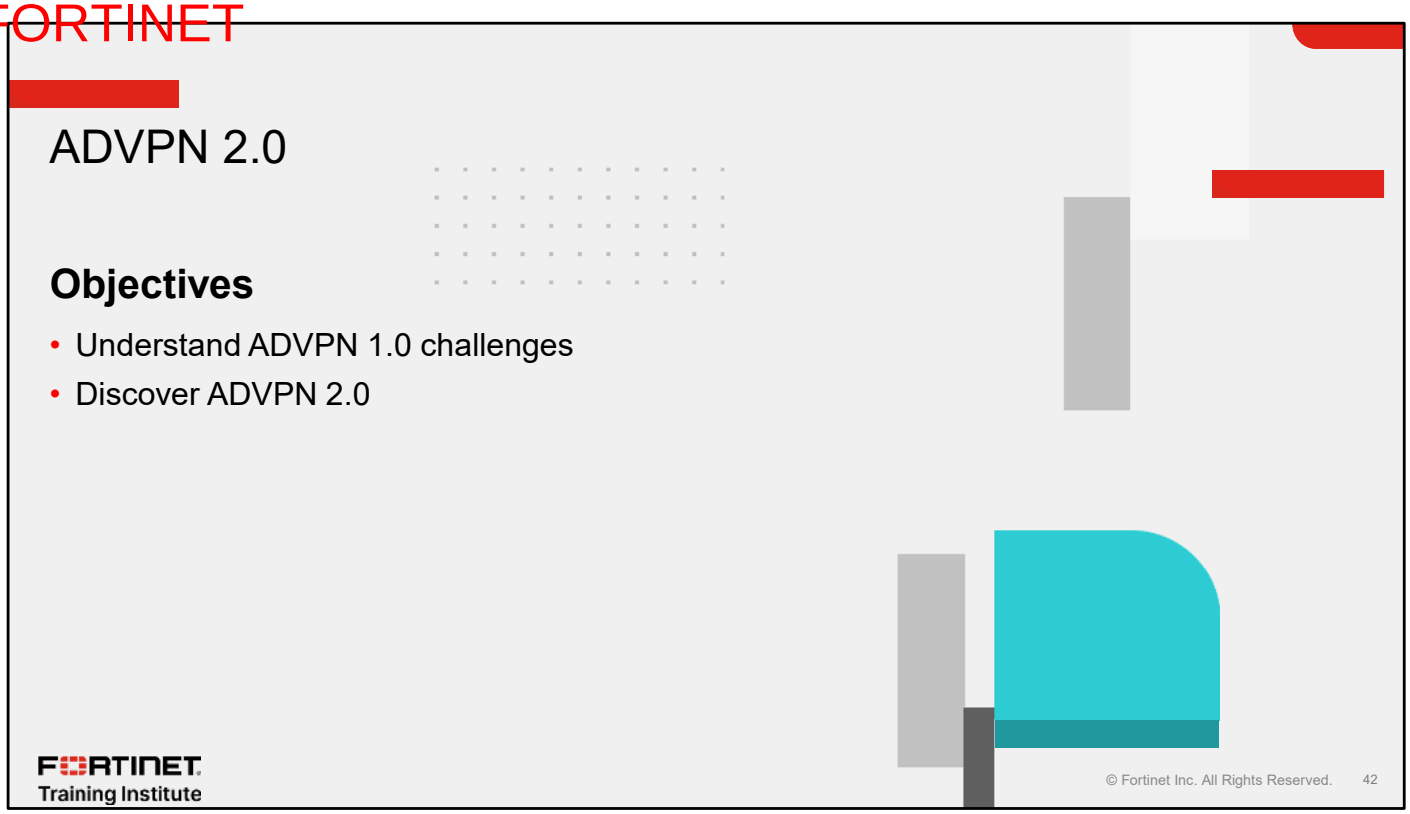
Note that the table presents *IPsec phase 2 selectors* in both sections. This is to highlight elements that administrators should consider when configuring ADVPN with IPsec selector and BGP routing on the overlay. However, remember that IPSec phase2 selectors allows ADVPN with static or OSPF routing on the overlay.

The information shown in the **BGP per overlay** > **BGP next-hop convergence** column, is related to the original ADVPN design. In this design, BGP neighbor relationships are established for each overlay for the branches-to-hub routing, and BGP next-hop convergence is established for routing on the ADVPN shortcuts between the branches. This is the design that you will implement in the lab exercises.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the improvements provided by ADVPN 2.0 and the challenges presented by ADVPN 1.0, you will know the benefits of ADVPN 2.0 and the basis of its configuration.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Why ADVPN 2.0?

- Original ADVPN challenges
  - Shortcuts initiated by the spokes but intensively involve the hub
  - Does not scale well to large networks (thousands of branches)
  - Tied to specific BGP routing designs or IPsec mechanisms
    - BGP route reflection and BGP next-hop recursive resolution
    - IPsec phase2 selectors
    - BGP per overlay or BGP on loopback
- Need for
  - Increased flexibility
  - Scalability for very large networks
  - Improved resiliency on ADVPN shortcut failure
  - Improved reaction to shortcut performance degradation

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

In this lesson, you learned about the challenges of using ADVPN 1.0 in large networks with thousands of branches. ADVPN 1.0 relies on BGP routing and the route reflection to inform every spoke device about possible route through the network, to allow ADVPN shortcut establishment and SD-WAN traffic steering. Because of this, the performances of ADVPN 1.0 designs degrades when it comes to working with large networks.

Fortinet improved ADVPN, and released a new version—ADVPN 2.0—which it introduced with FortiOS 7.4.2. You will learn more about ADVPN 2.0 in the remainder of this lesson.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# ADVPN 2.0 Objectives

- Natively designed for SD-WAN
- Support very large topologies, with hundreds of spokes
- Limit hub involvement
  - Edge discovery and path management from the spoke
- Improve underlay selection for tunnel establishment
  - Select underlays available on both spokes
  - Consider link performances from both spokes
- Improve resiliency against underlay outage or degraded performances
  - Native link selection
  - No dependance on specific BGP routing design

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

ADVPN 2.0 is a new, proprietary framework specially designed for SD-WAN and natively integrated with SD-WAN.

The SD-WAN with ADVPN solution has evolved to version 2.0 with major changes to the ADVPN design and operation. Designed with the objective of limiting the load and dependency on the hub, it moves tasks previously done on the hub, to the spokes. Edge discovery and path management are now done on ADVPN spokes.

ADVPN 2.0 incorporates intelligence into the spokes, to ensure shortcut tunnels (also known as shortcuts), are established using underlays available on both spokes, and chosen based on matching certain link health criteria. Previously, FortiGate considered the link health criteria on only the spoke initiating the shortcut.

Additionally, ADVPN 2.0 provides a more flexible SD-WAN solution than ADVPN 1.0. This solution provides resiliency against underlay outages or degraded underlay performance because it no longer depends on specific BGP routing designs or mechanisms, including route reflection, BGP next-hop recursive resolution, BGP per overlay, and BGP on loopback.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

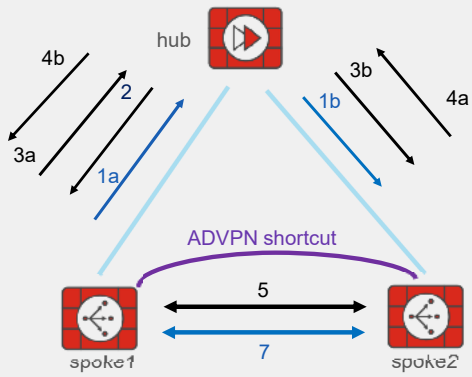
# ADVPN—Traffic Triggered Shortcut Establishment

- Identical sequence of events for ADVPN 2.0 and previous version of ADVPN

1. Traffic is forwarded through the hub (IPsec)
2. The hub sends a `shortcut-offer` to Branch1
3. Branch1 replies with a `shortcut-query`
   - The hub forwards the `shortcut-query`
4. Branch2 replies with `shortcut-reply`
   - The hub forwards the `shortcut-reply`
5. Shortcut establishment between both spokes
   - IPsec tunnel negotiation
6. Routing convergence

   According to the option selected:
   - BGP next-hop convergence
   - IPsec selector
   - Dynamic BGP
7. Traffic flow through the shortcut

Data plane
Control plane




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 45

The sequence of events to initiate the first shortcut between two spokes is identical with ADVPN 1.0 and ADVPN 2.0.

When a spoke, spoke1, receives traffic flow that must go through a second spoke, spoke2, it first sends the traffic through the hub. The hub forwards the traffic to spoke2 and starts the process of establishing a shortcut, as shown on this slide.

With ADVPN 2.0, the process remains similar when spoke1 establishes its *first* shortcut with spoke2. The difference comes when spoke1 needs to establish a new shortcut with spoke2, either because the performance of a link degrades or because and interface fails.

Note that ADVPN 2.0 supports only IPv4, while ADVPN 1.0 supports IPv4, as well as IPv6.

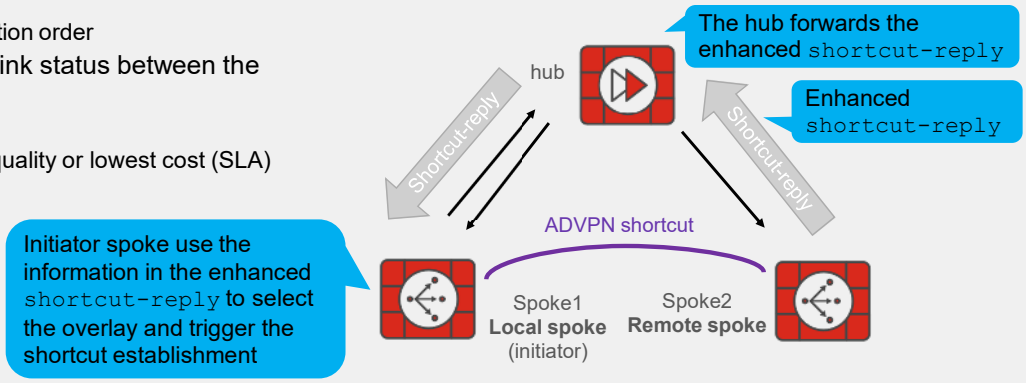


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Edge Discovery and Path Management

- Edge discovery
  - Expanded IKE shortcut-reply message
  - Initiator spoke learns the following WAN link information from the remote spoke:
    - IP address
    - Transport group
    - Link quality
    - Link cost
    - Member configuration order
  - Periodical update of link status between the two spokes
    - Every 5 seconds
    - For strategy best quality or lowest cost (SLA)
- Path management
  - Performed by the initiator spoke
  - It calculates the best shortcut path per SD-WAN service or rule
  - It advises the IKE process to establish a shortcut using the selected path




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 46

This slides presents the main new features introduced with ADVPN 2.0: edge discovery and path management.

Edge discovery expands the IKE shortcut-reply message to allow the local spoke (spoke where user traffic is initiated) to obtain the remote spoke (destination spoke for user traffic) WAN link information, which includes IP address, transport group, link quality, link cost, and member configuration order.

With the path management feature, the local spoke handles the remote spoke WAN link information, calculates the best shortcut path per SD-WAN service or rule, and then advises IKE to establish a shortcut using the selected path.

After the shortcut is established, the spoke devices can exchange their WAN link information (members transport group, link quality, and so on) every 5 seconds through the shortcut. They use UDP traffic to exchange this information, make sure to enable such traffic flow. The exchange of WAN link information is not configurable, it is done automatically for shortcuts associated with best quality or lowest cost (SLA) rules.

The path management function on the local spoke runs in the background. It monitors the WAN link information available for the local and the remote overlays and calculates the best shortcut path accordingly. If required, it advises IKE to establish a new shortcut between the spokes.

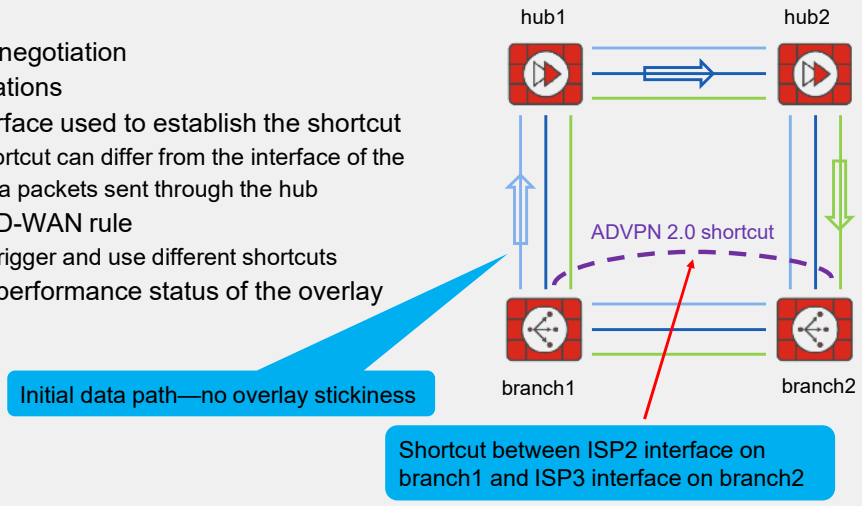


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Shortcut Endpoints Selection

- ADVPN 1.0
  - The path taken by the initial data, traffic flowing through the hub, determines the shortcut endpoints
    - ADVPN local and remote endpoints use the same interfaces as the original flow
- ADVPN 2.0
  - SD-WAN controls the shortcut negotiation
  - Spokes initiate shortcut negotiations
  - The spoke determines the interface used to establish the shortcut
    - The interface used for the shortcut can differ from the interface of the overlay used for the initial data packets sent through the hub
  - Shortcuts can differ for each SD-WAN rule
    - Different SD-WAN rules can trigger and use different shortcuts
  - The spoke can reevaluate the performance status of the overlay and negotiate a new shortcut




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 47

With ADVPN 1.0, the path taken by the initial data, traffic flowing through the hub, determines the shortcut endpoints. ADVPN local and remote endpoints use the same interfaces as the original flow. For this reason, you learned how to configure overlay stickiness policy routes to avoid cross overlay shortcuts and, possibly, physically impossible connections.

With ADVPN 2.0, the initial data needs to find only *a path* between the two spokes. This initial path selection has no influence on the interface that the local branch selects to establish the shortcut. The local branch selects which interface it establishes the shortcut with, based on link performance information and the information it received from the remote spoke.

With ADVPN 2.0, overlay stickiness is no longer relevant. However, the administrator can configure each link with a transport group ID to differentiate between compatible and incompatible interfaces.



Vouchers & Dumps are Available | WhatsApp +201224560923

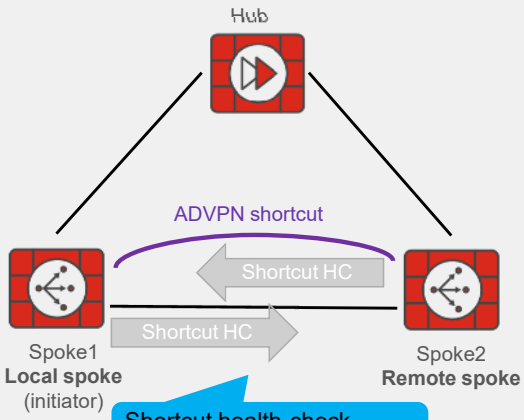
DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Health Check Through Shortcuts

- Spokes exchange health-check information through the shortcuts
  - UDP packets, port 4684
  - Contains, for all members of the branch:
    - Link status
    - Link quality
    - Transport groups of members
  - Allows shortcut reevaluation if performances degrades

```
branch1-fgt# diag sniffer packet any 'udp port 4684' 4 0
vpn1_0 out 10.200.1.2.4684 -> 10.200.1.1.4684: udp 348
vpn1_0 in 10.200.1.1.4684 -> 10.200.1.2.4684: udp 348
vpn1_0 out 10.200.1.2.4684 -> 10.200.1.1.4684: udp 348
vpn1_0 in 10.200.1.1.4684 -> 10.200.1.2.4684: udp 348
vpn1_0 out 10.200.1.2.4684 -> 10.200.1.1.4684: udp 348
```

Example of health-check traffic on a spoke over the shortcut tunnel `vpn1_0`




Shortcut health-check exchanged every 5 seconds

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 48

After the shortcut is established, when the SD-WAN rule that triggered the shortcut has for strategy best quality or lowest cost (SLA), the spoke devices exchange their WAN link information (members transport group, link quality, and status) through the shortcut. They use UDP traffic on port 4684 to exchange this information. Make sure to enable those flows on each spoke devices and on any intermediate devices.

The exchange of WAN link information is not configurable. It is done automatically, every 5 seconds, for shortcuts associated with best quality or lowest cost (SLA) rules.

The example on this slide shows a sniffer output filtered to show the health-check packets sent and received by a spoke device, branch1_fgt, after it established the shortcut vpn1_0.

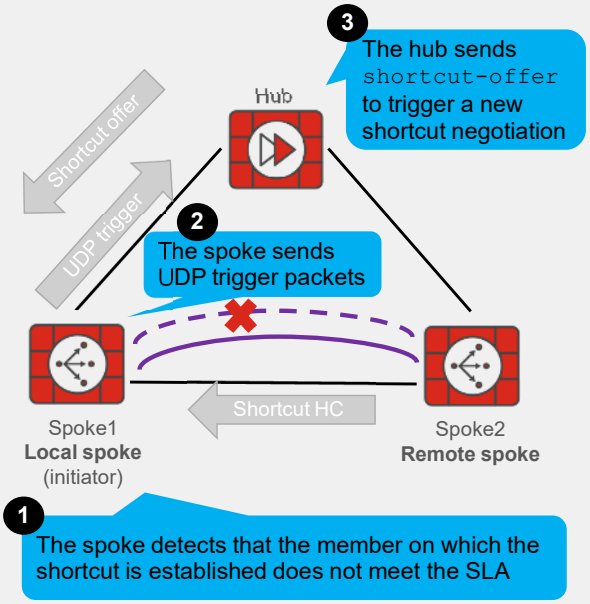


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Negotiating a New Shortcut—UDP Trigger Packets

- What happens when an SLA change invalidates the current shortcut?
  - The branches need to negotiate a new shortcut
  - The new shortcut negotiation requires exchanging shortcut messages via the hub
    - Shortcut offer, reply, and query
- The hub initiates a shortcut offer on reception of:
  - Data traffic: initial shortcut negotiation
  - ADVPN control packets
    - UDP trigger packets
    - Sent by the spoke to the hub to trigger a new shortcut negotiation
    - UDP port 4684




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 49

A spoke can detect that a member used to establish the shortcut does not meet the SLA requirements. It can detect that for its own members, or for the remote spoke members through the shortcut health checks. When a spoke detects a situation like this, it triggers the establishment of a new shortcut. To do so, with FortiOS 7.4, it requires the assistance of the hub.

The sequence of actions is as follows:

- First, the spoke detects that SLA changes invalidate the current shortcut.
- Then, the spoke sends ADVPN control packets, also called UDP trigger packets, to the hub.
- Lastly, the hub sends shortcut-offer packets to trigger the negotiation of a new shortcut between the two spokes.

Note that the spoke sends the ADVPN control packets, to trigger a new shortcut negotiation, on UDP port 4684. It uses its loopback IP address as a source and sends the packet to the hub loopback IP address. Make sure that you enable this type of traffic on the hub and on the spokes.



Vouchers & Dumps are Available | WhatsApp +201224560923

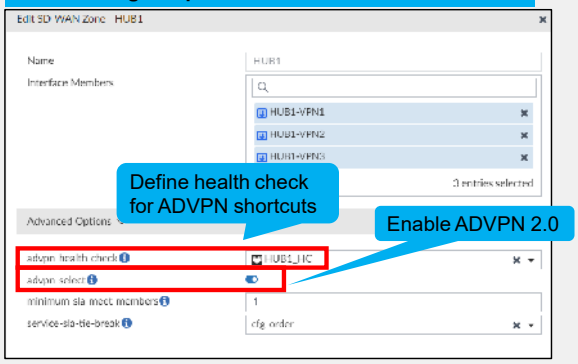
DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Configure ADVPN 2.0

- Two parts
  - IPSec
    - Similar to original ADVPN configuration
    - Main commands:
      - `auto-discovery-receiver`
      - `auto-discovery-sender`
      - `auto-discovery-forwarder`
  - SD-WAN
    - Configured on every spoke
    - Enable at SD-WAN zone level
      - `set advpn-select enable`
    - Define a transport group for each participating member
      - ADVPN can negotiate shortcuts only between members within the same transport group
- Backward compatibility
  - ADVPN 2.0 branches can establish shortcuts with ADVPN 1.0 branches

- Configuration with FortiManager

**Provisioning Templates > SD-WAN > SD-WAN Zones**




**SD-WAN > SD-WAN Member > Advanced Options**




Define group ID between 0-255 (default 0)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 50

You configure ADVPN 2.0 in two parts. First, within the IPsec phase1 configuration, you enable the parameter `auto-discovery-receiver` on the spokes, and the parameters `auto-discovery-sender` and `auto-discovery-forwarder` on the hub, like you do for ADVPN 1.0.

Then, in the SD-WAN section, you enable ADVPN 2.0 by enabling `advpn-select` at the SD-WAN zone level. Still at the SD-WAN zone level, you define the performance SLA that the spokes use to monitor shortcut performance. Optionally, you define a transport group for each SD-WAN member. By default, each member is transport group zero and the spokes can establish shortcuts between all of them. Use different transport group numbers to differentiate between members that are compatible for shortcuts, such as ISP interfaces, and members that are not compatible, such as MPLS interfaces.

You can configure those parameters on the FortiGate CLI, or for devices managed by FortiManager, in the SD-WAN template shown on this slide.

Note the backward compatibility. Branches configured with ADVPN 1.0 can establish shortcuts with branches configured with ADVPN 2.0. If it receives a shortcut-reply message that doesn't include WAN link details, a spoke configured for ADVPN 2.0 reverts to the original method of establishing shortcuts. This affects the connection to this remote spoke only and not to the full topology.

The hub configuration remains similar. You don't need to configure specific parameters to use ADVPN 2.0.



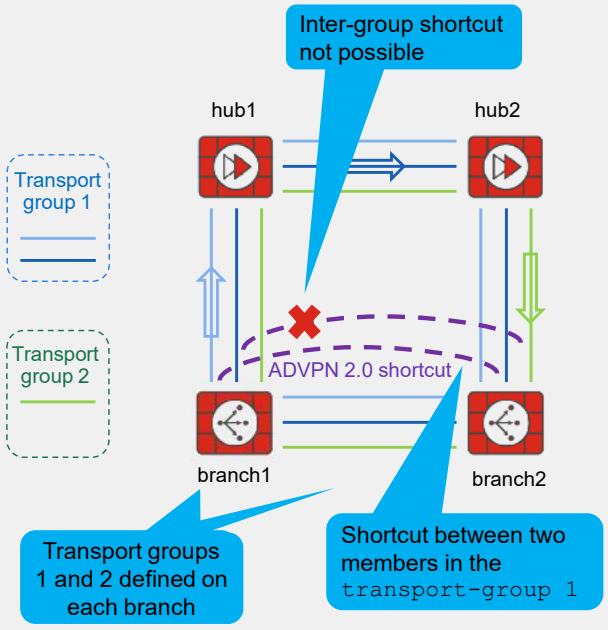
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Transport Groups

- How do you differentiate interfaces compatible for shortcuts from other interfaces?
  - Define transport groups

```
config members
     edit 1
       set interface "T1"
       set zone "overlay"
       set transport-group 1
     next
     edit 2
       set interface "T2"
       set zone "overlay"
       set transport-group 1
     next
     edit 3
       set interface "T3"
       set zone "overlay"
       set transport-group 2
     next
```




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 51

With ADVPN 2.0, the initial data needs to find only *a path* between the two spokes. This initial path selection has no influence on the interface that the local branch selects to establish the shortcut. However, there might be situation where the branch devices have interfaces that are not compatible to establish shortcuts. A common example of such incompatible interfaces are ISP interfaces and MPLS interfaces.

When the branches have interfaces that are not compatible to establish shortcuts, the administrator must define transport groups to identify the compatible interfaces. In the example shown on this slide, the administrator defines transport group 1 to the interfaces T1 and T2, and transport group 2 to the interface T3. This instructs the spoke FortiGate device to build shortcuts only between members of the same transport group.



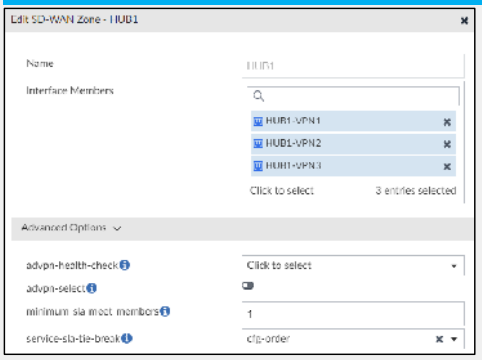
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

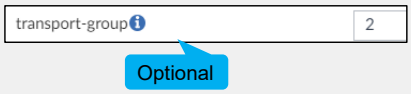
# SD-WAN Overlay Template and ADVPN 2.0

- ADVPN option on the SD-WAN overlay template that configures ADVPN 1.0
- To adjust the configuration for ADVPN 2.0
  - Edit the SD-WAN template
    - Update advanced options for the zones
      - **advpn-health-check**
      - **advpn-select**
    - Optional
      - Define a health-check that is specific to the shortcuts
      - Define transport groups for the members
  - IPsec templates
    - No changes required
  - BGP templates
    - Remove route reflection parameters (no longer mandatory)
  - Policy routes
    - Remove overlay stickiness configuration (optional)

**Provisioning Templates > SD-WAN > SD-WAN Zones**




**SD-WAN > SD-WAN Member > Advanced Options**




Optional

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 52

With the FortiManager SD-WAN overlay template, you can configure ADVPN 1.0 only. However, if you want to keep the routing topology with BGP per overlay and convert the ADVPN 1.0 configurations to allow ADVPN 2.0, the changes required are minimal.

On the SD-WAN template, you must edit the zone configuration and, in the **Advanced Options** section, enable **advpn-select**. To select the health check used for the shortcuts, use the parameter **advpn-health-check**. Optionally, if your topology requires it, you can define a dedicated health check for the shortcuts and transport groups to identify SD-WAN members compatible to establish shortcuts.

There are no mandatory changes that you must perform on the IPsec templates or on the routing side. However, you can remove the policy route configured for the overlay stickiness and remove the route reflection parameters from the BGP configuration, as they are no longer required.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Monitor Remote Spoke WAN Link Information

- Diagnostic command available on the local spoke to view the remote spoke WAN link details received: `diagnose sys sdwan advpn-session`

```
branch1_fgt # diag sys sdwan advpn-session
Session head branch2_fgt-0-HUB1:1)
(1) Service_ID(3), last_access(4136110), remote_health_check_info(3)
Selected path: local(HUB1-VPN1, port1) gw: 192.2.0.1  remote IP: 203.0.113.1(192.168.1.2)
Remote information:
1: latency: 1.833133 jitter: 0.482600 pktloss: 0.000000 mos: 4.403007          0x1 cost: 0 remote
gw: HUB1-VPN1 transport_group: 1 bandwidth up: 10239 down: 10239
ipv4: 203.0.113.1(192.168.1.2) ipv6 ::1bc2(20e6:7e0c:fe7f:0:1c:25
2: latency: 1.725933 jitter: 0.469833 pktloss: 0.000000 mos: 4.403073 sla: 0x1 cost: 0 remote
gw: HUB1-VPN2 transport_group: 1 bandwidth up: 10239 down: 10239 bidirection: 20478
ipv4: 203.0.113.9(192.168.1.66) ipv6
6465:7228:3229:2c20:6c6f:6361:6c20:636f(7374:2830:292c:2073:656c:6563:7465:6400)
3: latency: 1.240333 jitter: 0.269700 pktloss: 0.000000 mos: 4.403513 sla: 0x1 cost: 0 remote
gw: HUB1-VPN3 transport_group: 0 bandwidth up: 9999999 down: 9999999 bidirection: 19999998
ipv4: 172.16.0.9(192.168.1.130) ipv6 ::(::)
```

Remote spoke device name and name of the remote zone

Path selected for the shortcut

Link performance details received from the remote spoke, updated every 5 seconds

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 53

You can use the command `diagnose sys sdwan advpn-session` to view the WAN link information that the local spoke received from the remote spoke, as shown on this slide.

FortiGate refreshes the link performance details every 5 seconds with information received from its remote peer.

Note that this command provides no results for shortcuts that do not require SLA monitoring. FortiGate displays the output only for shortcuts associated with best quality or lowest cost (SLA) rules.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# What About Routing?

- Routing designs compatible with ADVPN before ADVPN 2.0
  - Limited set of options described in the previous slide
  - Heavy reliance on BGP routing
    - BGP on overlay with route reflection and next-hop convergence
    - BGP on loopback with route reflection on the hub
    - Dynamic BGP routing (FortiOS 7.4.1 and above)
- With ADVPN 2.0, routing provides only reachability information
  - Additional flexibility for the routing design and BGP option used
  - Easier use of BGP route summarization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 54

Historically, ADVPN was exclusively deployed with the BGP routing protocol on the overlay. For small to mid-size topologies, the most common design remains BGP on overlay with route reflection and next-hop convergence. For large deployments, administrators can select from the various options presented in this lesson, such as BGP on loopback or dynamic BGP.

With ADVPN 2.0, the routing between devices and between hub and spokes is required to provide only reachability information. The spoke devices build a dynamic BGP peering through the shortcut.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Review

- ✓ Describe ADVPN operation and configuration, and its support in SD-WAN
- ✓ Configure the network ID to allow multiple overlays between the same pair of gateways
- ✓ Discover alternative overlay and routing designs for ADVPN
- ✓ Understand BGP on loopback design
- ✓ Discover ADVPN without BGP route reflection
- ✓ Understand dynamic BGP
- ✓ Discover ADVPN 2.0

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 55

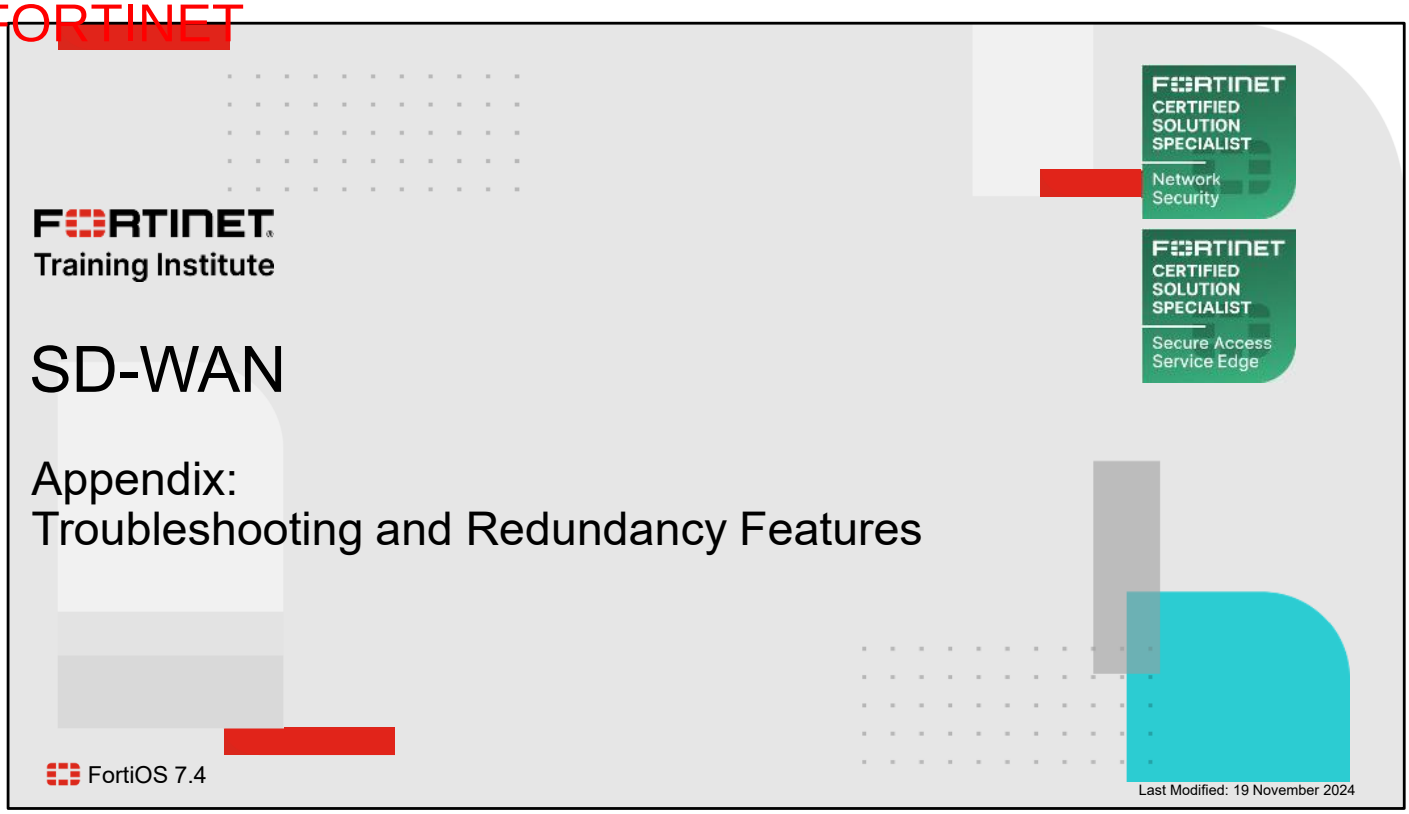
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to set up SD-WAN and ADVPN on a basic hub-and-spoke topology. You also discovered alternative overlay and routing designs suitable for ADVPN and what ADVPN 2.0 offers.



Vouchers & Dumps are Available | WhatsApp +201224560923

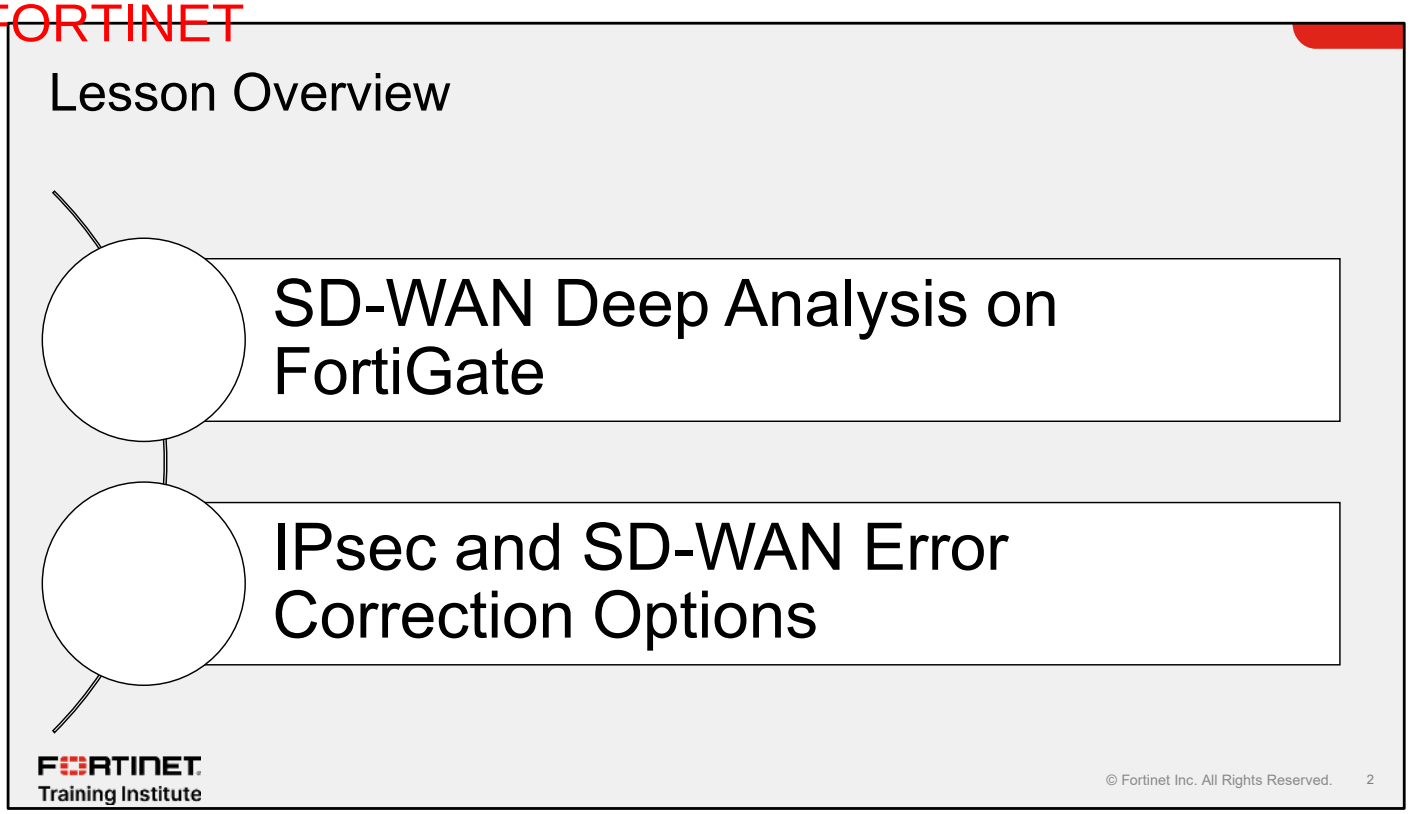
DO NOT REPRINT
© FORTINET
Brave-dumps.com




This appendix is divided into two parts. The first part summarizes the troubleshooting commands related to SD-WAN or specific to SD-WAN that you discovered through the lessons. The second part presents redundancy features that you can use with IPsec and SD-WAN topologies.


Vouchers & Dumps are Available | WhatsApp +201224560923

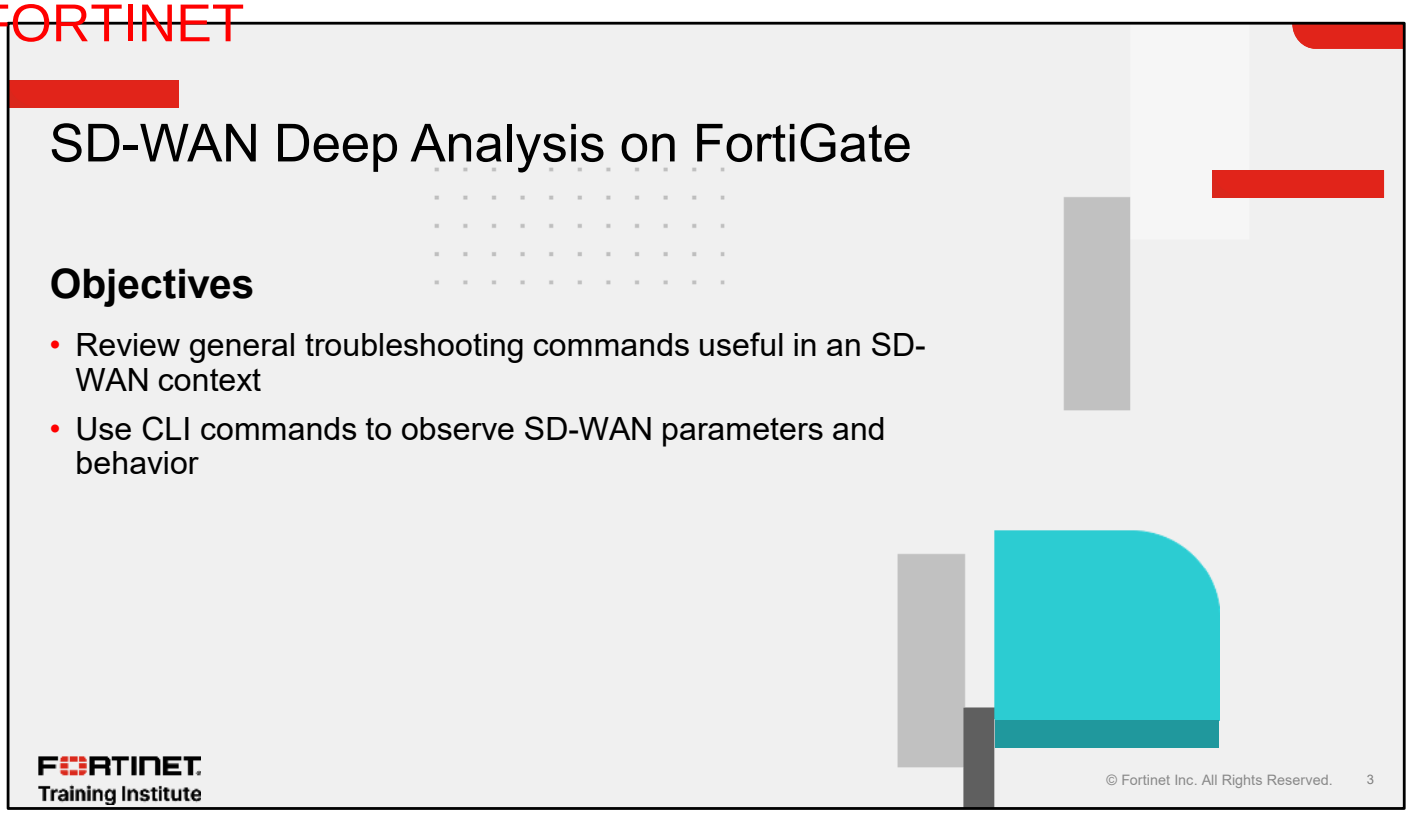
DO NOT REPRINT
© FORTINET
Brave-dumps.com




In this appendix, you will learn about the topics shown on this slide.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide. By demonstrating a competent understanding of FortiGate troubleshooting commands, you will be able to analyze and troubleshoot SD-WAN deployments.

This section summarizes the troubleshooting commands specific to SD-WAN that you learned about through this course. It also covers some general troubleshooting commands that you commonly use in an SD-WAN context.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## General-Purpose Troubleshooting Commands

- General-purpose troubleshooting and monitoring commands useful in an SD-WAN context
  - Collect traffic received and sent by the FortiGate device
    - `diagnose sniffer packet`
  - View how FortiGate handles a packet and decision taken
    - `diagnose debug flow`
  - Display established sessions
    - `get system session list`
    - `diagnose system session list`
  - Route lookup commands
    - `diagnose firewall proute list`
    - `get router info routing-table all`
    - `get router info routing-table database`
    - `get router info kernel`
    - `get router info bgp network`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

When troubleshooting SD-WAN on FortiGate, you can continue to use the general-purpose troubleshooting commands.

The main commands used in an SD-WAN context are:
- `diagnose sniffer packet`, to collect PCAP traces of traffic through FortiGate
- `diagnose debug flow`, for a detailed view of how FortiGate analyzes a packet and makes forwarding decisions
- `get system session list` and `diagnose sys session list`, to get a list of, and details about, established sessions
- Routing-related commands, and especially `diagnose firewall proute list`

On the next few slides, you will see SD-WAN-specific fields available for those commands.

Note that this appendix doesn't present the general principles and detailed usage for those commands. You can refer to the troubleshooting section of the *FortiGate Administration Guide* for additional details about commands usage.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Sniffer Capture

- Sniffer on the FortiGate CLI
  - Interface *any* or a specified interface (no zone)
  - Use trace level 4 to identify the outgoing interface selected
  - Disable traffic offloading to collect sniffer trace (when applicable)

Select any as interface to detect outgoing interface member

Filter on host, protocol,…

Trace level 4 to display header of packets with interface name

```
# diagnose sniffer packet any "host 10.0.2.101 and icmp" 4
2024-11-06 14:10:36.360797 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-11-06 14:10:36.386674 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-11-06 14:10:37.406708 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-11-06 14:10:37.406789 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-11-06 14:10:37.408639 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-11-06 14:10:37.408669 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-11-06 14:10:38.407970 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

In an SD-WAN deployment, you can collect a sniffer trace on the FortiGate CLI to examine the traffic flowing through the FortiGate device. If you collect a sniffer trace to determine the outgoing interface selected for a particular traffic flow, you will use the following settings:

- Trace level 4 to display the interface name, but only the header of the packet—for better readability
- Interface *any* to collect data on all possible outgoing interfaces
- Traffic filter to limit the capture to the flow you want to analyze

Remember that for FortiGate with NP2, NP4, or NP6 interfaces that are offloading traffic, you must disable offloading at the policy level before you collect a sniffer trace, otherwise the PCAP process cannot collect the traffic.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Debug Flow

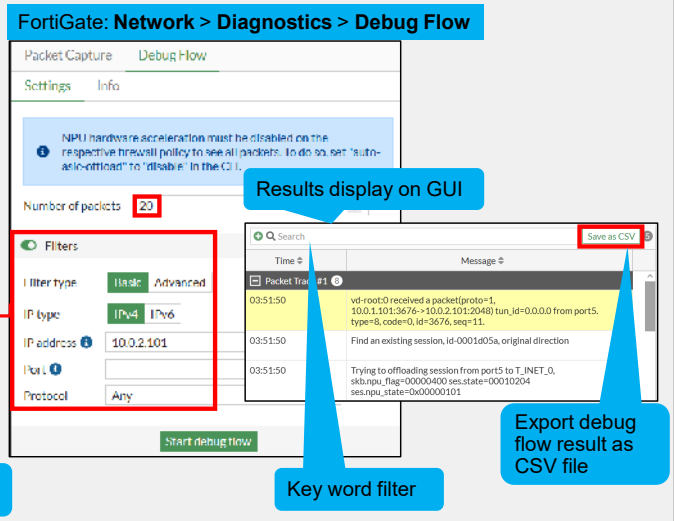
- Debug flow with CLI commands

```
# diagnose debug enable
# diagnose debug flow filter addr 10.0.2.101
# diagnose debug flow trace start 20
id=20085 trace_id=3 func=print_pkt_detail line=5783
msg="vd-root:0 received a packet(proto=1,
10.0.1.101:8605->10.0.2.101:2048) from port5. type=8,
code=0, id=8605, seq=1."
id=20085 trace_id=3 func=init_ip_session_common
line=5955 msg="allocate a new session-00000209"
id=20085 trace_id=3 func=rpdb_srv_match_input line=1030
msg="Match policy routing id=1: to 10.0.2.101 via
ifindex-21"
id=20085 trace_id=3 func=vf_ip_route_input_common
line=2605 msg="find a route: flag=04000000 gw-
172.16.1.5 via HUB1-VPN3"
id=20085 trace_id=3 func=fw_forward_handler line=869
msg="Allowed by Policy-2:"
id=20085 trace_id=3 func=ipsecdev_hard_start_xmit
line=625 msg="enter IPSec interface HUB1-VPN3"
...
```

Number of entries to capture

Set filters to limit the capture

- Debug flow on GUI




Training Institute

© Fortinet Inc. All Rights Reserved. 6

The debug flow indicates, in detail, how packets are handled by the FortiGate device. You can collect the data with CLI commands, or from the GUI as shown on this slide.

When debug flow is collected from the GUI, you can filter entries using key words and export the output as a CSV file.

On the CLI, you can use the command `diagnose debug flow filter ?` to list available filter criteria, and the command `diagnose debug flow filter` to review the filters in place.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Session List

- CLI commands
  - diag sys session filter
  - diag sys session list
  - diag sys session6 list
- SD-WAN information for the session
  - sdwan_mbr_seq
  - sdwan_service_id
  - None if traffic matches default SD-WAN rule
  - None if not an SD-WAN session

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=5
expire=3596 timeout=3600 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper= [...]
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 f02 app valid
statistic(bytes/packets/allow_err): org=3427/20/1
reply=4749/23/1 tuples=2
tx speed(Bps/kbps): 638/5 rx speed(Bps/kbps): 884/7
orgin->sink: org pre->post, reply pre->post dev=7-
>20/20->7 gwy=100.64.1.9/10.0.1.101
hook=pre dir=org act=noop 10.0.1.101:43020-
>10.1.0.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.7:22-
>10.0.1.101:43020(0.0.0.0:0)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=000b2f2d tos=ff/ff app_list=2002 app=16060
url_cat=0
sdwan_mbr_seq=4 sdwan_service_id=2
rpdb_link_id=ff000002 ngfwid=n/a
npu_state=0x001008
```

Firewall policy ID

Member and rule IDs

App ID (SSH)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

The CLI command `diagnose sys session filter` allows you to filter the sessions to display. Then, use the command `diagnose sys session list` to display the session detail.

You can use `diagnose sys session filter?` to view available filters, `diagnose sys session filter` to see active filters, and `diagnose sys session filter clear` to reset the filter settings. Use the command `diagnose sys session list` for IPv4 traffic, and `diagnose sys session6 list` for IPv6 traffic.

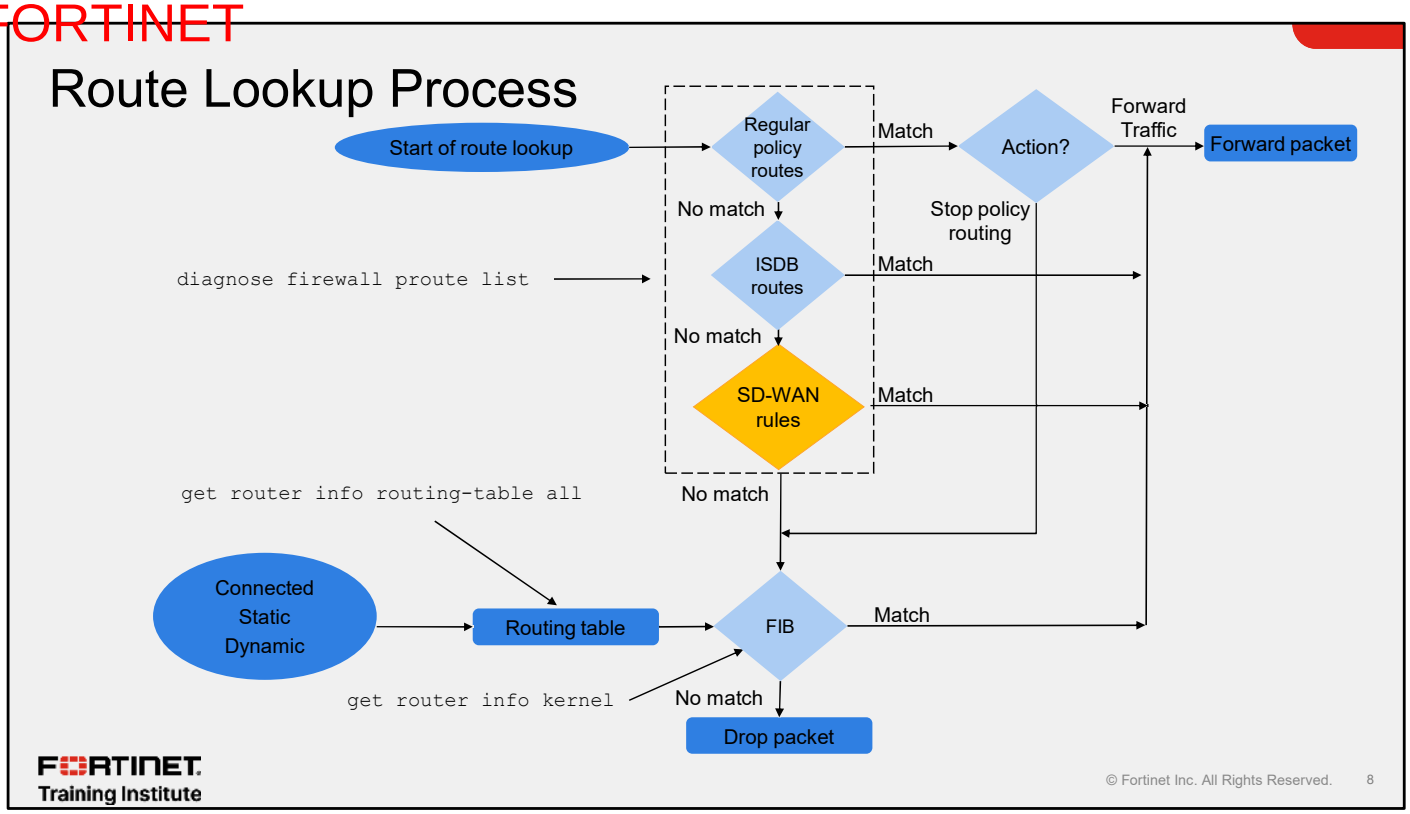
The right side of this slide shows an example output with detailed information about the session table entry. Note that the example does not show the traffic shaping information.

From left to right, and from top to bottom, the following information is highlighted:

- The IP protocol number and the protocol state
- The length of time until the session expires (if no more traffic matches the session)
- Session flags
- Received and transmitted packet and byte counters
- The original and reply direction of the traffic. If the device is doing NAT, this portion shows the type of NAT (source or destination) for each traffic direction, and the NAT IP address.
- The ID of the matching policy
- The SD-WAN-specific session information. `sdwan_mbr_seq` and `sdwan_service_id` indicate the SD-WAN member ID and the SD-WAN rule ID in use, respectively. If the session matched the SD-WAN implicit rule, and therefore was handled using standard FIB routing, those SD-WAN fields would not appear.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




You already discovered the flowchart on this slide in the routing and session lesson. You can use it to review the commands available to consult routing information on the FortiGate devices.

Note that the command `diagnose firewall proute list` displays all policy routes. You can determine the type of route by looking at the route ID.

A regular policy route has an ID between 1 and 65535. ISDB routes and routes derived from SD-WAN rules have an ID above 65535. You will see the SD-WAN service ID field only for SD-WAN rules (field `vwl_service`).


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Route Lookup Commands

- SD-WAN fields in proute list

```
# diagnose firewall proute list
list route policy info(vf=root):

id=2131034113(0x7f050001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc despite_flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(2) oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836842,0,0,0,0, 16354) Microsoft.Office.365.Portal(4294837313,0,0,0,0,
41468) Salesforce(4294837785,0,0,0,0, 16920)
hit_count=34219 last_used=2024-11-06 04:04:15

id=2131034115(0x7f050003) vwl_service=3(Corp) vwl_mbr_seq=3 4 5 dscp_tag=0xfc last_used_flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=19(HUB1-VPN1) oif=20(HUB1-VPN2)
oif=21(HUB1-VPN3)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=13 last_used=2024-11-06 11:31:42
```

SD-WAN rule ID and rule name

SD-WAN members by order of preference

Outgoing interface by order of preference

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

This slide shows an example of a policy route list output.

Note the fields `vwl_service` and `vwl_mbr`, which indicate the SD-WAN rule that allowed the route creation and the SD-WAN member used to steer the traffic.

The ID displayed in the `diagnose firewall proute list` command output corresponds to the ID displayed in the debug flow output when a packet matches a rule. The output also includes the outgoing interface list, with the interface preference sorted from left to right.

For troubleshooting purposes, the output of the `diagnose firewall proute list` command also displays the rule hit count and the last time the rule was hit.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Review Duplicate Routes

- Routing table database shows all duplicate routes received on a device

```
# get router info routing-table database
...
B     *> 10.0.1.0/24 [200/0] via 192.168.1.1 (recursive is directly connected, HUB1-VPN1), 01:05:02
      *>             [200/0] via 192.168.1.65 (recursive is directly connected, HUB1-VPN2), 01:05:02
      *>             [200/0] via 192.168.1.1 (recursive is directly connected, HUB1-VPN1), 01:05:02
      *>             [200/0] via 192.168.1.65 (recursive is directly connected, HUB1-VPN2), 01:05:02
```

- Duplicate routes are consolidated in the routing table

```
# get router info routing-table all
...
B       10.0.1.0/24 [200/0] via 192.168.1.1 [2] (recursive is directly connected, HUB1-VPN1), 01:03:45
                    [200/0] via 192.168.1.1 [2] (recursive is directly connected, HUB1-VPN2), 01:03:45
```

Number of duplicate routes available

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

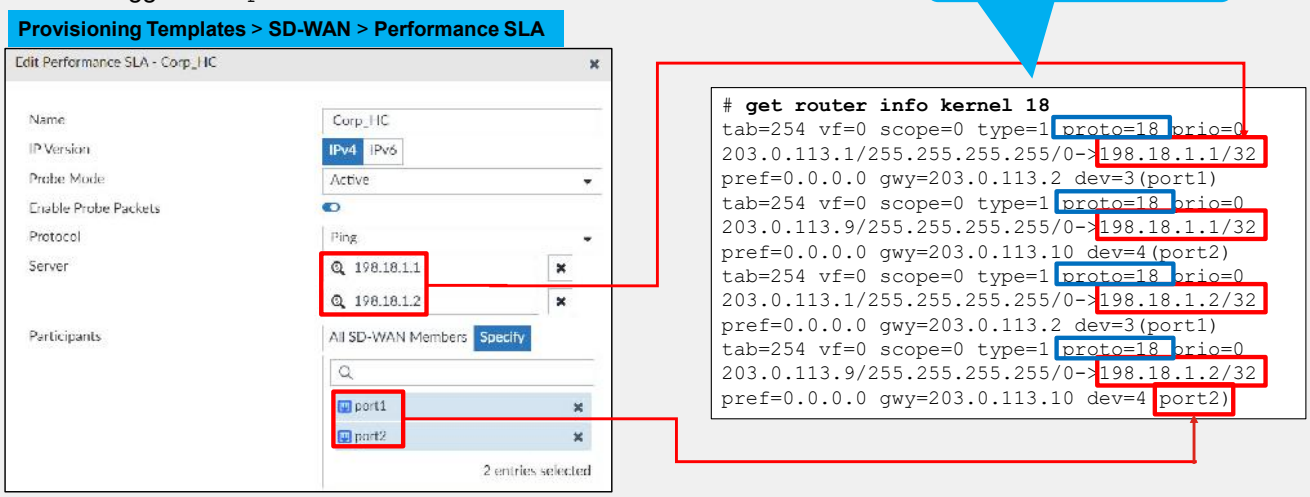
The routing table database shows all duplicate routes received. On the routing table, for easier readability, FortiOS consolidates the duplicate routes and indicates the number of duplicate routes available. Note that the duplicate routes are not filtered. They are consolidated only for cosmetic purposes.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Member Probe Routes

- FortiGate adds entries in FIB for probes
  - Flagged with `proto=18`




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

When you use active monitoring for measuring the performance of members, FortiGate doesn't use the entries in the routing table to route the probes. Instead, FortiGate adds a FIB route entry for the configured target servers through each monitoring member and its gateway. These kernel routes are flagged as `proto=18`, as shown on this slide.

Note that `proto=18` has nothing to do with assigned internet protocol numbers. It is an arbitrary protocol number assigned by Fortinet to identify entries in the FIB used for routing health-check traffic.

You can use the command `get router info kernel 18` to filter the kernel table route and display only the proto 18 routes. It is equivalent to the command `get router info kernel | grep proto=18`.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## SD-WAN-Specific Commands

- Review SD-WAN overall settings
  - `get sys sdwan`
- Display SD-WAN members and zones configuration and status
  - `diagnose sys sdwan member`
  - `diagnose sys sdwan zone`
- Review health-check and link monitor status
  - `diagnose sys sdwan health-check status`
  - `diagnose sys link-monitor interface <interface_name>`
  - `diagnose sys link-monitor-passive admin list`
- Review rules status
  - `diagnose sys sdwan service4`
  - `diagnose sys sdwan internet-service-app-ctrl-list`
- SLA logging
  - Activate: `sla-fail-log-period, sla-pass-log-period`
  - View performance SLA link status: `diagnose sys sdwan sla-log`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

This slide shows the main diagnostic commands to use when reviewing SD-WAN behavior on a FortiGate device.

Through the next few slides, you will learn how to use them and see example outputs for each of them.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Members and Zones

- Summary view of SD-WAN members and zones configuration

```
# diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0
Member(3): interface: HUB1-VPN1, flags=0xc , gateway: 100.64.1.1, priority: 0 1024, weight: 0

# diagnose sys sdwan zone
Zone overlay index=3
        members(1): 25(HUB1-VPN1)
Zone underlay index=2
        members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
        members(0):

# diagnose netlink interface list | grep index=25
if=HUB1-VPN1 family=00 type=768 index=25 mtu=1420 link=0 master=0
```

Configuration index number

Automatic gateway detection—tunnel ID for IPsec tunnels (`diagnose vpn tunnel list`)

For volume-based load balancing

Kernel interface index number

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

To check the SD-WAN members and zones configuration, you can use the CLI commands:

- `diagnose sys sdwan member`
- `diagnose sys sdwan zone`

Note that FortiGate adjusts the output of the command `diagnose sys sdwan member` according to the load-balance mode you configured for the rule. For instance, when you use *measured-volume-based,* the command shows the volume ratio, last reading time, and the remaining volume room.

The command `diagnose sys sdwan zone` indicates the interface kernel ID near the interface name. You can review the interface kernel IDs with the command `diagnose netlink interface list`.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Health-Check Status

- Performance SLA:

```
# diagnose sys sdwan health-check status
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393), bandwidth-up(10235),
bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378), bandwidth-up(10236),
bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 HUB1-VPN3): state(alive), packet-loss(0.000%) latency(131.3[illegible]), jitter(0.199), mos(4.330), bandwidth-
up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 HUB1-VPN2): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.245), mos(4.398), bandwidth-
up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
```

Configuration index number

SLA result

- Link monitor status:

```
# diagnose sys link-monitor interface port1
Interface(port1): state(up, since Tue Nov 5 08:22:49 2024), bandwidth(up:79743bps, down:1094502bps), session
count(IPv4:412, IPv6:0), tx(39720018 bytes), rx(202184681 bytes), latency(21.96), jitter(0.17), packet-
loss(0.00).
```

- Link monitor passive status:

```
# diagnose sys link-monitor-passive admin list
  HUB1-VPN1( 19) | service=0x00000000 | latency=70.0  14:21:35 | jitter=0.0  14:21:47 | pktloss=0.0 %  14:21:47
```

Last time for criteria check

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

To check the SD-WAN health-check status and SLA performance you can use the command `diagnose sys sdwan health-check status`. This command gives, for each configured health check, the status of each member, alive or dead, and an instant value for the available criteria (packet-loss, latency, jitter, MOS, and bandwidth). The `sla_map` summarizes the SLA targets missed or passed. You will see on the next slide how to interpret the value presented.

Note that the health-check command displays a value for each available parameter, but the SLA process considers only the parameters for which you configured a target SLA value to determine the link SLA status and SLA map result.

The performance SLAs rely on the FortiOS link monitor process (`lnkmt`) to monitor the state and performance of members. For this reason, you can run the `diagnose sys link-monitor interface` command to display similar member status information as the one displayed by the `diagnose sys sdwan health-check status` command.

In passive or prefer passive mode, the link monitor passive process (`lnkmt_passive`) is responsible for gathering the data and preparing the reports used by the link monitor process to calculate packet loss, latency, and jitter. For this reason, you can run the `diagnose sys link-monitor-passive admin list` command to display the passive data collected.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SLA Target Maps

- `sla_map` uses a bitmask to reference SLA targets and indicates their status
  - The `sla_map` value represents the hexadecimal value of a binary number
  - Number of bits = number of configured SLA targets
  - First configured SLA target is assigned bit 0, second configured SLA target bit 1, and so on
  - Bit of SLA target is set to 1 if met, otherwise to 0
- Possible `sla_map` values for three SLA targets:

| sla_map (hex) | SLA Target #3 (Bit 2) Value = $2^2 = 4$ | SLA Target #2 (Bit 1) Value = $2^1 = 2$ | SLA Target #1 (Bit 0) Value = $2^0 = 1$ |
|---|---|---|---|
| 0x7 | Pass (1) | Pass (1) | Pass (1) |
| 0x6 | Pass (1) | Pass (1) | Fail (0) |
| 0x5 | Pass (1) | Fail (0) | Pass (1) |
| 0x4 | Pass (1) | Fail (0) | Fail (0) |
| 0x3 | Fail (0) | Pass (1) | Pass (1) |
| 0x2 | Fail (0) | Pass (1) | Fail (0) |
| 0x1 | Fail (0) | Fail (0) | Pass (1) |
| 0x0* | Fail (0) | Fail (0) | Fail (0) |

* Also means that there are no SLA targets configured

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

The `sla_map` field included in the output of the `diagnose sys sdwan health-check status` command indicates whether the member meets the configured SLA targets or not. The field uses a bitmask representation to reference the SLA targets and their status. Follow these rules to understand the `sla_map` field:

- The `sla_map` value represents the hexadecimal value of a binary number.
- The number of bits in the binary number equals the number of configured SLA targets.
- The first configured SLA target is assigned bit 0, the second configured SLA target bit 1, and so on.
- If the member meets the SLA target, the bit of the SLA target is set to 1, otherwise it is set to 0.

This slide shows a table with all the possible `sla_map` values when you configure three SLA targets for a member. For example, an `sla_map` of `0x6` means that SLA targets 3 and 2 are met, but not SLA target 1 (6 = 4 + 2 + 0). Expand or reduce the table according to the number of SLA targets configured in your setup.

Note that an `sla_map` of `0x0` has two possible meanings. If you configure one or more SLA targets for a member, `0x0` means that none of the SLA targets are met. However, `0x0` can also mean that you didn't configure any SLA targets for the member. Therefore, make sure to check the performance SLA configuration to identify whether there are SLA targets configured or not.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Link Monitor for Passive Health Check

- Link monitor passive status measured by kernel (local device measurement):

```
# diagnose sys link-monitor-passive admin list
  port1( 3) | service=0x00000000 | latency=40.0    05:04:04 | jitter=50.0    05:06:56 | pktloss=0.0  % 05:06:56
  port1( 3) | service=0x00003fe2 | latency=40.0    04:49:26 | jitter=40.0    04:49:32 | pktloss=1.8  % 04:49:32
  port2( 4) | service=0x00000000 | latency=40.0    04:49:18 | jitter=60.0    04:49:19 | pktloss=0.0  % 04:49:19
```

Kernel interface index

- Ordered by interface

```
# diagnose sys link-monitor-passive admin list by-interface

Interface port1 (3):
  Microsoft.Office.365.Portal(0x0000a1fc): latency=40.0    03:14:46, jitter=20.0    03:14:47,
pktloss=10.7 % 03:14:47
    Salesforce(0x00004218): latency=10.0    03:14:45, jitter=40.0    03:14:50, pktloss=3.5  % 03:14:50
   GoToMeeting(0x00003fe2): latency=30.0    03:14:46, jitter=30.0    03:14:51, pktloss=1.2  % 03:14:51
       Default(0x00000000): latency=50.0    03:14:04, jitter=0.0     NA      , pktloss=0.0  % NA

Interface port2 (4):
       Default(0x00000000): latency=30.0    03:14:42, jitter=60.0    03:14:43, pktloss=0.1  % 03:14:43
      Facebook(0x00003dd8): latency=40.0    03:14:49, jitter=40.0    03:14:51, pktloss=0.0  % 03:14:51
      LinkedIn(0x00003fcb): latency=40.0    03:14:51, jitter=20.0    03:14:52, pktloss=1.3  % 03:14:52
    Salesforce(0x00004218): latency=10.0    03:14:51, jitter=60.0    03:14:52, pktloss=2.9  % 03:14:52
   GoToMeeting(0x00003fe2): latency=10.0    03:14:51, jitter=30.0    03:14:35, pktloss=0.8  % 03:14:35
```

Applications monitored on interface

Monitored parameters per applications and monitored time

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

In passive or prefer passive mode, the link monitor passive process (`lnkmt_passive`) is responsible for gathering the data and preparing the reports used by the link monitor process to calculate packet loss, latency, and jitter. When the local device performs the link monitoring—done at the kernel level—you can run the `diagnose sys link-monitor-passive admin list` command to display the passive data collected.

This command comes with various display and filtering modes:

- Overall view: `diagnose sys link-monitor-passive admin list`
- Detailed view of services monitored per interface, for all interfaces (no filter), or for a specified interface: `diagnose sys link-monitor-passive admin list by-interface [<interface name>]`
- Detailed view ordered by monitored application: `diagnose sys link-monitor-passive admin list by-application [<application ID or application name>]`

For a configuration in which FortiGate uses the SLA report measured by a remote peer device, use the command `diagnose sys link-monitor-passive remote list` to check SLA information.

Remember that when you want to use passive monitoring, you must enable passive measurement at the policy level with the command `set passive-wan-health-measurement enable`. Because SD-WAN passive measurement is not supported by NPU, FortiGate will automatically disable `auto-asic-offload` for a policy that has a passive health measurement.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Link Monitor for Passive Health-Check (Contd)

- Link monitor passive status:
  - Ordered by application:

```
# diagnose sys link-monitor-passive admin list by-application
Service: Unmatched (0x00000000)
         port1( 3): latency=0.0     03:31:30, jitter=50.0    03:21:56, pktloss=0.0  % 03:21:56

Service: Facebook (0x00003dd8)
         port2( 4): latency=30.0    03:31:57, jitter=40.0    03:31:55, pktloss=0.0  % 03:31:55
[...]

# diagnose sys link-monitor-passive admin list by-application LinkedIn
Service: LinkedIn (0x00003fcb)
         port2( 4): latency=50.0    03:33:29, jitter=20.0    03:33:27, pktloss=0.6  % 03:33:27

# diagnose sys link-monitor-passive admin list by-application 41468
Service: Microsoft.Office.365.Portal (0x0000a1fc)
         port1( 3): latency=40.0    03:34:25, jitter=20.0    03:34:25, pktloss=10.1 % 03:34:25
         port2( 4): latency=30.0    03:19:09, jitter=20.0    03:19:10, pktloss=11.7 % 03:19:10
```

Filter by application name

Filter by application ID or hex. ID

  - Application ID mapping:

```
#    # diag sys link-monitor-passive admin app-id-map
     0: vd=0 4294836715 (0xfffe01eb) -> 15832 (0x00003dd8) Facebook
     1: vd=0 4294836842 (0xfffe026a) -> 16354 (0x00003fe2) GoToMeeting
     2: vd=0 4294837313 (0xfffe0441) -> 41468 (0x0000a1fc) Microsoft.Office.365.Portal
```

Application ID | Application Hex. ID | Application name

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

This slide shows an example of a passive link monitor output ordered by applications.

Note that you can decide to display the output for all applications or for only one. When you filter by application, you can filter on application name, application ID, or application hexadecimal value.

The command `diag sys link-monitor-passive admin app-id-map` gives you the mapping between application name, application ID, and hexadecimal ID.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SD-WAN Rules

- Rule status

```
# diagnose sys sdwan service4

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(4 HUB1-VPN2), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(3 HUB1-VPN1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
  Internet Service(1): SSH(4294837953,0,0,0,0 16060)
  Src address(1):
        10.0.1.0-10.0.1.255
```

Matching criteria and rule mode

Outgoing interface list

```
# diagnose sys sdwan service4 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Service disabled caused by no destination.
  Members(2):
    1: Seq_num(4 HUB1-VPN2), alive, selected
    2: Seq_num(5 HUB1-VPN3), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255
```

Warning message

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

SD-WAN rules are dynamically updated based on the member status and performance. This means that the outgoing interface list can change over time, which is why it is useful to check their current status for troubleshooting purposes.

The best way to check the status of an SD-WAN rule is by running `diagnose sys sdwan service4` on the FortiGate CLI. As shown on this slide, the output indicates the matching criteria in use, the rule mode, and the outgoing interface list. You can specify the service ID to display output for a single service (`diagnose sys sdwan service4 <service_id>`).

When you check SD-WAN service status details, pay attention to the warning messages that might appear above the member list.

Some of the warning messages you can see are:

- `service disabled caused by no destination` (no route to destination in the routing table)
- `service disabled caused by no outgoing path` (all outgoing interfaces are down)


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# View the ISDB Application Cache

- View the ISDB application cache entries on the FortiGate CLI:

```
# diagnose sys sdwan internet-service-app-ctrl-list

LinkedIn(16331 4294838042): 104.244.42.65 6 443 Mon Nov 04 03:24:12 2024
SSH(16060 4294837753): 10.1.0.7 6 22 Mon Nov 04 02:44:18 2024
SSH 16060 4294837753 : 10.1.0.28 6 22 Mon Nov 04 02:48:27 2024
```

Multiple 3-tuple for SSH app

App ID | ISDB app ID | 3-tuple | Timestamp (8-hour lifetime); one application per 3T (most recent detected application is written to cache)

- SD-WAN rule correlation:

```
# diagnose sys sdwan service4 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(4 HUB1-VPN2), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
    2: Seq_num(3 HUB1-VPN1), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected
  Internet Service(1): SSH(4294837753,0,0,0 16060
  Src address(1):
        10.0.1.0-10.0.1.255
```

ISDB app ID | App ID (SSH)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

You can view the detected application entries in the ISDB application cache by running `diagnose sys sdwan internet-service-app-ctrl-list` on the FortiGate CLI. Each entry in the output indicates the application ID, the ISDB application ID, the 3-tuple, and the last time the entry was refreshed. Note that FortiGate maintains one application per 3-tuple but one application can be associated with multiple 3-tuples. If multiple applications are detected for the same 3-tuple, FortiGate uses the most recent detected application for the 3-tuple.

FortiGate uses the application ID, ISDB application ID, and 3-tuple to match the SD-WAN rule. In the example shown on this slide, one cache entry is for an SSH connection destined to `10.1.0.7` on TCP port 22. A connection that matches the cache entry also matches SD-WAN rule ID 2.

Note that entries in the ISDB application cache expire 8 hours after the last detected match.

You can run the command `diagnose sys sdwan internet-service-app-ctrl-flush` to clear all ISDB application cache entries,



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## SLA Logging

- Disabled by default
- Enable SLA fail logs and SLA pass log independently
- FortiGate stores 10 minutes of history
- Forward to FortiAnalyzer for longer history record

- Activate SLA log on CLI

```
config sys sdwan
   config health-check
      edit "VPN_PING"
          set sla-fail-log-period 10
          set sla-pass-log-period 20
      next
   end
```

Log frequency in seconds

- Activate SLA log on FortiManager SD-WAN template

**Device Manager > Provisioning template > SD-WAN Templates > Performance SLA > Advanced Options**

| | |
|---|---|
| sla-fail-log-period | 10 |
| sla-id-redistribute | 0 |
| sla-pass-log-period | 20 |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

As already introduced in the first section of this lesson, by default, FortiGate does not log the SLA health-check result. If you want to view past SLA status, you can enable SLA fail and SLA pass log collection with the commands `set sla-fail-log-period <frequency>` and `set sla-pass-log-period <frequency>` respectively. When configured, FortiGate stores the SLA status for each measured parameter at the frequency you defined. It will keep 10 minutes of log history. For a longer retention period, you can forward the log to an external storage device like FortiAnalyzer.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## View Member SLA Logs on the FortiGate CLI

- Member metrics: `diagnose sys sdwan sla-log <SLA target> <index>`

```
# diagnose sys sdwan sla-log Level3_DNS 1
Timestamp: Wed Nov 05 00:42:07 2024, vdom root, health-check Level3_DNS, interface: port1, status: up,
latency: 34.780, jitter: 0.166, packet loss: 0.000%.
Timestamp: Wed Nov 05 00:42:07 2024, vdom root, health-check Level3_DNS, interface: port1, status: up,
latency: 34.784, jitter: 0.164, packet loss: 0.000%.
...
Timestamp: Wed Nov 05 00:52:07 2024, vdom root, health-check Level3_DNS, interface: port1, status: up,
latency: 34.766, jitter: 0.170, packet loss: 0.000%.
```

Member configuration index number

10-min period

- Member utilization: `diagnose sys sdwan intf-sla-log <interface>`

```
# diagnose sys sdwan intf-sla-log port1
Timestamp: Wed Nov 05 00:41:54 2024, used inbandwidth: 1946bps, used outbandwidth: 1788bps, used
bibandwidth: 3734bps, tx bytes: 17460310429bytes, rx bytes: 5174715499bytes.
Timestamp: Wed Nov 05 00:42:04 2024, used inbandwidth: 2827bps, used outbandwidth: 2322bps, used
bibandwidth: 5149bps, tx bytes: 17460315966bytes, rx bytes: 5174723207bytes.
...
Timestamp: Wed Nov 05 00:51:54 2024, used inbandwidth: 3128bps, used outbandwidth: 2319bps, used
bibandwidth: 5447bps, tx bytes: 17460497678bytes, rx bytes: 5174940763bytes.
```

10-min period

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

FortiOS stores the measured metrics and utilization of members for the last 10 minutes. This historical data is used by both the FortiManager and FortiGate GUIs to build their performance SLA graphs.

You can view the stored member metrics by running the `diagnose sys sdwan sla-log` command. Note that you must indicate the name of the performance SLA followed by the member configuration index number. To display the SLA logs per interface, you run the `diagnose sys sdwan intf-sla-log` command.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Troubleshoot ADVPN Shortcut Negotiation

- Use the command `diagnose debug application ike -1`
  - Look for message with:
    - `shortcut-query`
    - `shortcut-reply`
    - `shortcut-offer`

Example of a hub that send `shortcut-offer` to a spoke

```
ike V=root:0: shortcut VPN1_0:192.2.0.1:0 to VPN1_1:203.0.113.1:0 for 10.0.1.101->10.0.2.101 0
ike 0 ike_ui_admin_caps_trigger sport 2048, dport 0, proto 1, iif 20
ike V=root:0 send shortcut-offer to VPN1_0
```

- Specify multiple IP addresses to filter the IKE real-time debug
  - Useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations

```
diagnose debug console timestamp enable
diagnose vpn ike log filter clear
diagnose vpn ike log filter mrem-addr4 <ip.of.hub> <ip.of.spoke>
diagnose debug application ike -1
diagnose debug enable
```

Filter on multiple IPv4 destination address (mrem-addr6 for IPv6 address)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

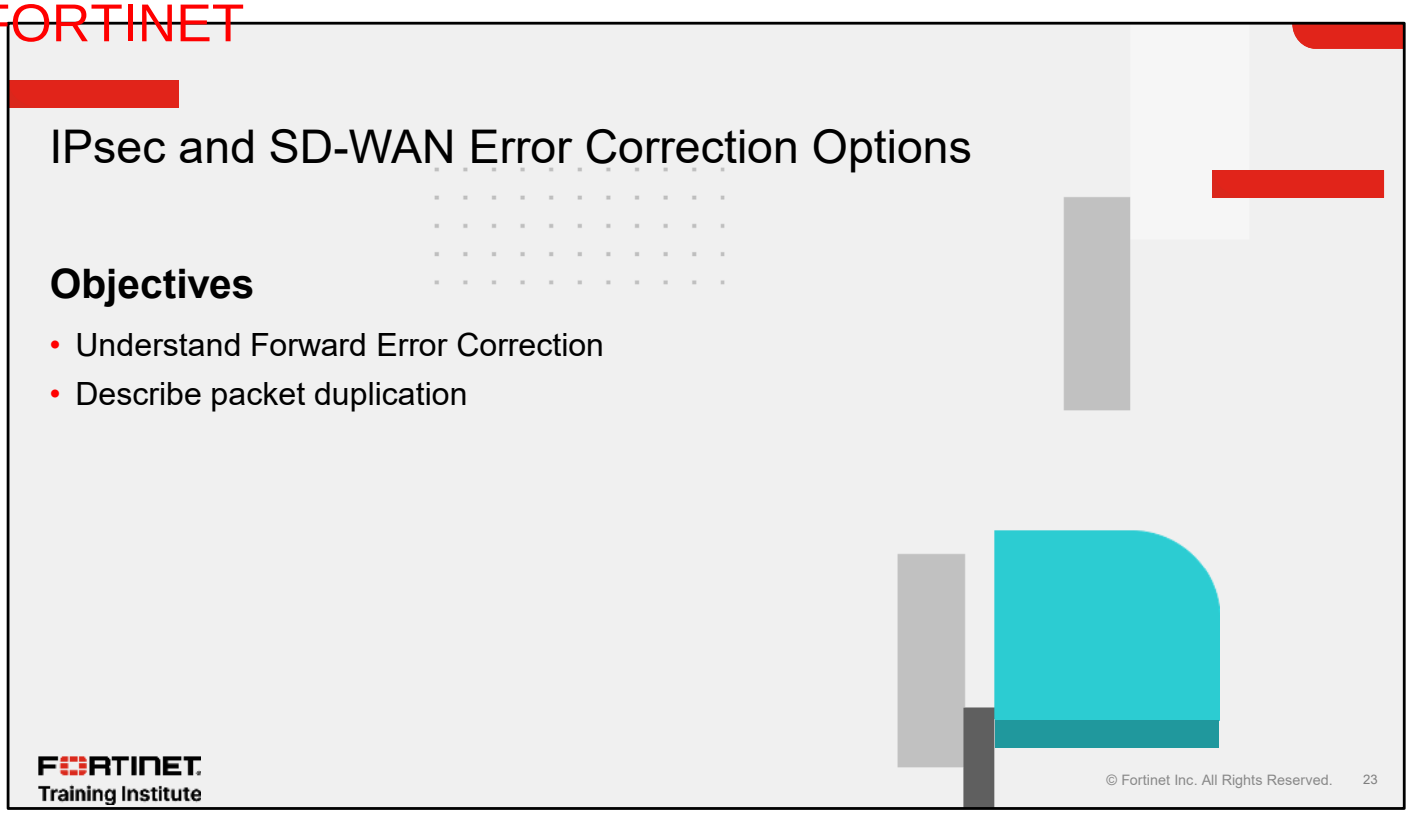
To troubleshoot ADVPN shortcut negotiation you can use the diagnose commands related to IPsec and IKE, such as `diagnose debug application ike -1`.

Enable debug of IKE to debug ADVPN shortcut negotiation, as shown on this slide.

In the IKE log filter, you can specify multiple IP addresses to print debug messages for. This is very useful when debugging ADVPN shortcuts and spoke-to-spoke ADVPN negotiation issues.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




After completing this section, you should be able to achieve the objectives shown on this slide.

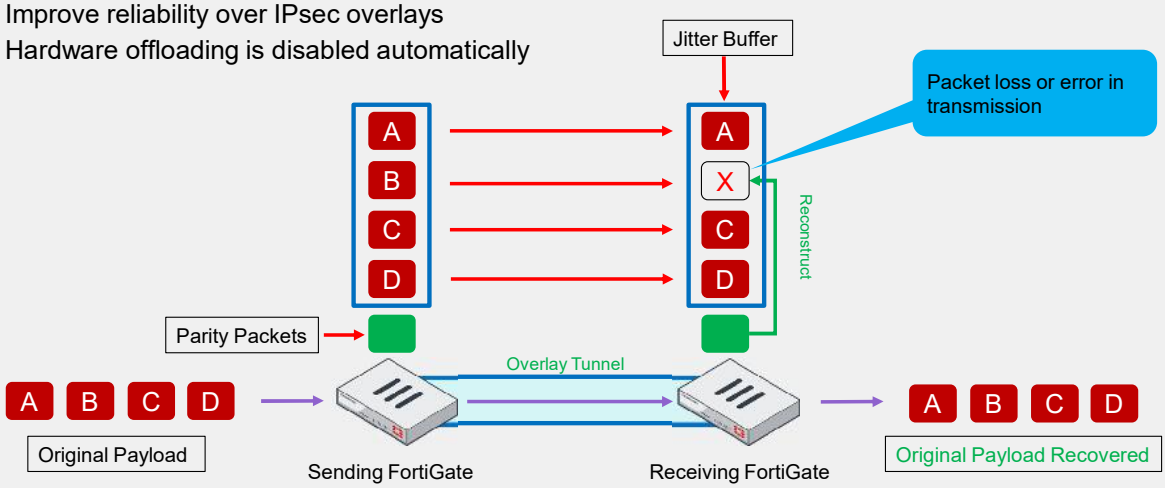
By demonstrating competence in advanced IPsec features, you will be able to configure IPsec to improve overlay performance and reliability.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Forward Error Correction

- Send additional parity packets that contain error-correcting data
  - Fortinet proprietary implementation
- Recipient can use the parity packets to reconstruct data loss
  - Improve reliability over IPsec overlays
  - Hardware offloading is disabled automatically




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

Forward error correction (FEC) is an error correction technique available for IPsec overlays. FEC is used to control and correct errors in data transmission by sending redundant data across the VPN in anticipation of dropped packets occurring during transit. The FEC implementation on FortiGate doesn't work with third-party IPsec gateways.

When you enable FEC on an IPsec overlay, the sending FortiGate transmits additional packets—called parity packets—through the tunnel. The parity packets contain error-correcting data that is calculated based on the data contained in the original packets. The receiving FortiGate can then use the parity packets to reconstruct any lost packet, or any packet that arrived with errors.

Although FEC increases the bandwidth usage on an IPsec tunnel, it also improves the reliability of overlays by overcoming adverse WAN conditions, such as lossy or noisy underlays. FEC is useful for delivering a better user experience for business-critical applications, like voice and video services.

Note that FortiOS automatically disables hardware offload for traffic that is subject to FEC and therefore increases CPU usage.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# FEC Configuration

- CLI configuration:

```
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        set fec-egress enable
        set fec-ingress enable
        set fec-base 20
        set fec-redundant 2
        set fec-send-timeout 8
    next
end
config firewall policy
    edit <id>
        set fec enable
    next
end
```

Send parity packets on egress

Process parity packets on ingress

Timeout for parity packets (milliseconds)

Enable FEC on the traffic matching firewall policy to generate parity packets

**IPsec Tunnel > Advanced Options**

| | |
|---|---|
| fec-base | 20 |
| fec-codec | rs |
| fec-egress | |
| fec-ingress | |
| fec-mapping-profile | Click to select |
| fec-receive-timeout | 50 |
| fec-redundant | 2 |
| fec-send-timeout | 8 |

- Within `fec-send-timeout` period, send two `fec-redundant` parity packets for every twenty `fec-base` packets
- FEC uses a specific SPI (`0x00000001`) for original and parity packets:

```
16.601180 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
16.841846 port1 out 192.2.0.1 -> 100.64.1.1: ESP(spi=0xbd0b3bad,seq=0xe13)
16.841871 port1 out 192.2.0.1 -> 100.64.1.1: ESP(spi=0x00000001,seq=0xefec)
17.101768 port1 out 192.2.0.1 -> 100.64.1.1: ESP(spi=0x00000001,seq=0xefec)
```

Original packets

Parity packets

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

This slide shows a basic configuration for FEC on an IPsec overlay using the FortiGate CLI.

FEC works by sending a `fec-redundant` number of parity packets for every `fec-base` number of packets sent within the `fec-send-timeout` period. However, if `fec-send-timeout` is reached, FortiGate sends the parity packets regardless of `fec-base`. The `fec-send-timeout` period starts after FortiGate receives the first packet destined for the tunnel. If you apply the configuration shown on this slide, then FortiGate sends two parity packets over HUB1-VPN1 for every 20 packets sent through the tunnel over a period of eight milliseconds.

Also note that you must indicate the direction that you want FEC to run on. For example, if you want FortiGate to send parity packets in the egress direction, then you must enable `fec-egress`. Similarly, if you want FortiGate to process parity packets sent by the remote FortiGate, then you must enable `fec-ingress`. You must also enable `fec` on the firewall policy that matches the traffic that you want to generate parity packets for. Note that you don't have to manually disable hardware offloading. FortiOS will do that automatically for you on sessions that are subject to FEC.

Note that when you enable FEC, FortiGate uses the specific security payload index shown on this slide for original and parity packets.

This slide also shows a packet capture taken using the example configuration. The packet capture shows the original packet—an ICMP echo request to `10.0.2.101`—egressing the HUB1-VPN1 overlay, which is bound to port1. The packet capture also shows three more Encapsulating Security Payload (ESP) packets egressing port1. Although not revealed in the output, the first ESP packet carries the original ICMP echo request packet. The following two ESP packets are parity packets of the original ICMP echo request packet.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Impact of FEC on Overlay Quality

- Before enabling FEC:

```
root@branch1-client-cli:~# ping 10.0.2.101 -i 0.2 -c 100
PING 10.0.2.101 (10.0.2.101) 56(84) bytes of data.
...
--- 10.0.2.101 ping statistics ---
100 packets transmitted, 73 received, 27% packet loss, time 964ms
rtt min/avg/max/mdev = 1.002/2.619/5.433/0.895 ms
```

- After enabling FEC (`fec-egress: enable`, `fec-ingress: enable`, `fec-redundant: 1`, `fec-base: 20`, `fec-send-timeout: 8`):

```
--- 10.0.2.101 ping statistics ---
100 packets transmitted, 88 received, 12% packet loss, time 914ms
rtt min/avg/max/mdev = 1.749/4.497/13.317/2.851 ms
```

- After increasing `fec-redundant` to `3`:

```
--- 10.0.2.101 ping statistics ---
100 packets transmitted, 99 received, 1% packet loss, time 891ms
rtt min/avg/max/mdev = 2.133/4.317/13.098/2.271 ms
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

This slide shows the positive impact that FEC has on the quality of IPsec overlays. The test consists of generating 100 ICMP echo request packets across a noisy overlay, and then identifying the amount of packet loss reported by the ping tool before and after enabling FEC.

The first output shows the ping statistics before enabling FEC. The reported packet loss is 27%.

The second output shows the ping statistics after the administrator enables FEC on both local and remote FortiGate devices using the settings shown on this slide. The packet loss is reduced to 12%.

The administrator then increases the `fec-redundant` setting from `1` to `3` on both ends of the tunnels. As a result, the packet loss is reduced to 1%.

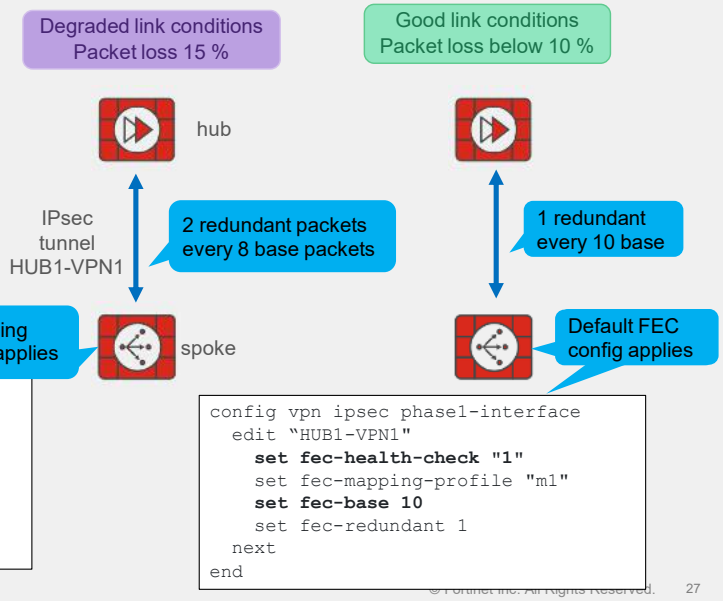
Therefore, you can increase the quality of noisy overlays by enabling FEC and increasing the `fec-redundant` setting. Just keep in mind that the higher the value of `fec-redundant`, the more bandwidth is used.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Adaptative FEC

- Dynamically adjusts the FEC packet ratio according to the link conditions
  - Adjust FEC base
  - Adjust FEC redundant packets
- Use cases
  - Apply per policy
  - Reserve to streams sensitive to packet loss
  - Example: UDP-based VoIP protocol
- Limitations
  - FEC does not support NPU offloading




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Adaptive FEC considers link conditions and dynamically adjusts the FEC packet ratio. The FEC base and redundant packet relationship is dynamically adjusted based on changes to the network SLA metrics defined in the SD-WAN SLA health checks. For example, when there is no or low packet loss in the network, FEC can work a low redundancy level sending only one redundant packet for every 10 base packets. As packet loss increases, the number of redundant packets sent rises accordingly.

Because FEC does not support network processing unit (NPU) offloading, you should not apply it to every traffic flow and apply it only to the streams that are the most sensitive packet loss. For example, policies that allow the UDP-based Voice over IP (VoIP) protocol can enable FEC, while TCP-based traffic policies do not. This reduces unnecessary bandwidth consumption by FEC and limits the number of policies that require NPU offload to be disabled.

The example shown on this slide shows a FEC mapping rule, `m1`, configured to send two redundant packets for every eight base packets if the link performance degrades to a packet loss rate above 10%. The configuration of the IPsec tunnel `HUB1-VPN1` defines a default FEC rate of one redundant packet every 10 base packets and applies the mapping profile `m1`.

Also configured on the spoke, but not shown on this slide, are the following:
- The SD-WAN SLA configuration
- HUB1-VPN1 IPsec tunnel with `fec-egress` enabled
- A firewall policy that disables NPU offload, enables FEC, and allows the traffic flow

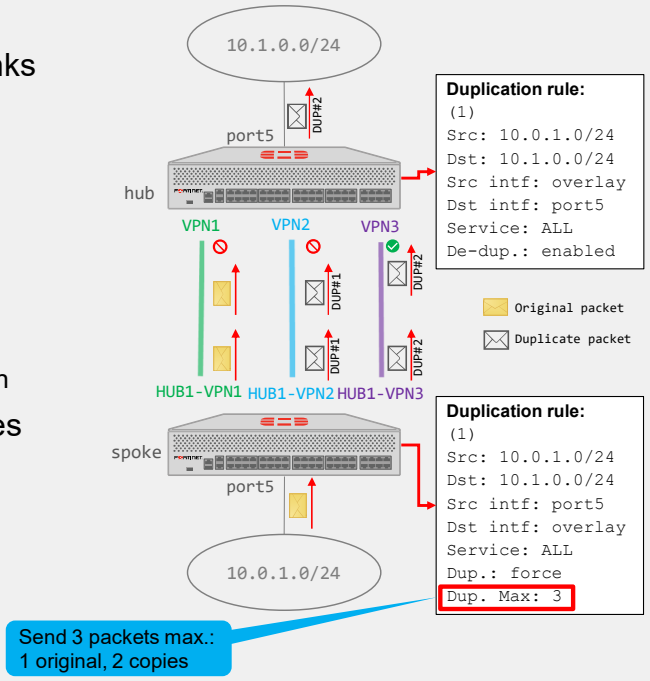
To work with the configuration on the spoke, you must enable `fec-ingress` on the hub IPsec tunnel configuration.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

## Packet Duplication

- Send duplicate packets through additional links
  - Can be underlay or overlay
  - Supports hardware offloading
- Requirements
  - Best route must match an SD-WAN member
  - Member must have route to destination
- Duplicate packets are exact copies of the original packet
  - Useful for data loss protection and OOB inspection
- Enable deduplication to drop additional copies
  - First arriving packet is accepted, others dropped




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

FEC provides an efficient way to reduce data loss on IPsec tunnels. However, FEC doesn't leverage multiple IPsec tunnels. In addition, FEC doesn't support hardware offload or links that are not IPsec.

Packet duplication is an SD-WAN feature that enables you to send duplicate packets through up to three additional members of any kind, provided the best route to the destination is an SD-WAN member, and the links used for duplication have a route to the destination. Unlike the parity packets in FEC, which are not exact copies of the original packets, the duplicate packets are verbatim copies of the original packet. This way, the duplicate packets can be used for data loss protection and out-of-band inspection or packet capture.

You can also enable packet deduplication on the receiving FortiGate. When you do this, the receiving FortiGate accepts only the first copy of the packet received, and drops the additional copies. The goal is to save resources at the receiving end by instructing FortiGate to forward one copy only, instead of forwarding all copies and letting the next hop discard the additional packets.

The example on this slide shows two FortiGate devices connected through three IPsec overlays, which are members of the overlay zone. On the spoke FortiGate, the administrator configured a duplication rule that instructs FortiGate to always duplicate (forced duplication) any packet sourced from 10.0.1.0/24 and destined to 10.1.0.0/24, to up to three links. On the hub FortiGate, the administrator configured a duplication rule to deduplicate the same traffic.

The result is that when the spoke FortiGate receives a packet that matches the duplication rule, it forwards the original packet to the preferred member in the zone, plus two additional copies through two additional links, for a total of three packets. On the remote side, the hub FortiGate accepts only the packet received through VPN3 because it was the first packet to arrive, and drops the additional copies received through VPN1 and VPN2. The result is that one packet only is forwarded to the local interface (port5).



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Forced Packet Duplication

- Spoke CLI configuration:

```
config system sdwan
    set duplication-max-num 3
    config duplication
        edit 1
            set srcaddr "10.0.1.0/24"
            set dstaddr "10.1.0.0/24"
            set srcintf "port5"
            set dstintf "overlay"
            set service "ALL"
            set packet-duplication force
        next
    end
end
```

Always duplicate; an alternative is `on-demand`

- Hub CLI configuration:

```
config system sdwan
    config duplication
        edit 1
            set srcaddr "10.0.1.0/24"
            set dstaddr "10.1.0.0/24"
            set srcintf "overlay"
            set dstintf "port5"
            set service "ALL"
            set packet-de-duplication enable
        next
    end
end
```

- Spoke packet duplication:

```
port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN3 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN3 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

3 copies (original plus 2 duplicates)

- Hub packet deduplication:

```
VPN3 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
VPN2 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
VPN1 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
VPN3out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

First to arrive, only to be accepted

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

This slide shows the configuration used for the packet duplication example shown on the previous slide, which uses forced packet duplication.

The duplication rules on both spoke and hub indicate the 5-tuple of the traffic to duplicate and deduplicate, respectively. On the spoke, `duplication-max-num` is set to `3`. This instructs FortiGate to forward up to three copies of the packet—the original packet plus two duplicates. Moreover, each copy is sent through a different member. On the spoke, `packet-duplication` is set to `force`, which instructs FortiGate to always duplicate packets. An alternative is to set `packet-duplication` to `on-demand`, which instructs FortiGate to duplicate packets based on the SLA status of the outgoing interface.

On the hub side, `packet-de-duplication` is enabled to instruct FortiGate to accept one copy of the packet only—the first to arrive—and drop any additional copies.

This slide also shows the sniffer output for the corresponding duplicated and deduplicated packets on the spoke and hub, respectively. On the spoke, the original ICMP echo request packet is received at port5, and then forwarded to HUB1-VPN2. The spoke also forwards two more copies, one to HUB1-VPN3, and another to HUB1-VPN1. On the hub side, all three packets are received, but only the first packet received—the packet received at HUB1-VPN3—is accepted and forwarded. The hub FortiGate then creates a session with HUB1-VPN3 as the incoming interface, which is why the ICMP echo reply packet is forwarded to the same interface.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# On-Demand Packet Duplication

- Consider link quality before duplicating packets:
  - Don't duplicate if:
    - Outgoing interface meets at least one of the SLA targets
  - Duplicate packets if:
    - Outgoing interface doesn't meet any SLA targets, or no SLA targets are configured
- Example (outgoing interface is HUB1-VPN1):
  - HUB1-VPN1 meets at least one SLA target (no duplication):

```
# diagnose sys sdwan health-check status
Health Check(VPN):
Seq(3 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(1.500), jitter(0.291) sla_map=0x3
Seq(4 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.415), jitter(0.281) sla_map=0x3
Seq(5 HUB1-VPN3): state(alive), packet-loss(0.000%) latency(1.116), jitter(0.225) sla_map=0x3
```

  - HUB1-VPN1 doesn't meet any SLA targets (perform duplication):

No SLA targets met

```
# diagnose sys sdwan health-check status
Health Check(VPN):
Seq(3 HUB1-VPN1): state(alive), packet-loss(1.000%) latency(171.729), jitter(0.340) sla_map=0x0
Seq(4 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.506), jitter(0.419) sla_map=0x3
Seq(5 HUB1-VPN3): state(alive), packet-loss(0.000%) latency(1.061), jitter(0.280) sla_map=0x3
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

Forced packet duplication instructs FortiGate to always duplicate packets. But what if you want FortiGate to perform duplication only when the quality of the outgoing interface is poor? This way, you can save network resources by avoiding duplicate traffic when the outgoing interface is performing well, and the original packet is likely to be successfully delivered.

When you configure on-demand packet duplication, FortiGate considers the quality of the outgoing interface selected to route the original packet before creating any duplicates. The outgoing interface is selected based on the SD-WAN rule lookup for the packet. That is, the packet doesn't have to match a user-defined SD-WAN rule for duplication to be triggered. This is also true for forced packet duplication.

FortiGate determines the quality of the outgoing interface based on the status of the SLA targets configured. If the interface meets at least one of its configured SLA targets, FortiGate considers the quality to be acceptable and doesn't create duplicates. If the interface doesn't meet any of its configured SLA targets, or if the interface doesn't have any SLA targets configured, then FortiGate performs duplication.

This slide shows the health of three overlays taken at different times. Assuming HUB1-VPN1 is the selected outgoing interface for the original packet, then FortiGate doesn't create duplicates when the performance of HUB1-VPN1 is the one shown in the first output. However, if the performance is the one shown in the second output, then FortiGate creates duplicates because HUB1-VPN1 doesn't meet any of the SLA targets.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

# Restrict Packet Duplication to SD-WAN Rules

- Duplicate traffic that matches one or more SD-WAN rules
  - More granular control and flexibility
  - Reduced configuration
- CLI configuration:

```
config system sdwan
    set duplication-max-num 3
    config duplication
        edit 1
            set service-id 1
            set packet-duplication force
        next
    end
end
```

- SD-WAN rule ID 1 status:

```
Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(1: 1->65535), Mode(manual)
  Members(3):
    1: Seq_num(3 HUB1-VPN1), alive, selected
    2: Seq_num(4 HUB1-VPN2), alive, selected
    3: Seq_num(5 HUB1-VPN3), alive, selected
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        10.1.0.7-10.1.0.7
```

- ICMP traffic to 10.1.0.7 is duplicated:

```
port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN3 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
```

- Other traffic, like SSH, is not duplicated:

```
port5 in 10.0.1.101.55030 -> 10.1.0.7.22: syn 122428627
HUB1-VPN1 out 10.0.1.101.55030 -> 10.1.0.7.22: syn 122428627
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

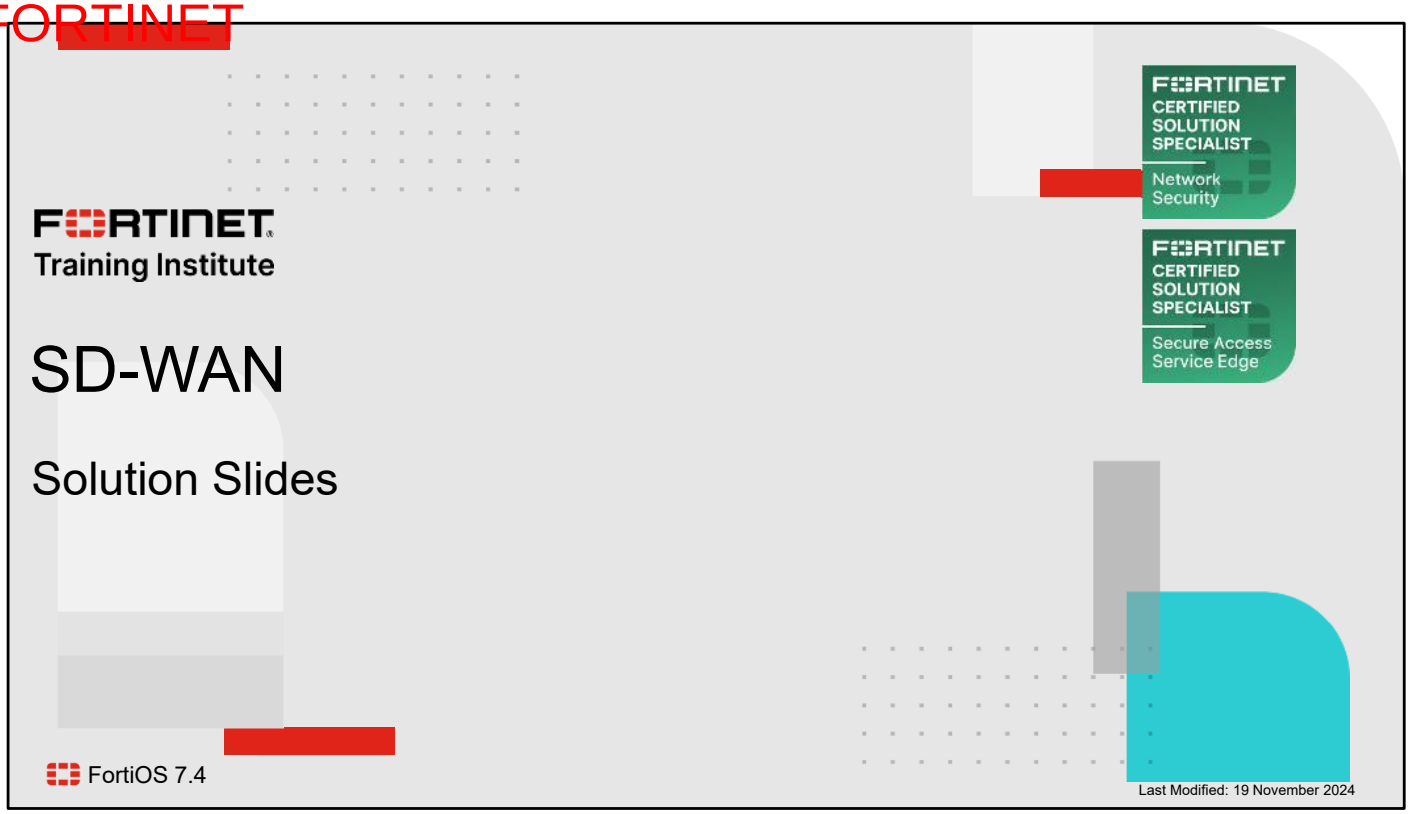
You can configure packet duplication rules to duplicate packets that match one or more SD-WAN rules. This enables you to have more granular control and flexibility over duplicated traffic, as well as reduce the configuration required. For example, you can leverage the application steering feature of SD-WAN rules to duplicate traffic based on the detected application, rather than using the fixed 5-tuple configuration on a duplication rule to identify the traffic. Similarly, you can leverage ISDB and route tags to identify the destination of the traffic to duplicate.

This slide shows an example of a forced packet duplication rule that matches the SD-WAN rule ID 1. Note that after you configure the SD-WAN rule ID using the service setting, the options to define the 5-tuple of the traffic on the duplicate rule are hidden. This is because the matching criteria is now defined by the SD-WAN rule.

This slide also shows the SD-WAN rule status. The output indicates that the SD-WAN rule matches ICMP traffic from any source to 10.1.0.7. The result is that FortiGate duplicates only the traffic that matches the SD-WAN rule ID 1. Other traffic, such as SSH, is not duplicated.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

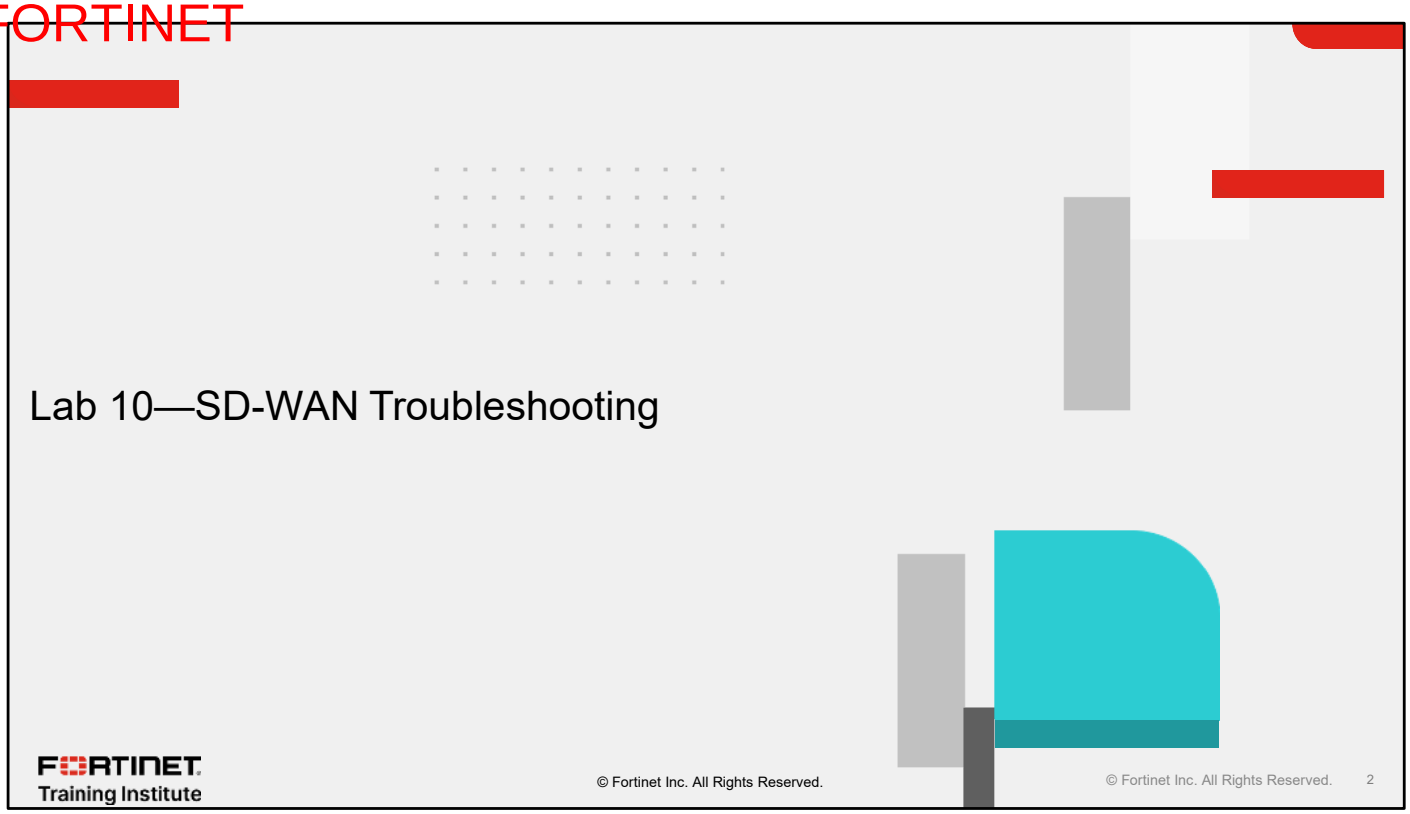



These slides contain the solutions to the troubleshooting exercises.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

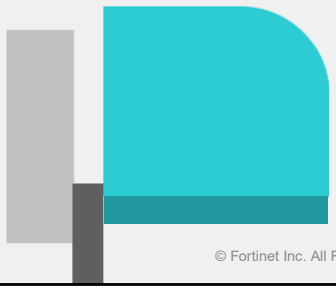



You will review the solutions for the troubleshooting exercises in the SD-WAN troubleshooting lab.


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Troubleshooting Spoke-to-Spoke Traffic (Single Hub)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 3


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 1—Issue Description

- Issue:
  - Traffic from branch1_client to branch2_client is always routed over HUB1-VPN3
- Expected behavior:
  - Use HUB1-VPN1 as primary
  - Use HUB1-VPN3 as failover (when HUB1-VPN1 is dead)
  - After HUB1-VPN1 recovers, fail back to HUB1-VPN1

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

The administrator has identified the following issue:

- Traffic from branch1_client to branch2_client is always routed over HUB1-VPN3.

However, the administrator wants to see the following behavior:

- branch1_fgt uses HUB1-VPN1 as the primary member to route traffic to branch2_fgt.
- branch1_fgt uses HUB1-VPN3 to route traffic to branch2_fgt only if HUB1-VPN1 is determined to be dead.
- After HUB1-VPN1 recovers, spoke-to-spoke traffic is routed through HUB1-VPN1 again.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Issue Confirmation

- Ping branch2_client (`10.0.2.101`) from branch1_client (`10.0.1.101`)
- Sniff traffic on branch1_fgt:

```
branch1_fgt # diagnose sniffer packet any "host 10.0.2.101" 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.2.101]
2024-07-24 18:47:55.886529 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 18:47:55.886600 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 18:47:55.888757 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 18:47:55.888781 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

- Traffic is routed over HUB1-VPN3, but HUB1-VPN1 is alive and is the preferred member for the expected matching SD-WAN rule (ID 3):

**Network > SD-WAN > Performance SLAs**

| Name | Detect Server | Packet Loss | Latency | Jitter |
|---|---|---|---|---|
| VPN_PING | 10.200.99.1 | HUB1-VPN1: 0.00%<br>HUB1-VPN3: 0.00% | HUB1-VPN1: 0.83ms<br>HUB1-VPN3: 0.65ms | HUB1-VPN1: 0.14ms<br>HUB1-VPN3: 0.11ms |

**Network > SD-WAN > SD-WAN Rules**

| ID | Name | Source | Destination | Members |
|---|---|---|---|---|
| 3 | Corp | LAN-net | Corp-net | HUB1-VPN1<br>HUB1-VPN3 |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 5

You can confirm the issue by pinging `10.0.2.101` from branch1_client, while at the same time running a sniffer on the FortiGate CLI. You can see that FortiGate routes the ICMP packets over HUB1-VPN3. However, when you check the health of HUB1-VPN1 and the SD-WAN rule configuration on the FortiGate GUI, you can see that HUB1-VPN1 is alive and is the preferred member for SD-WAN rule ID 3. SD-WAN rule ID 3 is the expected matching rule for spoke-to-spoke traffic.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Troubleshooting

- Debug flow:

```
id=20085 trace_id=3 func=print_pkt_detail line=5783 msg="vd-root:0 received a packet(proto=1, 10.0.1.101:8605-
>10.0.2.101:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=8605, seq=1."
id=20085 trace_id=3 func=init_ip_session_common line=5955 msg="allocate a new session-00000209"
id=20085 trace_id=3 func=rpdb_srv_match_input line=1030 msg="Match policy routing id=1: to 10.0.2.101 via ifindex-21"
id=20085 trace_id=3 func=vf_ip_route_input_common line=2605 msg="find a route: flag=00000000 gw-172.16.1.5 via HUB1-VPN3"
id=20085 trace_id=3 func=fw_forward_handler line=869 msg="Allowed by Policy-2:"
id=20085 trace_id=3 func=ipsecdev_hard_start_xmit line=625 msg="enter IPSec interface HUB1-VPN3, tun_id=0.0.0.0"
id=20085 trace_id=3 func=_do_ipsecdev_hard_start_xmit line=229 msg="output to IPSec tunnel HUB1-VPN3, tun_id=172.16.1.5,
vrf 0"
id=20085 trace_id=3 func=esp_output4 line=867 msg="IPsec encrypt/auth"
...
id=20085 trace_id=3 func=ipsec_output_finish line=546 msg="send to 172.16.0.2 via intf-port4"
...
```

- Traffic matches policy route ID 1
  - ID ≤ 65535, so the policy route is a regular policy route
  - Traffic should match SD-WAN rule ID 3

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

If you run a debug flow, you can see that the traffic matches policy route ID 1. The ID is lower than 65535, which means that the policy route is a regular policy route. However, the traffic should match the SD-WAN rule ID 3 instead.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Troubleshooting (Contd)

- Policy route table:

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=7(port5) path(1):
oif=22(HUB1-VPN3) path_last_used=2024-11-05 07:40:49
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=19 last_used=2024-11-05 07:40:49
...
```

- Regular policy route configuration:

**Network > Policy Routes**

| Seq.# | Incoming Interface | Outgoing Interface | Source | Destination |
|---|---|---|---|---|
| 1 | port5 | HUB1-VPN3 | LAN-net | Corp-net |

- Root cause: Presence of a regular policy route (precedence over other types of policy routes)
- Solution: Remove the regular policy route

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 7

If you view the policy route table, you can see the details of the regular policy route ID 1. On the FortiGate GUI, you can see the corresponding regular policy route configuration.

The presence of the regular policy route, which has precedence over other types of policy routes, including SD-WAN rules, results in traffic being sent to HUB1-VPN3. You can solve the issue by removing the regular policy route from the configuration.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Testing Member Selection

- Regular policy route is removed
- Ping branch2_client (`10.0.2.101`) from branch1_client (`10.0.1.101`)
- Sniff traffic on branch1_fgt:

```
2023-01-04 18:51:56.537826 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2023-01-04 18:51:56.537926 HUB1-VPN2 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2023-01-04 18:51:56.543305 HUB1-VPN2 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2023-01-04 18:51:56.543327 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

- Debug flow:

```
id=20085 trace_id=5 func=print_pkt_detail line=5783 msg="vd-root:0 received a packet(proto=1, 10.0.1.101:8608-
>10.0.2.101:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=8608, seq=1."
id=20085 trace_id=5 func=init_ip_session_common line=5955 msg="allocate a new session-00000262"
id=20085 trace_id=5 func=vf_ip_route_input_rcu line=2605 msg="find a route: flag=00000000 gw-100.64.1.9 via HUB1-VPN2"
id=20085 trace_id=5 func=fw_forward_handler line=869 msg="Allowed by Policy-4:"
id=20085 trace_id=5 func=ipsecdev_hard_start_xmit line=625 msg="enter IPSec interface HUB1-VPN2, tun_id=0.0.0.0."
id=20085 trace_id=5 func=_do_ipsecdev_hard_start_xmit line=229 msg="output to IPSec tunnel HUB1-VPN2, tun_id=100.64.1.9,
vrf 0"
```

- No policy route match:
  - SD-WAN rules are skipped
  - Traffic is routed over HUB1-VPN2 after FIB lookup (implicit rule)
  - Traffic should be routed over HUB1-VPN1

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 8

After you remove the regular policy route, repeat the test. You can see that traffic is now routed to HUB1-VPN2, instead of HUB1-VPN1.

When you run a debug flow, you can see that the traffic doesn't match a policy route. Instead, the traffic is handled using standard FIB routing, and the best route resolves to HUB1-VPN2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Route Lookup and SD-WAN Members

- Route lookup for `10.0.2.101`:

```
branch1_fgt # get router info routing-table details 10.0.2.101

Routing table for VRF=0
Routing entry for 10.0.2.0/24
  Known via "static", distance 10, metric 0, best
  * via HUB1-VPN2 tunnel 100.64.1.9 vrf 0, tun_id
```

- SD-WAN members:

```
branch1_fgt # diagnose sys sdwan member
Member(1): transport-group: 0, interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 1 1024,
weight: 0
Member(2): transport-group: 0, interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 1 1024,
weight: 0
Member(3): transport-group: 0, interface: HUB1-VPN1, flags=0xc , gateway: 100.64.1.1, priority: 1 1024,
weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN3, flags=0xc , gateway: 172.16.1.5, priority: 1 1024,
weight: 0
```

HUB1-VPN2 is not listed

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 9

When you perform a route lookup on the FortiGate CLI for `10.0.2.101`, you can confirm that HUB1-VPN2 is the best route. Then, if you view the status of SD-WAN members, you can see that HUB1-VPN2 is not included in the list.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Checking Configured Static Routes

- Static route configuration:

**Network > Static Routes**

| Destination | Gateway IP | Interface | Status |
|---|---|---|---|
| 0.0.0.0/0 | | underlay | Enabled |
| 10.0.2.0/24 | | HUB1-VPN2 | Enabled |
| 172.16.0.0/16 | 172.16.0.2 | port4 | Enabled |
| 10.0.0.0/8 | | overlay | Enabled |

Best route to `10.0.2.101`

- Root cause: Best route to destination isn't an SD-WAN member
  - Rule ID 3 is skipped
- Solution: Delete static route for HUB1-VPN2
- Route lookup for `10.0.2.101`:

```
branch1_fgt # get router info routing-table details 10.0.2.101

Routing table for VRF=0
Routing entry for 10.0.0.0/8
  Known via "static", distance 1, metric 0, best
  * via HUB1-VPN3 tunnel 172.16.1.5 vrf 0, origin 2
```

  - Best route to destination is now an SD-WAN member

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 10

If you check the configured static routes, you can confirm that there is a static route configured for HUB1-VPN2.

Because the best route to the destination isn't an SD-WAN member, by default, FortiGate skips the SD-WAN rule during the matching process. The result is that the traffic matches the SD-WAN implicit rule. That is, FortiGate performs standard FIB routing for the traffic.

You can solve the issue by removing the static route for HUB1-VPN2. After you remove the static route and perform another route lookup for `10.0.2.101`, you can see that HUB1-VPN3, an SD-WAN member, is now the best route.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Testing Member Selection (Contd)

- Ping branch2_client (10.0.2.101) from branch1_client (10.0.1.101)
- Sniff traffic on branch1_fgt:

```
2023-01-04 13:24:29.262836 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2023-01-04 13:24:29.263035 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2023-01-04 13:24:29.270880 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2023-01-04 13:24:29.270924 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

- Debug flow and policy route table:

```
...
id=20085 trace_id=5 func=rpdb_srv_match_input line=1148 msg="Match policy routing id=2130903043: to 10.0.2.101 via
ifindex-22"
...
id=20085 trace_id=5 func=ipsecdev_hard_start_xmit line=662 msg="enter IPSec interface HUB1-VPN3, tun_id=0.0.0.0"
id=20085 trace_id=5 func=_do_ipsecdev_hard_start_xmit line=222 msg="output to IPSec tunnel HUB1-VPN3, tun_id=172.16.1.5,
vrf 0"
branch1_fgt # diagnose firewall proute list
...
id= 2130903043(0x7f030003) vwl_service=3(Corp) vwl_mbr_seq=3 5 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00
protocol=0 port=src(0->0):dst(0->0) iif=0(any) path(2): oif=20(HUB1-VPN1) path_last used=2024-07-25 02:37:11,
oif=22(HUB1-VPN3) path_last_used=2024-07-25 02:42:55...
```

- SD-WAN rule ID 3 is matched, but HUB1-VPN3 is used
  - Seems that HUB1-VPN1 is skipped

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 11

If you repeat the ping test, you can see that FortiGate routes the traffic over HUB1-VPN3. If you run a debug flow, you can see that the traffic matches a policy route. The policy route corresponds to the SD-WAN rule ID 3, based on the policy route table output.

Even though the traffic now matches the expected SD-WAN rule (ID 3), FortiGate routes the traffic to HUB1-VPN3, instead of HUB1-VPN1. Therefore, it seems that FortiGate skips HUB1-VPN1 during the rule lookup process.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Routing Table and Static Routes

- Routing table:

```
branch1_fgt # get router info routing-table all
...
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
S       10.0.0.0/8 [1/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
```

No routes over HUB1-VPN1

- Static route configuration:

**Network > Static Routes**

| Destination | Gateway IP | Interface | Status |
|---|---|---|---|
| 10.0.0.0/8 | | overlay | Enabled |
| 172.16.0.0/16 | 172.16.0.2 | port4 | Enabled |
| 0.0.0.0/0 | | underlay | Enabled |

Static route references the **overlay** zone

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 12

If you view the routing table on the FortiGate CLI, you can see that there are no routes to `10.0.2.101` over HUB1-VPN1. In fact, there are no routes over HUB1-VPN1. If you check the configured static routes, you can see that the route that matches the destination references the overlay zone.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

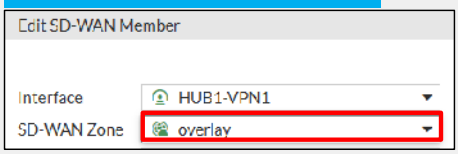
# Exercise 1—SD-WAN Zones

- SD-WAN zones:

```
branch1_fgt # diagnose sys sdwan zone
Zone overlay index=3
         members(1): 22(HUB1-VPN3)
Zone underlay index=2
         members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
         members(1): 20(HUB1-VPN1)
```

- Root cause: HUB1-VPN1 doesn't have a valid route to the destination
  - HUB1-VPN1 is not a member of the `overlay` zone
  - HUB1-VPN1 is skipped
- Solution: Move HUB1-VPN1 to the **overlay** zone

**Network > SD-WAN > SD-WAN Zones**




FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 13

If you check the SD-WAN zone diagnostic command, you can see that HUB1-VPN1 is a member of the default `virtual-wan-link` zone, instead of the `overlay` zone.

Because the static route references the `overlay` zone, but HUB1-VPN1 is not a member of that zone, FortiOS doesn't add the corresponding static route for HUB1-VPN1. Then, because HUB1-VPN1 doesn't have a valid route to the destination, FortiGate skips the member during the rule lookup process.

You can solve this issue by placing HUB1-VPN1 in the **overlay** zone.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Testing Member Selection (Contd)

- Routing table:

```
branch1_fgt # get router info routing-table all
...
S       10.0.0.0/8 [1/0] via HUB1-VPN1 tunnel 100.64.1.1, [1/0]
                   [1/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
...
```

Valid route to destination over HUB1-VPN1

- Ping branch2_client (10.0.2.101) from branch1_client (10.0.1.101)
- Sniff traffic on branch1_fgt:

```
2024-07-24 14:06:59.332990 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:06:59.333146 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:06:59.341167 HUB1-VPN1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 14:06:59.341196 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

  - Traffic is now routed to HUB1-VPN1

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 14

After you place HUB1-VPN1 in the **overlay** zone, you can see that the routing table now contains a route to the destination over HUB1-VPN1. If you repeat the test, you can see that the traffic is now routed over HUB1-VPN1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Testing Failover

- Run extended ping to branch2_client (10.0.2.101) from branch1_client (10.0.1.101)
- Sniff traffic on branch1_fgt
- port1 (BR1-ISP) is up, check sniffer:

```
2024-07-24 14:10:22.334962 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:22.335090 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:22.342919 HUB1-VPN1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 14:10:22.342967 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

  - Traffic is routed to HUB1-VPN1 (expected)
- Bring down port1 (BR1-ISP) using the WAN simulator and check the sniffer:

```
2024-07-24 14:10:36.386674 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:37.406708 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:37.406789 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:37.408639 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 14:10:37.408669 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 14:10:38.407970 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
```

  - Traffic fails over to HUB1-VPN3 (expected)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 15

You can test failover by running an extended ping to the destination while sniffing traffic on the FortiGate CLI. After you bring down port1 using the WAN simulator, you can see that traffic is now being routed over HUB1-VPN3.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 1—Testing Failback

- Bring port1 back up (BR1-ISP) using the WAN simulator and check the sniffer:

```
2024-07-24 14:10:46.418326 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:46.419584 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 14:10:46.419602 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2024-07-24 14:10:47.419802 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:47.419858 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2024-07-24 14:10:47.421946 HUB1-VPN1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

  - Traffic fails back to HUB1-VPN1 (expected)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 16

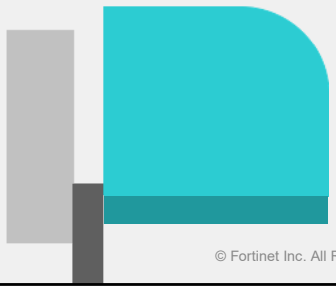
You can test failback by bringing port1 back up, and then looking at the sniffer output. You can see that traffic is being routed over HUB1-VPN1 again.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Troubleshooting DIA Traffic



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 2—Issue 1—Description

- Issue 1:
  - If both port1 and port2 are alive, non-critical internet traffic is load balanced across port1 and port2
- Expected behavior:
  - port2 is used only if port1 is dead

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 18

The administrator has identified this issue— if both port1 and port2 are alive, and the administrator generates internet traffic, critical traffic is routed to port1, which is expected. However, non-critical traffic is load balanced across port1 and port2.

The administrator wants port2 to be used for internet traffic only if port1 is down.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 1—Confirmation

- Ping `8.8.8.8`, `8.8.4.4`, `4.2.2.3`, and `4.2.2.4` from branch1_client (`10.0.1.101`)
- Sniff traffic on branch1_fgt, and notice that some traffic is routed over port2:

```
2024-07-24 14:45:41.128669 port5 in 10.0.1.101 -> 4.2.2.3: icmp: echo request
2024-07-24 14:45:41.129065 port2 out 192.2.0.9 -> 4.2.2.3: icmp: echo request
2024-07-24 14:45:41.131183 port2 in 4.2.2.3 -> 192.2.0.9: icmp: echo reply
2024-07-24 14:45:41.131259 port5 out 4.2.2.3 -> 10.0.1.101: icmp: echo reply
```

- But port1 and port2 are alive, and the preferred member for non-critical traffic is port1:

**Network > SD-WAN > Performance SLAs**

| Name | Detect Server | Packet Loss | Latency | Jitter |
|---|---|---|---|---|
| Corp_HC | 198.18.1.1<br>198.18.1.2 | port1: 0.00%<br>port2: 0.00% | port1: 0.93ms<br>port2: 0.72ms | port1: 0.17ms<br>port2: 0.13ms |

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 19

You can confirm the issue by pinging the addresses shown on this slide from branch1_client, while at the same time running a sniffer on the FortiGate CLI.

You can see that, for some destinations, FortiGate routes ICMP packets over port2. However, when you check the health of port1 and port2, both members are alive. Therefore, FortiGate should route all internet traffic over port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 1—Troubleshooting

- Session details:

```
branch1_fgt # diagnose sys session list

session info: proto=1 proto_state=00 duration=13 expire=46 timeout=0 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=4
...
orgin->sink: org pre->post, reply pre->post dev=7->4/4->7 gwy=192.2.0.10/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:1252->4.2.2.3:8(192.2.0.9:61668)
hook=pre dir=reply act=dnat 4.2.2.3:61668->192.2.0.9:0(10.0.1.101:1252)
hook=post dir=reply act=noop 4.2.2.3:1252->10.0.1.101:0(0.0.0.0:0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=00000355 tos=ff/ff app_list=2000 app=24466 url_cat=0
rpdb_link_id=80000000 ngfwid=n/a
...
```

No reference to SD-WAN rule.
Traffic matches implicit SD-WAN rule (standard FIB routing)

- Routing table:

```
branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
...
```

Matching route is ECMP

- Root cause: Matching route is ECMP, and FortiGate load balances the traffic
- Solution: Break ECMP by increasing priority of port2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 20

If you view the session details for the internet traffic that is routed over port2, you can see that the traffic does not match the explicit SD-WAN rule. This means that FortiGate performs standard FIB routing for this traffic.

Then, if you check the routing table, you can see that there are ECMP default routes: one for port1 and another for port2. As a result, FortiGate load balances the internet traffic that matches the implicit rule.

You can solve this issue by breaking the ECMP default route, by increasing the priority of port2.



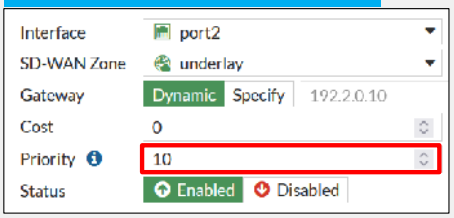
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 1—Increase the Priority of port2

- Set port2 priority to 10:

**Network > SD-WAN > SD-WAN Zones**




- Routing table:

```
branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [10/0]
```

port1 is now preferred for standard FIB routing

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 21

If you increase the member priority of port2 to 10, you can see a change in the routing table. The default routes are no longer ECMP routes, because port1 and port2 have different priorities. That is, port2 has a lower priority (higher number) than port1. The result is that FortiGate routes internet traffic over port1, because port1 has a higher priority.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 1—Testing

- Start a new ping session to 10.0.1.101 and sniff the traffic:

```
2023-01-04 15:06:50.586525 port5 in 10.0.1.101 -> 4.2.2.3: icmp: echo request
2023-01-04 15:06:50.587095 port1 out 192.2.0.1 -> 4.2.2.3: icmp: echo request
2023-01-04 15:06:50.589153 port1 in 4.2.2.3 -> 192.2.0.1: icmp: echo reply
2023-01-04 15:06:50.589238 port5 out 4.2.2.3 -> 10.0.1.101: icmp: echo reply
```

  - All internet traffic is now routed to port1 (no load balancing)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

If you repeat the test, you can see that all internet traffic, including non-critical traffic, is routed over port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Description

- Issue 2:
  - During a failover from port1 to port2 (port1 is dead), existing TCP sessions time out
  - For example, an SSH connection to the internet web server (`128.66.0.1`) from branch1_client times out during the failover
- Expected behavior:
  - Existing TCP sessions fail over to port2 successfully and not time out

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

There is another issue to troubleshoot. During a failover from port1 to port2 (port1 is dead), existing TCP sessions time out. For example, an SSH connection to the internet web server (`128.66.0.1`) from branch1_client times out during the failover.

The administrator wants existing TCP sessions to fail over to port2 successfully and do not time out.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Confirmation

- Connect to `128.66.0.1` over SSH from branch1_client (`10.0.1.101`), and log in with username `root` and password `password`

```
root@branch1-client-cli:~# ssh 128.66.0.1
Warning: Permanently added '128.66.0.1' (ECDSA) to the list of known hosts.
root@128.66.0.1's password:
...
root@www-webserver-lab:~#
```

- Bring down port1 (BR1-ISP) using the WAN simulator
- Check if the SSH connection responds to user commands
  - The SSH session is unresponsive

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

You can confirm the issue by connecting to `128.66.0.1` over SSH from branch1_client. Then, you can bring down port1 using the WAN simulator. After that, you can see that the SSH connection no longer responds to user commands.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Troubleshooting

- Bring port1 back up
- On branch1_client, restart the SSH connection, and log in to the web server
- On branch1_fgt, check the SSH session details:

```
session info: proto=6 proto_state=11 duration=44 expire=3557 timeout=3600 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3421/20/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 76/0 rx speed(Bps/kbps): 84/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:49262->128.66.0.1:22(192.2.0.1:49262)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:49262(10.0.1.101:49262)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:49262(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
rpdb_link_id=ff000002 ngfwid=n/a
npu_state=0x001108
```

- `may_dirty` flag is present
- Outgoing device is index `3` (port1)
- Outgoing gateway is `192.2.0.2` (port1)
- Matching firewall policy is `2`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 25

Bring port1 back up to repeat the test. After you connect to the web server over SSH, you can check the SSH session details on the FortiGate CLI.

You can see that the `may_dirty` flag is present, and that the outgoing device is the one with index `3`, which is port1. Although it is not shown on this slide, you can view the device index numbers in the output of the `diagnose netlink interface list` command.

You can also see that the outgoing gateway is `192.2.0.2`, which is the gateway that port1 uses, and that the matching firewall policy is `2`.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Troubleshooting (Contd)

- Bring down port1, and check the SSH session details:

```
session info: proto=6 proto_state=11 duration=352 expire=3249 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0
use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3421/20/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:49262->128.66.0.1:22(192.2.0.1:49262)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:49262(10.0.1.101:49262)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:49262(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
rpdb_link_id=ff000002 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008
```

- `dirty` flag is present
- Outgoing device is still index `3` (port1)
- Gateway information not yet updated

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 26

Continue troubleshooting by bringing down port1, and then checking the SSH session details again. In the output, you can see that the `dirty` flag is present.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Troubleshooting (Contd)

- Set up debug flow, and then check if SSH connection responds to user commands
  - SSH connection is unresponsive
- Observe the debug flow output:

```
id=20085 trace_id=1 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=6, 10.0.1.101:49262->128.66.0.1:22) from port5. flag [.], seq 3783503819, ack 3805876270, win 501"
id=20085 trace_id=1 func=resolve_ip_tuple_fast line=60030 msg="Find an existing session, id-000032d9, original direction"
id=20085 trace_id=1 func=rpdb_srv_match_input line=1148 msg="Match policy routing id=2130903042: to 128.66.0.1 via ifindex-4"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2605 msg="find a route: flag=00000000 gw-192.2.0.10 via port2"
id=20085 trace_id=1 func=get_new_addr line=1274 msg="find SNAT: IP-192.2.0.9(from IPPOOL), port-42614"
id=20085 trace_id=1 func=fw_strict_dirty_session_check line=264 msg="SNAT IP 192.2.0.1 != 192.2.0.9, drop"
id=20085 trace_id=2 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=6, 10.0.1.101:49262->128.66.0.1:22) from port5. flag [.], seq 3783503819, ack 3805876270, win 501"
id=20085 trace_id=2 func=rpdb_srv_match_input line=1148 msg="Match policy routing id=2130903042: to 128.66.0.1 via ifindex-4"
id=20085 trace_id=2 func=vf_ip_route_input_common line=1988 msg="find a route: flag=04000000 gw-192.2.0.10 via port2"
id=20085 trace_id=2 func=fw_forward_dirty_handler line=400 msg="no session matched"
```

- FortiGate:
  - Performs route lookup for the next packet (reevaluation, dirty flag)
  - Resolves to port2 as the new gateway, but drops the packet because its SNAT IP address changed
  - Clears the session and drops subsequent packets because they don't match an existing session

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 27

If you set up debug flow for the test traffic, and then you enter commands on the SSH test connection, you can see the following:

- FortiGate performs a route lookup for the next packet. This is because the session is flagged as dirty, as a result of a route change. This instructs FortiOS to reevaluate the session.
- FortiGate resolves to port2 as the new gateway. However, FortiGate drops the packet because the SNAT IP address on the packet changed. It was `192.2.0.1`, and now it is `192.2.0.9`.
- Because of the SNAT IP address change, FortiGate clears the session and drops subsequent packets, because they don't match an existing session.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Troubleshooting (Contd)

- Check the matching firewall policy configuration:

```
branch1_fgt # show firewall policy 2
config firewall policy
    edit 2
        set name "DIA"
        set uuid 96a6df1a-729a-51ec-089b-cba0021dd4d0
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set nat enable
    next
end
```

- Firewall policy references the `underlay` zone
- No IP pool, different SNAT IP address per member

- Root cause: No IP pool results in a different SNAT IP address per member
- Solution: Configure IP pool on firewall policy 2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 28

The matching firewall policy is `2`. If you check the firewall policy configuration, you can see that it references the `underlay` zone, but it doesn't have IP pool enabled. This means that FortiGate uses the IP address of the selected member in the `underlay` zone as the SNAT IP address. This explains why the SNAT IP address changed during the failover.

You can solve the issue by configuring an IP pool on firewall policy 2. The goal is for FortiGate to use the same SNAT IP address, regardless of the selected member.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Configure IP Pool

- View configured IP pools:

```
branch1_fgt # show firewall ippool
config firewall ippool
    edit "192.2.0.100"
        set startip 192.2.0.100
        set endip 192.2.0.100
    next
end
```

IP pool 192.2.0.100 has been preconfigured for you

- Apply IP pool on firewall policy 2:

```
config firewall policy
    edit 2
        set ippool enable
        set poolname "192.2.0.100"
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 29

If you view the configured IP pools, you can see that IP pool 192.2.0.100 has been preconfigured for you. The administrator wants FortiGate to SNAT internet traffic with the 192.2.0.100 IP address, so you must apply the IP pool on the firewall policy, as shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 2—Testing

- Bring port1 back up and repeat the test
- During failover, confirm that the SSH connection remains responsive, and then check the debug flow output:

```
id=20085 trace_id=59 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=6,
10.0.1.101:49608->128.66.0.1:22) tun_id=0.0.0.0 from port5. flag [.], seq 1331221955, ack 3504353634,
win 501"
id=20085 trace_id=59 func=resolve_ip_tuple_fast line=6030 msg="Find an existing session, id-000034bd,
original direction"
id=20085 trace_id=59 func=rpdb_srv_match_input line=1148 msg="Match policy routing id=2130968578: to
128.66.0.1 via ifindex-4"
id=20085 trace_id=59 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-
192.2.0.10 via port2"
id=20085 trace_id=59 func=get_new_addr line=1274 msg="find SNAT: IP-192.2.0.100(from IPPOOL), port-
60445"
id=20085 trace_id=59 func=ids_receive line=328 msg="send to ips"
id=20085 trace_id=59 func=__ip_session_run_tuple line=3474 msg="SNAT 10.0.1.101->192.2.0.100:49608"
```

- FortiGate now forwards the packet out (no SNAT IP address change error)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 30

Bring port1 back up, and then repeat the test. This time, you can see that the SSH connection remains responsive during the failover. Also, the debug flow no longer shows the SNAT IP address change error, which means that FortiGate is forwarding the packets successfully.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 2—Issue 3—Description

- Issue 3:
  - After existing sessions fail over to port2 successfully, sessions don't fail back to port1 after port1 recovers
- Expected behavior:
  - Sessions fail back to port1 after port1 recovers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 31

There is another issue to troubleshoot. After existing sessions fail over to port2 successfully, the sessions don't fail back to port1, after port1 recovers.

The administrator wants the sessions to fail back to port1 after port1 recovers.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 3—Confirmation

- Bring port1 back up, and repeat the test of issue 2
- Confirm the SSH connection fails over to port2 successfully
- Bring port1 back up, and then test the SSH connection while sniffing SSH traffic:

```
5.244388 port5 in 10.0.1.101.49608 -> 128.66.0.1.22: psh 1331222171 ack 3504354210
5.244739 port2 out 192.2.0.100.49608 -> 128.66.0.1.22: psh 1331222171 ack 3504354210
5.253437 port2 in 128.66.0.1.22 -> 192.2.0.100.49608: psh 3504354210 ack 1331222207
```

  - SSH connection is still responsive, but FortiGate continues to forward packets to port2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 32

You can confirm the issue by bringing port1 up, and then repeating the test you used for issue 2. You can confirm that the SSH connection fails over to port2 successfully. Then, if you bring port1 back up, the SSH connection continues to respond to user commands. However, if you sniff the SSH traffic, you can see that FortiGate continues to route the traffic to port2, instead of routing it to port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 3—Troubleshooting

- Repeat the test
- Check the SSH session after you bring port1 back up:

```
session info: proto=6 proto_state=11 duration=21 expire=3586 timeout=3600 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=4077/28/1 reply=4517/22/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->4/4->7 gwy=192.2.0.10/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:49858->128.66.0.1:22(192.2.0.100:49858)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:49858(10.0.1.101:49858)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:49858(0.0.0.0:0)
...
```

- The `dirty` flag is present
- However, the gateway info is not flushed
- Gateway address will not be updated

- Root cause: By default, FortiOS doesn't change routing information of SNAT sessions, unless existing gateway is no longer valid
- Solution: Enable `snat-route-change` setting

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 33

You troubleshoot the issue by repeating the test, and then checking the SSH session details after bringing port1 back up—that is, during failback. The SSH session shows the dirty flag, but the gateway information is not flushed. That is, FortiGate does not update the gateway information for this session.

The reason is that, by default, FortiOS doesn't change the routing information of SNAT sessions, unless their existing gateway is no longer valid, which is not the case here. That is, port2, which is the device that the session uses to reach the current gateway, is still up and so are the respective routes.

You can solve this issue by enabling the `snat-route-change` setting. When you enable this setting, FortiGate refreshes the routing information of SNAT sessions, following a routing change that impacts the sessions.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 2—Issue 3—Enable snat-route-change

- Enable `snat-route-change` setting:

```
config system global
    set snat-route-change enable
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 34

You can enable the `snat-route-change` setting by entering the commands shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 3—Testing

- Repeat the test
- Check the SSH session after you bring port1 back up:

```
session info: proto=6 proto_state=11 duration=37 expire=3570 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0
use=4
...
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=4477/35/1 reply=4925/28/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->4/4->7 gwy=192.2.0.10/0.0.0.0
...
```

- The `dirty` flag is present
- Gateway address can be updated

- Test the SSH connection, and confirm that it remains up
- Check the SSH session again:

```
session info: proto=6 proto_state=11 duration=289 expire=3597 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0
use=4
...
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=5705/54/1 reply=6273/42/1 tuples=3
tx speed(Bps/kbps): 8/0 rx speed(Bps/kbps): 9/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/10.0.1.101
...
```

- The `dirty` flag was removed
- The outgoing device was updated (port1)
- The outgoing gateway was updated (port1)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 35

If you repeat the test, you can see that FortiOS now flushes the gateway information during the failback. The result is that FortiGate updates the gateway information, so it uses port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 3—Testing (Contd)

- Test the SSH connection while sniffing SSH traffic:

```
2.715688 port5 in 10.0.1.101.50374 -> 128.66.0.1.22: psh 56438236 ack 1749555534
2.715943 port1 out 192.2.0.100.50374 -> 128.66.0.1.22: psh 56438236 ack 1749555534
2.716672 port1 in 128.66.0.1.22 -> 192.2.0.100.50374: ack 56438272
```

  - Traffic fails back to port1

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 36

If you also sniff the SSH traffic during the failback, you can see that FortiGate is routing packets to port1 again.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 2—Issue 4—Description

- Issue 4:
  - When port1 is dead, and new sessions are established through port2, the sessions don't fail over to port1 after port1 recovers—they continue to use port2
- Expected behavior:
  - Sessions fail over to port1 after port1 recovers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 37

There is one last issue to troubleshoot in this exercise. When port1 is dead, and new sessions are established through port2, the sessions don't fail over to port1, after port1 recovers. That is, the sessions continue to use port2.

The administrator wants these sessions to fail over to port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 4—Confirmation

- Bring down port1
- Connect to `128.66.0.1` over SSH from branch1_client (`10.0.1.101`)
- Sniff SSH traffic to confirm packets are routed over port2:

```
1.527331 port5 in 10.0.1.101.50552 -> 128.66.0.1.22: syn 1461883675
1.528100 port2 out 192.2.0.100.50552 -> 128.66.0.1.22: syn 1461883675
```

- Bring port1 back up, and then test the SSH connection while sniffing SSH traffic:

```
115.083422 port5 in 10.0.1.101.50552 -> 128.66.0.1.22: psh 1461885277 ack 2970972072
115.083928 port2 out 192.2.0.100.50552 -> 128.66.0.1.22: psh 1461885277 ack 2970972072
```

  - FortiGate continues to route packets over port2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 38

Confirm the issue by bringing down port1, and then connecting to the web server over SSH. Sniff the SSH traffic to confirm that packets are routed over port2. Then, bring port1 back up, and test the SSH connection. The SSH connection works, but FortiGate continues to route the packets over port2, instead of routing them over port1 again.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 4—Troubleshooting

- Repeat the test, and then check the SSH session before you bring port1 back up:

```
session info: proto=6 proto_state=11 duration=9 expire=3594 timeout=3600 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty ndr f00 app_valid route_preserve
...
```

- The `route_preserve` flag is present
- Interface stickiness is enabled
- Gateway address will not be updated

- Check port2 configuration:

```
branch1_fgt # show system interface port2
config system interface
    edit "port2"
...
        set preserve-session-route enable
...
```

- Root cause: Interface stickiness is enabled on port2, and gateway address is not updated unless existing gateway is no longer valid
- Solution: Disable `preserve-session-route` setting on port2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 39

To troubleshoot this issue, repeat the test. Check the SSH session details before you bring port1 back up (failback event). In the session, the `route_preserve` flag is present. That is, interface stickiness is enabled on the outgoing interface—port2, in this case. The result is that the gateway address will not be updated, unless the existing gateway is no longer valid, which is not the case.

If you check the port2 configuration, you can see that the `preserve-session-route` setting is enabled. You can solve the issue by disabling the setting on port2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 4—Disable Interface Stickiness

- Disable interface stickiness on port2:

```
config system interface
    edit "port2"
        set preserve-session-route disable
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

You can disable the `preserve-session-route` setting on port2 by entering the commands shown on this slide.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 2—Issue 4—Testing

- Repeat the test, and then check the SSH session before you bring port1 back up:

```
session info: proto=6 proto_state=11 duration=14 expire=3595 timeout=3600 refresh_dir=both
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty ndr f00 app_valid
...
```

- `route_preserve` flag is not present

- Bring port1 back up, test the SSH connection, and then sniff the traffic to confirm packets are routed over port1:

```
1.030673 port5 in 10.0.1.101.50746 -> 128.66.0.1.22: psh 931097527 ack 721063059
1.030838 port1 out 192.2.0.100.50746 -> 128.66.0.1.22: psh 931097527 ack 721063059
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 41

If you repeat the test, you can no longer see the `route_preserve` flag in the session. The result is that FortiGate can now update the gateway information during the failover to port1. Therefore, FortiGate routes the SSH traffic over port1 again.

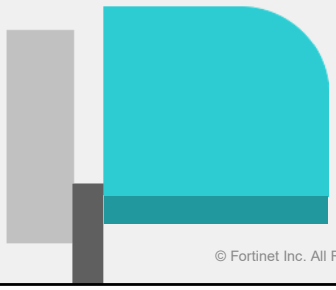
Note that, even if FortiGate now sends the packets through port1, you may see replies coming in on port2. This is because the server connects to a router with no SD-WAN capabilities. This router sends the reply packets through any of its valid interfaces.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Troubleshooting Rules



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 3—Issue 1—Description

- Issue 1:
  - If port1 is up, internet traffic on branch1_fgt is successfully routed over port1
  - If port1 is down, internet traffic is dropped
- Expected behavior:
  - If port1 is down, internet traffic fails over to the overlays (RIA)
    - Overlays: HUB1-VPN2 and HUB1-VPN3

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 43

The administrator identified the following issue: If port1 is down, branch1_fgt drops internet traffic from branch1_client. However, the administrator wants internet traffic to fail over to the overlays to perform remote internet access (RIA). The overlays are HUB1-VPN2 and HUB1-VPN3.

Note that, if port1 is up, internet traffic on branch1_fgt is routed successfully over port1.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 3—Issue 1—Confirmation

- Ping `8.8.8.8` from branch1_client (`10.0.1.101`) and sniff the traffic:

```
2023-01-06 07:34:08.479281 port5 in 10.0.1.101 -> 8.8.8.8: icmp: echo request
2023-01-06 07:34:08.480259 port1 out 192.2.0.1 -> 8.8.8.8: icmp: echo request
2023-01-06 07:34:08.481387 port1 in 8.8.8.8 -> 192.2.0.1: icmp: echo reply
2023-01-06 07:34:08.481725 port5 out 8.8.8.8 -> 10.0.1.101: icmp: echo reply
```

  - You can ping the address, and the sniffer shows that the traffic is routed over port1

- Bring down port1, and repeat the test:

```
2023-01-06 08:00:34.881429 port5 in 10.0.1.101 -> 8.8.8.8: icmp: echo request
2023-01-06 08:00:35.902681 port5 in 10.0.1.101 -> 8.8.8.8: icmp: echo request
```

  - You can't ping the address
  - The sniffer shows that FortiGate drops the packets

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 44

You can confirm the issue by pinging `8.8.8.8` from branch1_client, while at the same time running a sniffer on the FortiGate CLI.

You will see that when port1 is up, FortiGate routes the ICMP packets over port1, which is the expected behavior. However, when port1 is down, FortiGate drops the packets, instead of routing them over the overlays.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 3—Issue 1—Troubleshooting—Routing Table

- Bring down port1, and then check the routing table:

```
branch1_fgt # get router info routing-table all
...
Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 192.2.0.10, port2, [1/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 10.202.1.254 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 00:17:00, [1/0]
                    [200/0] via 10.203.1.254 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 00:17:00, [1/0]
C       10.202.1.0/24 is directly connected, HUB1-VPN2
C       10.202.1.1/32 is directly connected, HUB1-VPN2
S       10.202.1.254/32 [15/0] via HUB1-VPN2 tunnel 100.64.1.9, [1/0]
C       10.203.1.0/24 is directly connected, HUB1-VPN3
C       10.203.1.1/32 is directly connected, HUB1-VPN3
S       10.203.1.254/32 [15/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
S       100.64.1.9/32 [10/0] via 192.2.0.10, port2, [1/0]
..
```

- The default static route is through port2—it has a priority of 5
- A priority 5 static route is automatically defined for each DHCP interface, uses the gateway the DHCP server defined for the interface

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 45

FortiGate has a route to the destination through port2, however the traffic does not get through.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 3—Issue 1—Troubleshooting—Debug Flow

- Bring down port1, launch the ping to 8.8.8.8, and then check the debug flow:

```
branch1_fgt # diagnose debug enable

branch1_fgt # diagnose debug flow filter addr 8.8.8.8

branch1_fgt # diagnose debug flow trace start 10

branch1_fgt # id=65308 trace_id=41 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=17,
10.0.1.100:33563->8.8.8.8:53) tun_id=0.0.0.0 from port5. "
id=65308 trace_id=41 func=init_ip_session_common line=6127 msg="allocate a new session-00000a70"
id=65308 trace_id=41 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-192.2.0.10 via port2"
id=65308 trace_id=41 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=60, len=1"
id=65308 trace_id=41 func=fw_forward_handler line=839 msg="Denied by forward policy check (policy 0)"
id=65308 trace_id=42 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=17, 10.0.1.100:46557-
>8.8.8.8:53) tun_id=0.0.0.0 from port5. "
id=65308 trace_id=42 func=init_ip_session_common line=6127 msg="allocate a new session-00000a72"
id=65308 trace_id=42 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-192.2.0.10 via port2"
id=65308 trace_id=42 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=60, len=1"
id=65308 trace_id=42 func=fw_forward_handler line=839 msg="Denied by forward policy check (policy 0)"
id=65308 trace_id=43 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=17, 10.0.1.100:36698-
>8.8.8.8:53) tun_id=0.0.0.0 from port5. "
...
```

- FortiGate doesn’t have a policy that allows the flow

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 46

FortiGate has a route to the destination through port2, however it doesn’t have a policy to allow this traffic flow.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 1—Troubleshooting—Firewall Policies

- Check the firewall policies:

```
branch1_fgt # show firewall policy
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set nat enable
    next
...
```

- FortiGate has a policy that allows this traffic through the underlay SD-WAN zone

- Check the SD-WAN zone configuration:

```
branch1_fgt # diagnose sys sdwan zone
Zone overlay index=3
        members(2): 21(HUB1-VPN2) 22(HUB1-VPN3)
Zone underlay index=2
        members(1): 3(port1)
Zone virtual-wan-link index=1
        members(2): 4(port2) 20(HUB1-VPN1)
```

- port2 is not a member of the underlay zone

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 47

FortiGate has a policy that allows traffic through the underlay zone. The ping to `8.8.8.8` matches the source address, destination address, and protocol of this policy. However, the destination interface of this policy is the underlay zone and port2 is not a member of this zone.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 3—Issue 1—Root Causes and Solution

- Root causes
  - FortiGate cannot route the traffic through port2 because it doesn't have a policy to allow it
  - FortiGate cannot route the traffic through the overlay zone because it doesn't have a route to allow it
- Solution
  - Add a static default route through the overlay zone
  - Adjust the route distance with the following constraints:
    - Must be below the distance of the static default route through DHCP interface port2 (default distance 5)
    - Must be above the distance of the static route through the underlay zone (default distance 1)

```
config router static
    edit 6
        set distance 4
        set sdwan-zone "overlay"
    next
end
```

- Comments
  - Adding port2 to the underlay zone would allow the flow through port2, but it is not the desired behavior

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 48

The root causes for this issue are that FortiGate cannot route the traffic through port2 because it doesn't have a policy to allow such a flow. FortiGate cannot route the traffic through the overlay zone because it doesn't have a route to `8.8.8.8`, and no default route, through the overlay zone.

A simple solution would be to add port2 to the underlay zone. In that configuration, when port1 is down, FortiGate will reroute the traffic through port2. However, this is not the behavior that the administrator wants.

To reroute the internet traffic through the overlay zone when port1 is down, you must add a default route through the overlay zone. When doing this, you must pay attention to another constraint: when port1 is up, FortiGate should not load balance the traffic through port1 and the overlay links. You can achieve this by creating a static route through the overlay zone with a distance that is higher than the existing default routes.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 1—Testing

- Repeat the test and sniff the traffic:

```
2024-08-01 01:49:47.484635 port5 in 10.0.1.101 -> 8.8.8.8: icmp: echo request
2024-08-01 01:49:47.484653 HUB1-VPN2 out 192.2.0.1 -> 8.8.8.8: icmp: echo request
2024-08-01 01:49:48.504658 port5 in 10.0.1.101 -> 8.8.8.8: icmp: echo request
2024-08-01 01:49:48.504682 HUB1-VPN2 out 192.2.0.1 -> 8.8.8.8: icmp: echo request
```

  - FortiGate routes the traffic over the HUB1-VPN2 overlay

- Session details:

```
session info: proto=1 proto_state=00 duration=139 expire=59 timeout=0 refresh_dir=both flags=00000000 socktype=0
...
state=log may_dirty f00 app_valid
statistic(bytes/packets/allow_err): org=11592/138/1 reply=2100/25/1 tuples=3
tx speed(Bps/kbps): 82/0 rx speed(Bps/kbps): 15/0
orgin->sink: org pre->post, reply pre->post dev=7->21/3->7 gwy=100.64.1.9/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:421->8.8.8.8:8(192.2.0.1:60838)
hook=pre dir=reply act=dnat 8.8.8.8:60838->192.2.0.1:0(10.0.1.101:421)
hook=post dir=reply act=noop 8.8.8.8:421->10.0.1.101:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=15836 auth_info=0 chk_client_info=0 vd=0
serial=0000118f tos=ff/ff app_list=2000 app=24466 url_cat=0
sdwan_mbr_seq=4 sdwan_service_id=2
...
```

  - Connection matches SD-WAN rule ID 2 and member ID 4 (HUB1-VPN2)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

If you repeat the test, you will see that FortiGate routes the ICMP packets over HUB1-VPN2, which is the expected behavior when port1 is down.

Session information shows that the traffic matches SD-WAN rule ID 2 and member ID 4. Both correspond to HUB1-VPN2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 1—Testing (Contd)

- Check the routing table when all interfaces are up:

```
branch1_fgt # get router info routing-table all
...
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 10.202.1.254 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 01:29:03, [1/0]
                    [200/0] via 10.203.1.254 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 01:29:03, [1/0]
C       10.202.1.0/24 is directly connected, HUB1-VPN2
C       10.202.1.1/32 is directly connected, HUB1-VPN2
...
```

  - Only one default route, through port1

- Check the routing table when port1 is down:

```
branch1_fgt # get router info routing-table all
...
Routing table for VRF=0
S*      0.0.0.0/0 [4/0] via HUB1-VPN2 tunnel 100.64.1.9, [1/0]
                  [4/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
C       10.0.1.0/24 is directly connected, port5
...
```

  - ECMP default routes through the overlay members

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 50

Confirm that when port1 is up, the only default route available is through port1. When port1 is down, the ECMP default routes direct the traffic through the interfaces of the overlay zone. In this example, the administrator set a distance of 4. You can choose any value above 1—the default distance for default routes through SD-WAN zones—and below 5—the default distance for default routes through DHCP interfaces.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

## Exercise 3—Issue 2—Description

- Expected behavior:
  - For traffic that matches rule ID 1, branch1_fgt prefers the member with the best route to the destination
  - Goal: Control member preference by advertising, from dc1_fgt, a better route over a preferred overlay
    - You can't change the rule mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

The last task is to fulfill a request by the administrator. The administrator wants branch1_fgt to prefer the member with the best route to the destination. This way, the administrator can control the member preference by advertising a better route, over its preferred overlay, from dc1_fgt, without having to change the configuration on the branch.

Remember that you can't change the rule mode, which is currently set to manual.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 2—Confirmation

- SD-WAN rule ID 1 and overlay zone tiebreaker configuration:

```
branch1_fgt # config system sdwan

branch1_fgt (sdwan) # config service

branch1_fgt (service) # edit 1

branch1_fgt (1) # get | grep tie-break
tie-break           : zone

branch1_fgt (1) # end

branch1_fgt (sdwan) # config zone

branch1_fgt (zone) # edit overlay

branch1_fgt (overlay) # get | grep service-sla-tie-break
service-sla-tie-break: cfg-order
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

You can confirm the issue by checking the rule or zone configuration. By default, rules use the member priority as the first tiebreaker. That is, they use the order of the interface preference list, as the first tiebreaker in all applicable rules, which includes manual mode rules.

The setting that controls the first tiebreaker on the rule level is `tie-break`. By default, it is set to `zone`, which means that it follows the zone-level setting. The zone-level setting, `service-sla-tie-break`, is set to `cfg-order` (member priority).



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 2—Set Tiebreaker to Best Route

- Set the tiebreaker to the best route at the rule level:

```
config system sdwan
    config service
        edit 1
            set tie-break fib-best-match
        next
    end
end
```

  - Usually, it's better to change the setting at the rule level, to minimize impact

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 53

The example on this slide shows how to change the tiebreaker to the best route at the rule level. Usually, it's better to change this setting at the rule level so that only the rule in question is impacted. If you make the change at the zone level, it will impact all the rules that reference the zone.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 2—Testing

- Route lookup for `10.1.0.7`:

```
branch1_fgt # get router info routing-table details 10.1.0.7

Routing table for VRF=0
Routing entry for 10.1.0.0/24
  Known via "bgp", distance 200, metric 0, best
   Last update 00:20:50 ago
  * vrf 0 10.202.1.254 priority 1 (recursive via HUB1-VPN2 tunnel 100.64.1.9)
  * vrf 0 10.203.1.254 priority 1 (recursive via HUB1-VPN3 tunnel 172.16.1.5)
```

  - Both routes are the best ones (ECMP)

- View SD-WAN rule ID 1 status:

```
branch1_fgt # diagnose sys sdwan service4
...
    1: Seq_num(4 HUB1-VPN2), alive, selected
    2: Seq_num(5 HUB1-VPN3), alive, selected
...
```

  - HUB1-VPN2 wins because it has a higher member priority

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 54

To test the solution, you can first perform a route lookup for the destination (`10.1.0.7`). FortiOS should report that both members have ECMP routes. This means that both members have equally good routes. Because of this, FortiOS will use the member priority as a tiebreaker to identify the preferred member, which in this case is HUB1-VPN2.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 2—Testing (Contd)

- Ping `10.1.0.7` from branch1_client and sniff the traffic:

```
2024-08-01 15:03:07.854051 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
2024-08-01 15:03:07.854168 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
2024-08-01 15:03:07.855574 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
2024-08-01 15:03:07.855590 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

  - FortiGate routes traffic over HUB1-VPN2

- Apply the following configuration on dc1_fgt to test best route as tiebreaker:

```
config router bgp
   config neighbor-group
      edit Branches_VPN3
          set route-map-out prefer-dc1_host
      next
   end
end
# execute router clear bgp all soft
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 

If you ping `10.1.0.7` from branch1_client while sniffing the traffic, you can confirm that FortiGate routes the packets over HUB1-VPN2.

The lab instructions indicate that you should apply the configuration shown on this slide to test the best route as a tiebreaker. After that, you must soft clear all BGP peerings so that the configuration takes effect.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

# Exercise 3—Issue 2—Testing (Contd)

- Route lookup for `10.1.0.7` and routing table:

```
branch1_fgt # get router info routing-table details 10.1.0.7
...
  * vrf 0 10.203.1.254 priority 1 (recursive via HUB1-VPN3 tunnel 172.16.1.5)

branch1_fgt # get router info routing-table all
...
B       10.1.0.0/24 [200/0] via 10.202.1.254 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 00:28:07, [1/0]
                    [200/0] via 10.203.1.254 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 00:28:07, [1/0]
B       10.1.0.7/32 [200/0] via 10.203.1.254 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 00:02:00, [1/0]
...
```

  - Both HUB1-VPN2 and HUB1-VPN3 have a valid route, but best route is over HUB1-VPN3

- Ping `10.1.0.7` from branch1_client and sniff the traffic:

```
2023-01-06 15:10:56.076849 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
2023-01-06 15:10:56.077000 HUB1-VPN3 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
2023-01-06 15:10:56.078056 HUB1-VPN3 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
2023-01-06 15:10:56.078348 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

  - HUB1-VPN3 is now used (best route)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 56

After making the changes indicated in the lab instructions on dc1_fgt, you can perform another route lookup. You will now see that the best route to the destination is over HUB1-VPN3. Note that both members have a valid route to the destination, but HUB1-VPN3 has the best one.

When you ping `10.1.0.7` again, you will see that FortiGate now routes the packets over HUB1-VPN3, because HUB1-VPN3 has the best route.



Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com




Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FORTINET

**No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.**

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923