DO NOT REPRINT
© FORTINET
Braindumps.com

Enterprise Firewall Study Guide

for FortiOS 7.2

FORTINET
Training Institute

Vouchers & Dumps are Available | WhatsApp +2348138183833

DO NOT REPRINT Brave-dumps.com
© FORTINET

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

FORTINET

5/4/2023

Vouchers & Dumps are Available | WhatsApp +201224560923

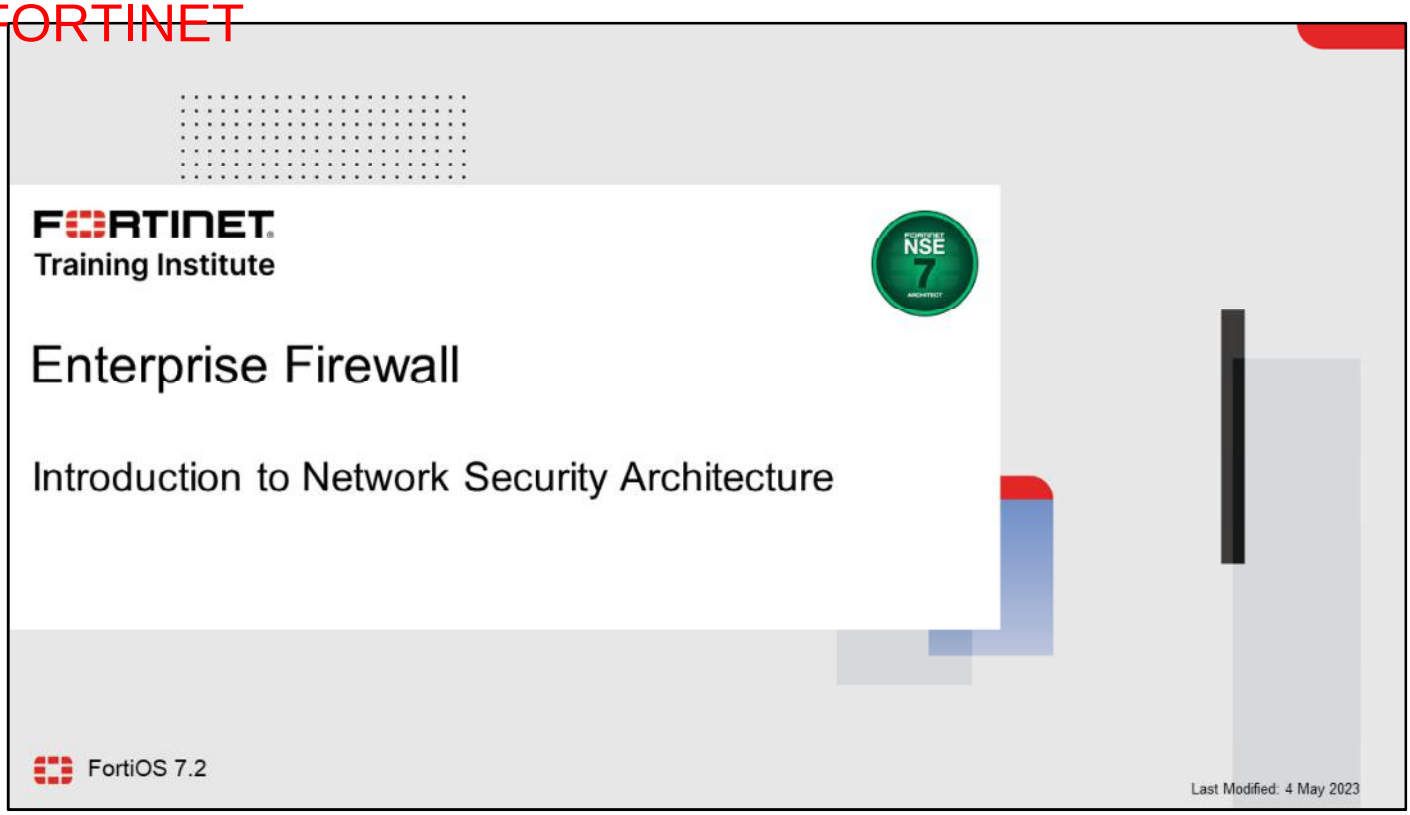
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Introduction to Network Security Architecture 4
02 Hardware Acceleration 30
03 Security Fabric 59
04 High Availability 90
05 Central Management 129
06 OSPF 163
07 Border Gateway Protocol 189
08 FortiGuard and Security Profiles 215
09 Intrusion Prevention System 260
10 IPsec 290
11 Auto-Discovery VPN 325
Dynamic Routing Supplement 349

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the architecture of FortiOS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Describe the enterprise firewall solution
- Explain the network security reference architecture and the Fortinet products it comprises
- Describe the roles of firewalls and their placement in the network
- Understand FortiOS workspace mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating competence in Fortinet network security architecture, you will be able to understand the enterprise firewall solution and the network security reference architecture, and the Fortinet products it comprises. You will be able to also understand the roles of firewalls and their placement in the network.

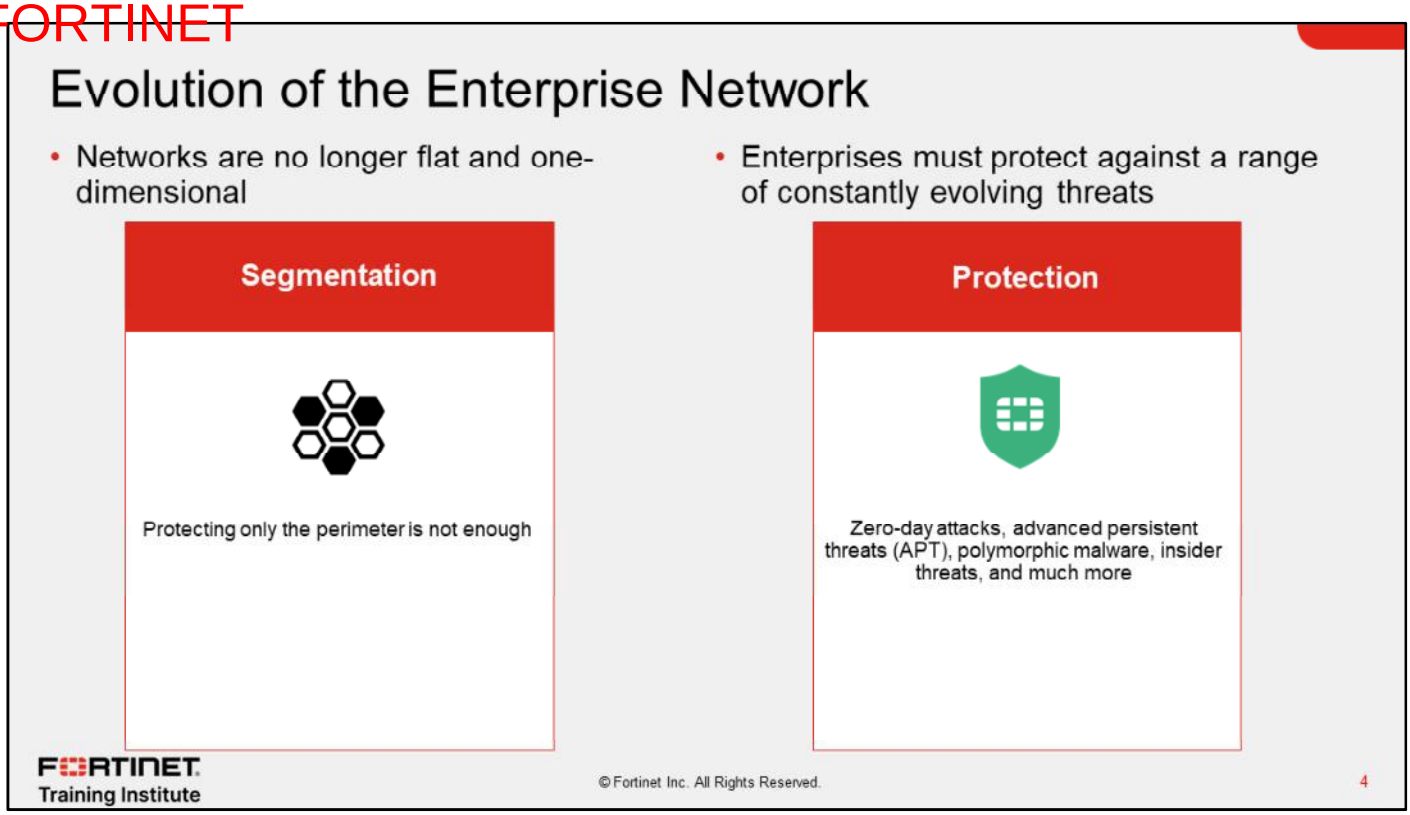
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

In this section, you will learn about the Fortinet enterprise firewall solution at a high level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

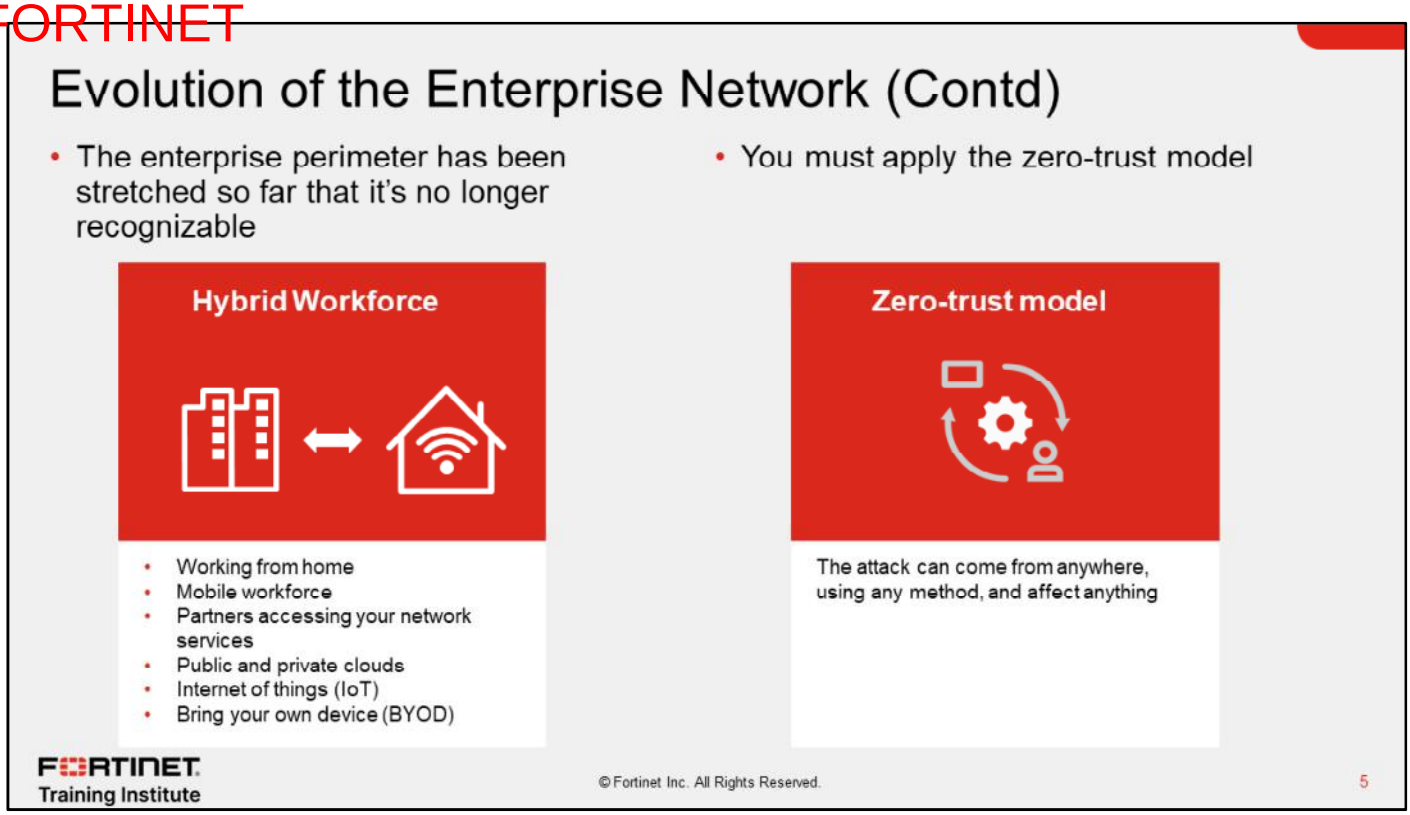


The traditional way of protecting a network by securing the perimeter has become a thing of the past. Network and security administrators today must protect against a wide range of threats such as zero-day attacks, APTs, polymorphic malware, and many more. They must also protect the network from any potential insider threats.

Malware can easily bypass any entry-point firewall and get inside the network. This could happen through an infected USB stick, or an employee's compromised personal device being connected to the corporate network. Additionally, network administrators can no longer take for granted that everything and everyone inside the network can be trusted. Attacks can now come from inside the network. To secure such a vast network, you must apply the zero-trust model. The attack can come from anywhere, using any method, and affect anything.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

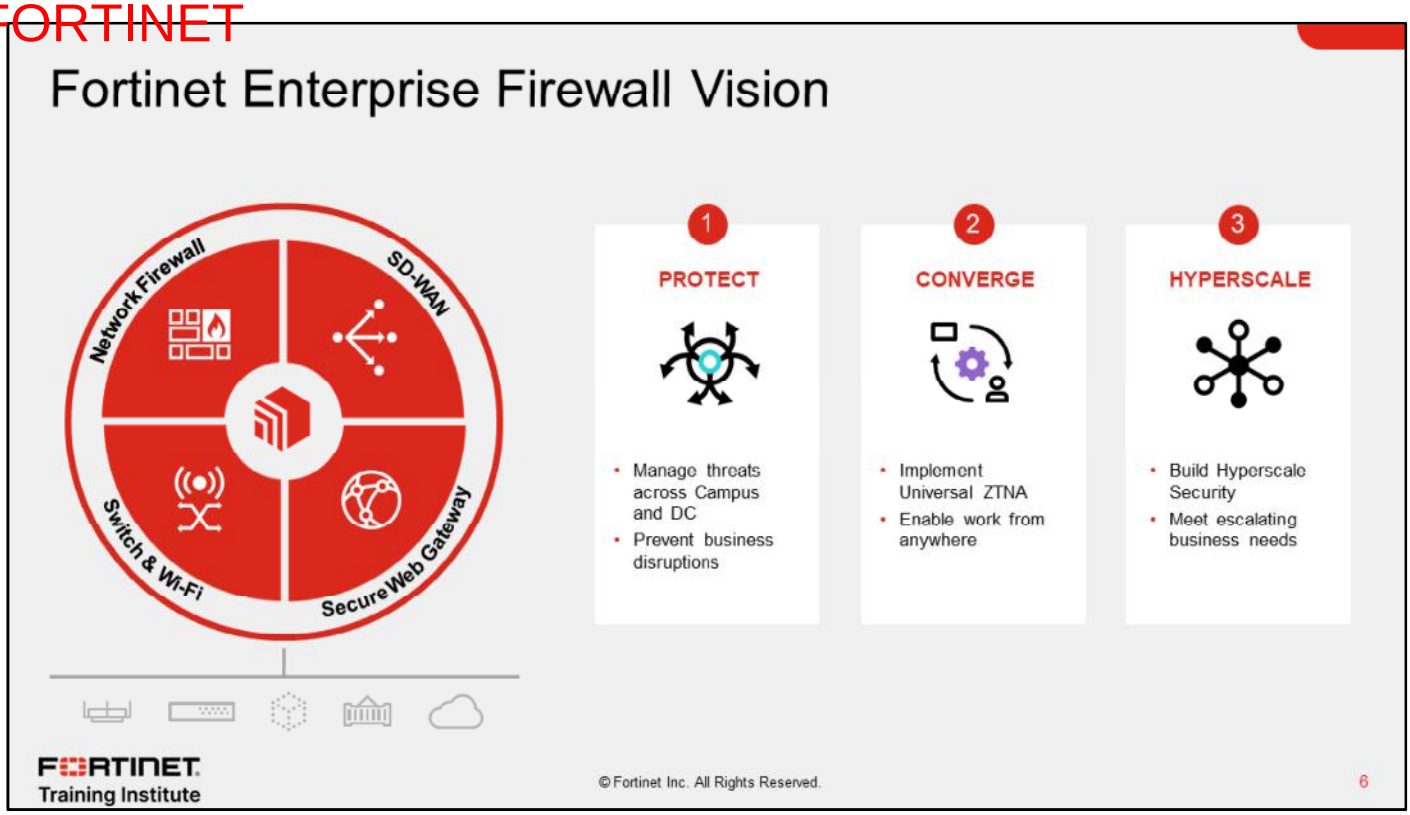


Working from home, BYOD, mobile users, a remote workforce, and evolving cloud technologies are creating borderless networks, which is further compounding the challenge of securing such complex networks.

Additionally, network administrators can no longer take for granted that everything and everyone inside the network can be trusted. Attacks can now come from inside the network. To secure such a vast network, you must apply the zero-trust model. The attack can come from anywhere, using any method, and affect anything.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

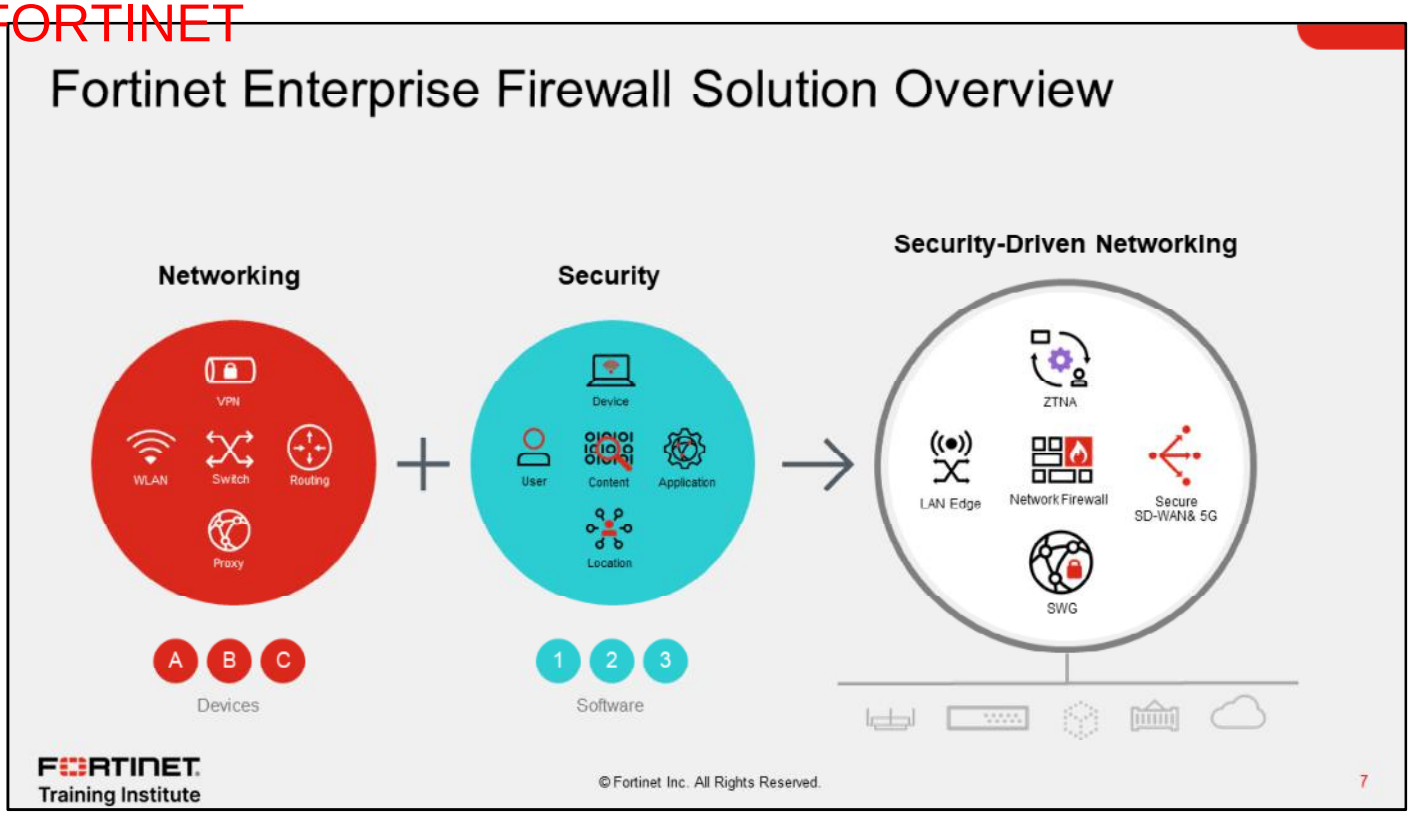


The Fortinet enterprise firewall comprises converged networking and security with a flexible deployment model through devices (security processing unit), virtual machines, containers, and SaaS.

The vision also includes a unified operating system with native integration of NGFW, SWG, SD-WAN, and ZTNA available across all network edges.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The Fortinet enterprise firewall solution answers networking and security challenges. It offers effective and fast end-to-end security with a consolidated operating system—FortiOS. The core of the solution is the Security Fabric, which enables the communication of all the security devices in an enterprise network. The Fortinet enterprise firewall solution offers guidelines about where to install your network security devices and what roles they'll have in each part of the enterprise network. You can deliver single-pane-of-glass management and reporting for all of the deployments across the enterprise using FortiManager and FortiAnalyzer, respectively.

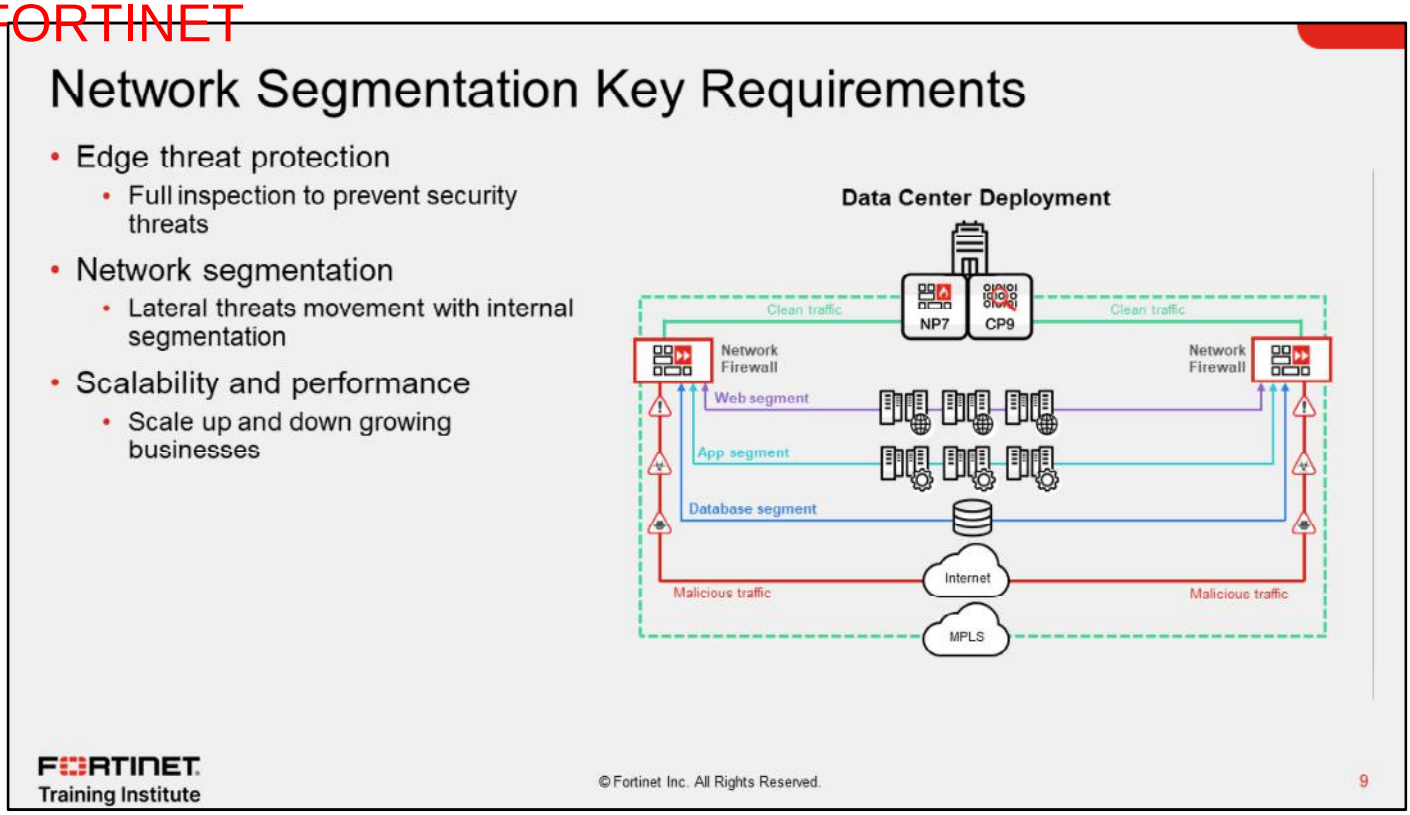
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

In this section, you will learn about the Fortinet network security reference architecture at a high level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



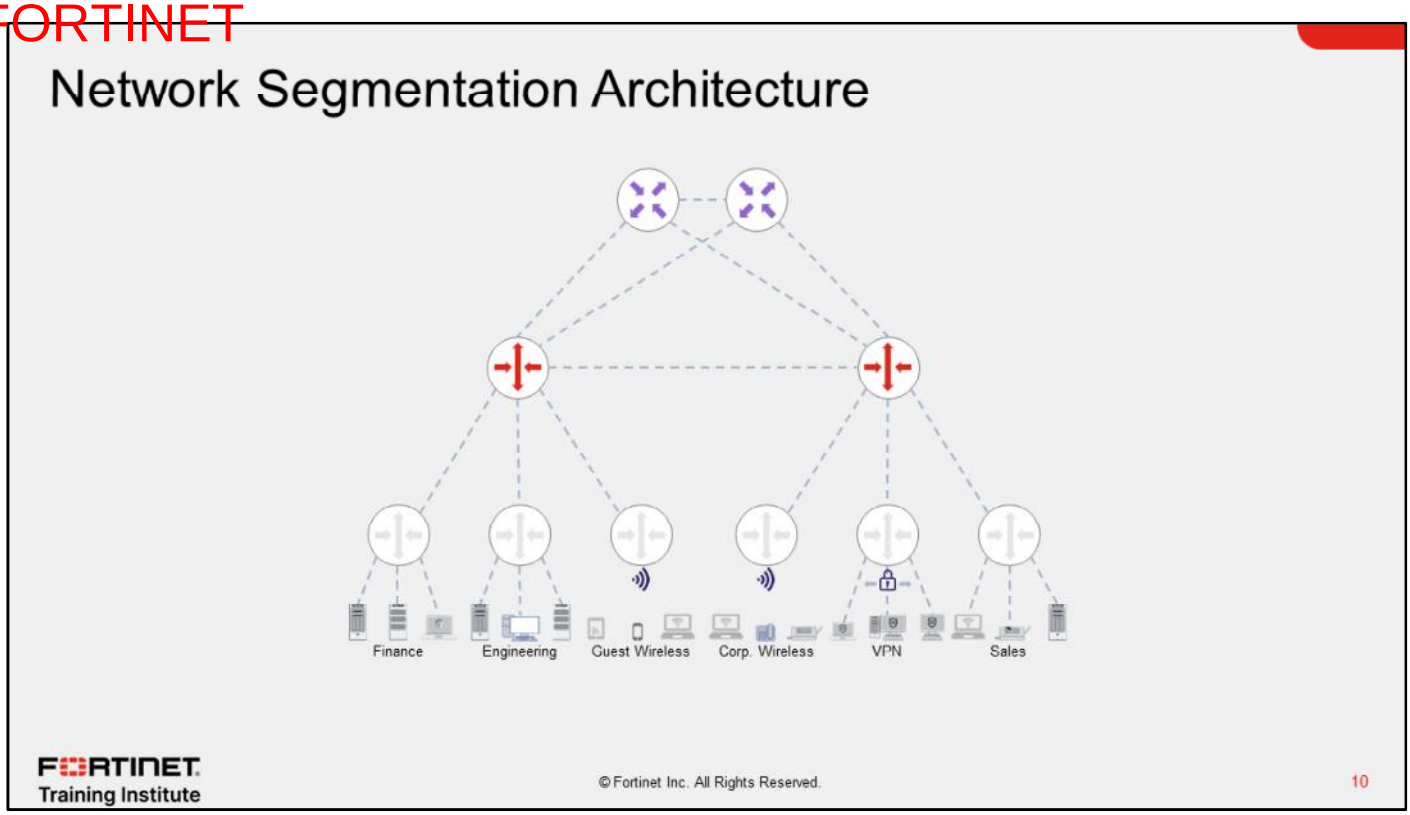
You can inspect all traffic for full visibility and to prevent known, zero-day, and unknown security threats using IPS and advanced security services to prevent business disruptions.

To prevent lateral movement of threats, you can manage the internal risks using internal segmentation. Enable explicit usage of applications with zero trust network access enforcement for any user to any application.

You can have the ability to scale up and down your business to meet growing business requirements, such as higher performance, concurrent connections and high availability for data-center protection. Automate all enterprise workflows.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



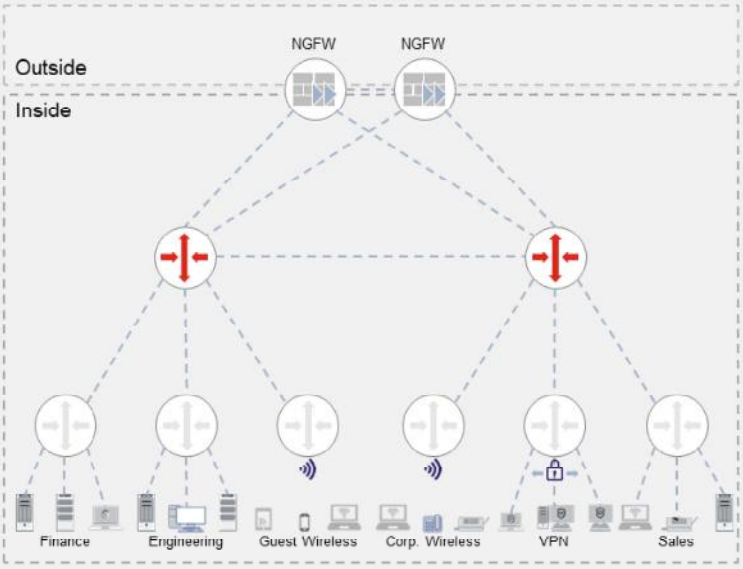
Adding segmentation across the enterprise network can increase cost, reduce flexibility, and hinder performance. Network segmentation architecture helps to adopt a deep segmentation architecture.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Today's Border Security

- The problem:
  - Protect business from outside attacks
  - Protect users from external threats
  - Keep users productive
- The solution:
  - Apply all security at the internet edge
  - Flat network provides no internal security
  - Visibility into the network severely limited
  - Risk of compromise is very high



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

To protect the enterprise business from outside attacks and protect users from external threats, you can implement a simple network segmentation with an edge firewall. The firewall divides the outside of the network from the inside.

You may use network addresses, or, in the case of an NGFW, identity and applications to establish who has trust and access. Advanced security like IPS, AV, and web content filtering can keep the business protected.

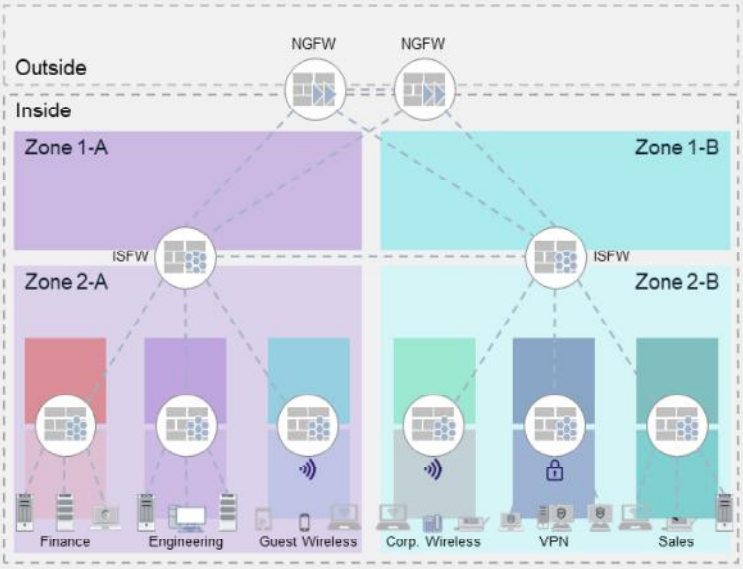
But all of this is focused at the internet edge. The inside of the network is flat, and there is no security to protect the business assets from attackers. Since there is no visibility inside the network, the fact about who is accessing the network remains a concern. The risk of compromise is very high if a simple segmentation is only partially planned for the enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case—Reducing Attack Surface

- The problem:
  - The flat internal network
  - Lack of internal visibility
  - Weak internal security
- The solution:
  - Add more enforcement points
  - Create containment zones
  - Perform deep SSL inspection
  - Inspect applications
  - Check for zero-day malware
  - Protect critical assets



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

You can reduce the attack surface of enterprise network by eliminating the flat network, and increasing visibility and security. On this slide, there are a number of internal segmentation firewalls to the network as enforcement points. These enforcement points create multiple containment zones that can be as granular as needed.

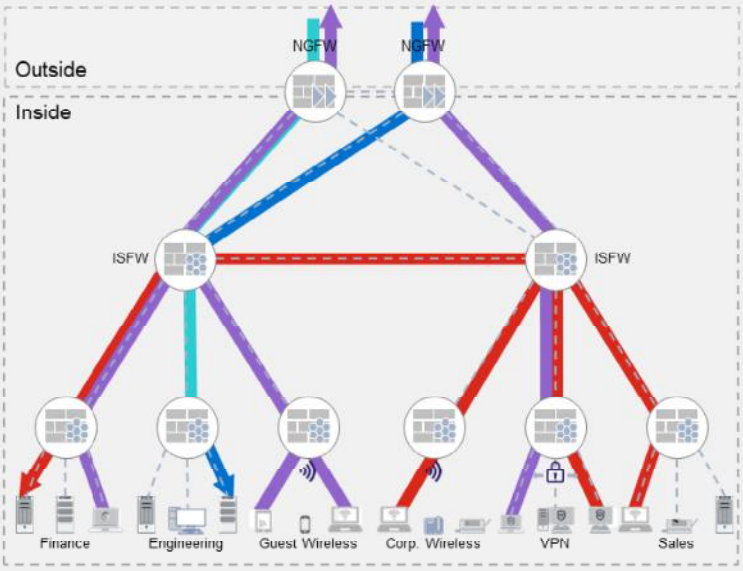
Unlike border security, reducing the attack surface focuses on securing the internal portions of the network, so some security measures, like a web content filter, are not required. However, because malware can be hiding inside encrypted sessions, doing deep SSL inspection is mandatory, as well as using advanced threat protection for zero-day threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case—Trusted Application Integrity

- The problem:
  - Secure business-critical applications
  - Multiple applications protection
  - Users in multiple locations
- The solution:
  - Secure applications with solutions that share security intelligence
  - Utilize security that works with mobility and cloud usage
  - Inspect SSL to make sure only trusted transactions take place
  - Establish trust with sources inside and outside the network



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

You can improve the security posture by securing critical business applications that keep the business running. It is not as simple anymore to deal with all of the applications. Cloud and mobility also create challenges that you must deal with.

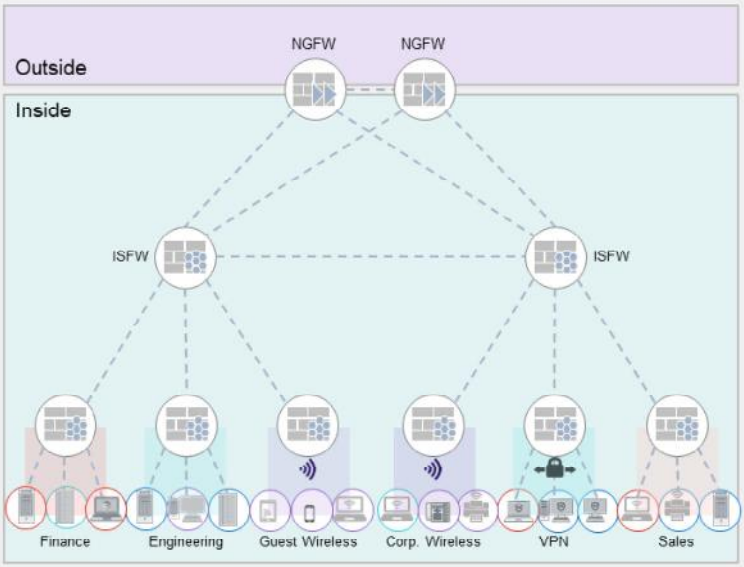
Network segmentation uses the flexibility of the network to handle multiple use cases, but also embraces other security products that cooperate to improve the security posture of the enterprise. Cloud-based email is the most common vector for attacks. A secured email gateway is imperative. Servers exposed to the internet need the protection of a web application firewall. Internal applications, such as those used by HR, can be targets for attacks, which makes using SSL to inspect transactions key. With so many things to secure, ensuring that security information is shared among all of the solutions helps keep your critical infrastructure safe.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case—Achieving Compliance

- The problem
  - Enforcing regulated access
  - Standard network boundaries
  - Critical compliance policies
- The solution
  - Multiple enforcement point locations
  - Endpoint coverage for specific needs
  - Network coverage for IoT
  - Visibility for audits
  - Keep critical systems running



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

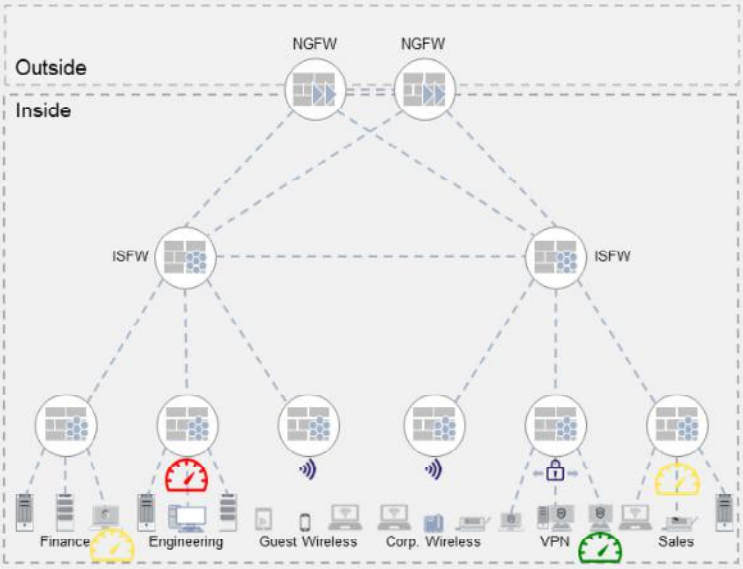
A lot of businesses have to deal with compliance in one form or another, which creates certain challenges. Often, the policies required do not follow standard network boundaries. And internet of things (IoT) devices may not all be able to have endpoint enforcement enabled. If only the like colored elements can talk to each other, you cannot create network policies that follow these requirements. This means you have to use the business logic, user identity, and device identity to achieve policies that enforce compliance. It's not feasible to redesign the network every time a new compliance requirement comes along.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case—Tiered Cloud Access

- The problem
  - Unexpected cloud costs
  - Shadow IT
  - Lack of cloud data visibility
- The solution
  - Combine cloud usage statistics with local enforcement
  - Regulate access to cloud resources from authorized users
  - Maintain audit trails of cloud-hosted data
  - Prevent data exfiltration



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

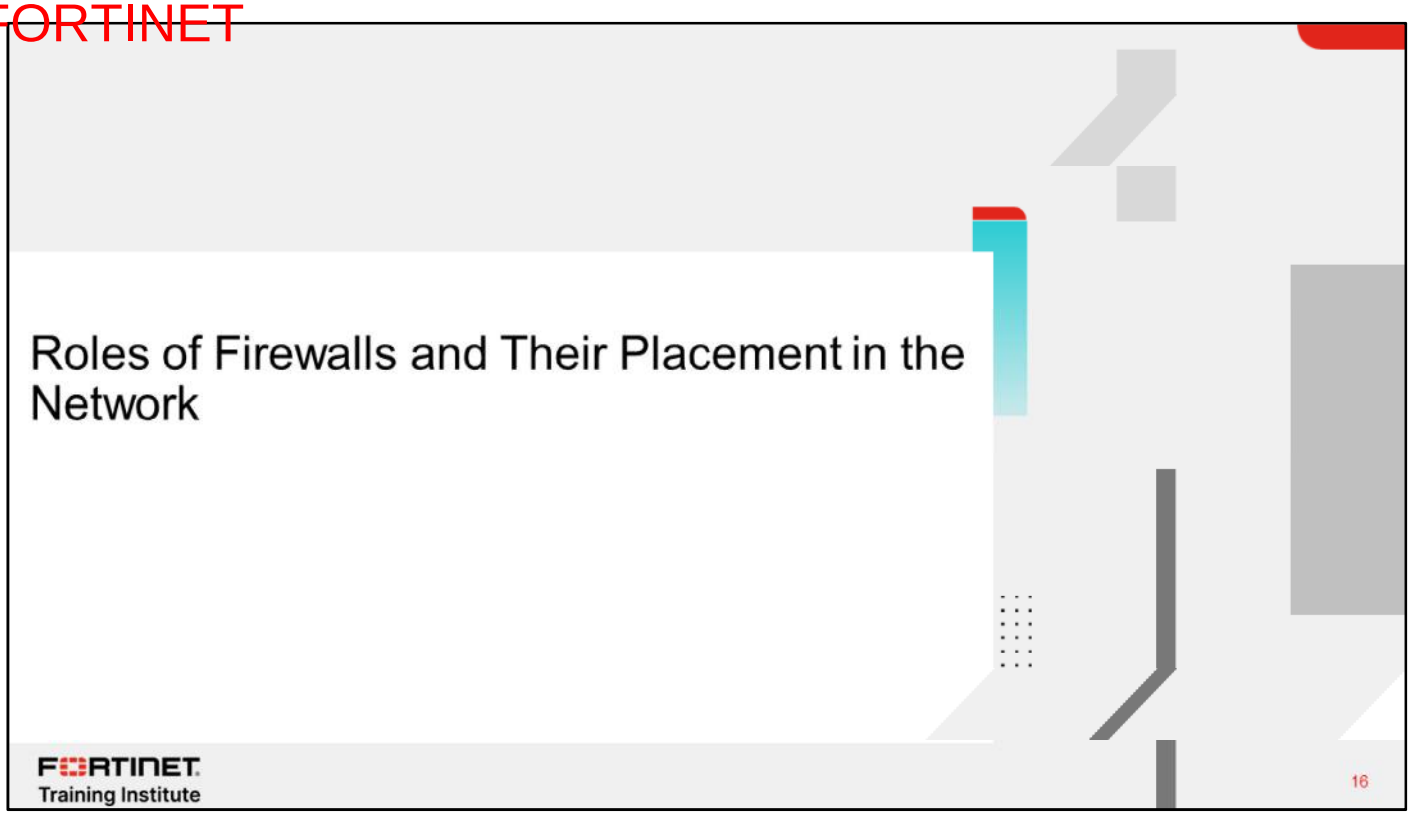
15

In order to align the business segmentation with what security the network can provide, sometimes integration with outside sources is required. Most firewalls have no visibility into the metadata of cloud providers, which means the costs are unknown without post-service billing. Shadow IT, and other non-sanctioned cloud instances can provide channels into the enterprise network that you may not be aware of. You must orchestrate the network security with the cloud services you use with an application programming interface (API).

This keeps the network visibility high, even inside the cloud, while data is safe. Once integrated, the amount of cloud usage that is retrieved from the cloud providers themselves, can be monitored for users or whole groups to keep your cloud under your control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

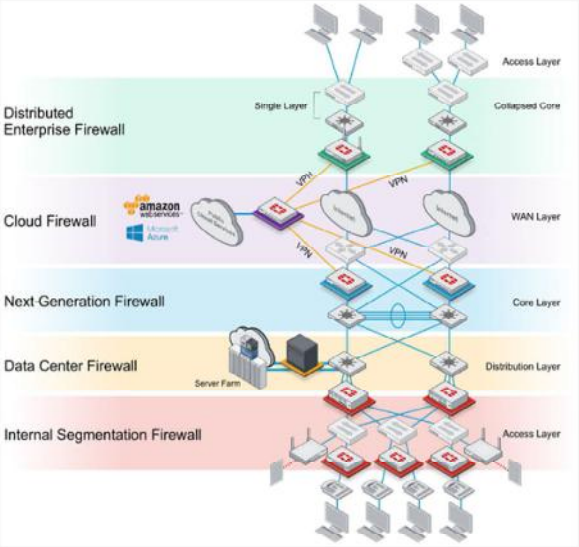


In this section, you will learn about the Fortinet Enterprise Firewall solution at a high level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Firewall Roles in the Enterprise Firewall Solution



Firewall Role	Purpose	Deployment Layer	Target Throughput	Typical Features Deployed
Distributed Enterprise Firewall (DEFW)	Branch office with VPN to HQ	Access/Edge (All-in-one)	Up to 1 Gbps	Firewall, App Control, Web Filter, IPS, antivirus & VPN
Next-Generation Firewall (NGFW)	Separate private network from public networks	Edge or Core	1 – 40 Gbps	Firewall, App Control, IPS, antivirus & VPN
Data Center Firewall (DCFW)	Inbound protection from internal and external threats	Distribution	10 Gbps – 1 Tbps	Firewall, App Control & IPS
Internal Segmentation Firewall (ISFW)	Breach containment and segment isolation	Access	1 Gbps – 100 Gbps	Firewall, App Control, Web Filter & IPS

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

In the Enterprise Firewall solution, each FortiGate device has a specific role, depending on where it is installed and what assets it is protecting. In this lesson, you will learn about the Distributed Enterprise Firewall (DEFW), Next-Generation Firewall (NGFW), Data Center Firewall (DCFW), and Internal Segmentation Firewall (ISFW).

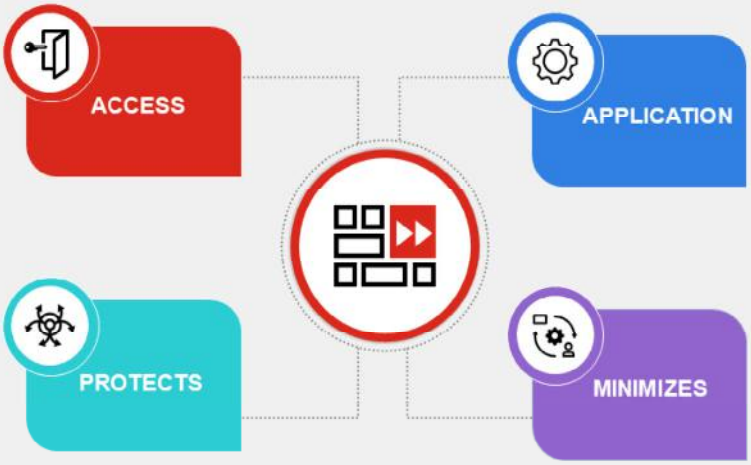
- DEFWs are usually smaller devices installed in branch offices and remote sites. Distributed enterprises usually don't follow a standardized enterprise network design, and therefore multiple layers are collapsed into one or two layers. They are connected to the corporate headquarters using a VPN. DEFWs are all-in-one security devices, doing firewall, application control, IPS, web filtering, and antivirus inspection.
- NGFWs are usually deployed for firewall, application visibility, intrusion prevention, malware detection, and VPNs. NGFWs can play the traditional role of the entry-point firewall or, depending on the network infrastructure, can be deployed in the core.
- DCFWs protect corporate services. They focus on inspecting incoming traffic and are usually installed at the distribution layer. Because of the high-performance requirements, in most cases the security functions are kept to a minimum: firewall, application control, and IPS.
- ISFWs split your network into multiple security segments. They serve as breach containers for attacks that come from inside. Firewall, application control, web filtering, and IPS are the features that are commonly enabled in these firewalls.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Next-Generation Firewall (NGFW)

- Access to the internet
- Application to access local DC and cloud with ZTNA
- Protects network from external threats
- Minimizes and contains breach by implementing dynamic segmentation



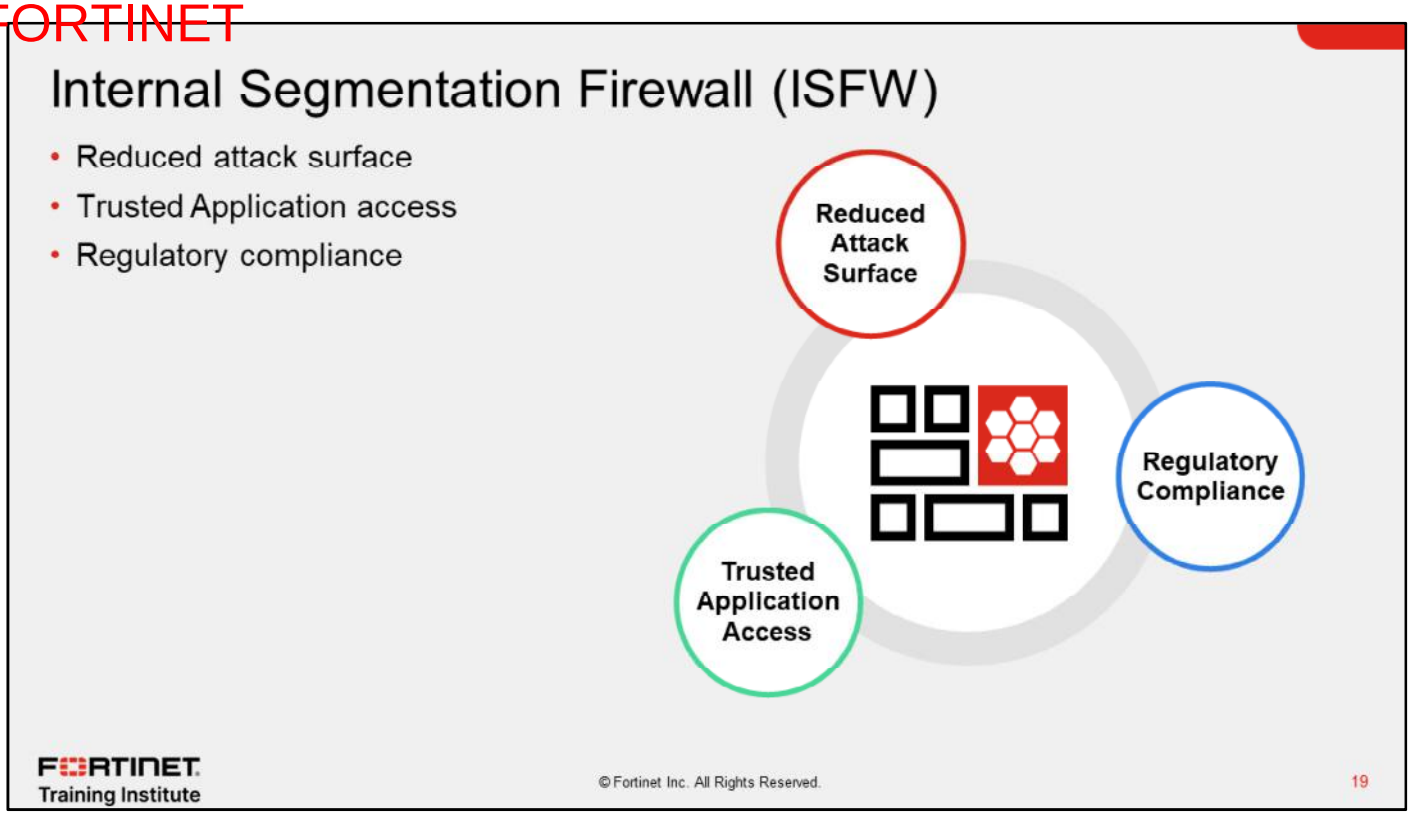
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



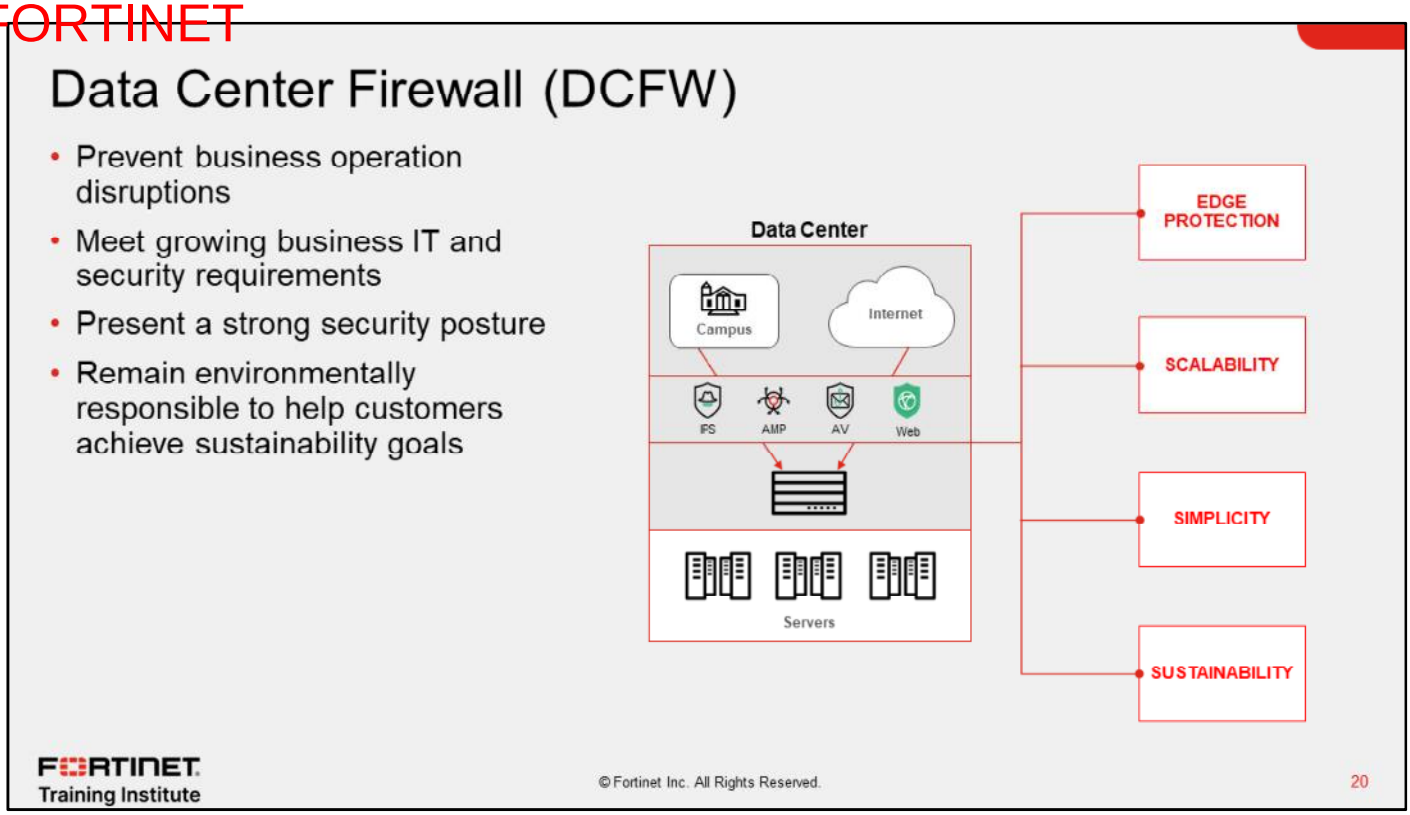
You can proactively manage attack vectors and risks and implement defense in-depth with cost-effective enforcement points.

You can improve security posture by securing critical applications and utilize open API integration with trust management and broad security platforms.

You can implement regulatory policy to secure compliance assets, security assessment, and business logic-driven security policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



DCFW offers edge threat protection to handle risk management and prevent business disruptions with full visibility and advanced security.

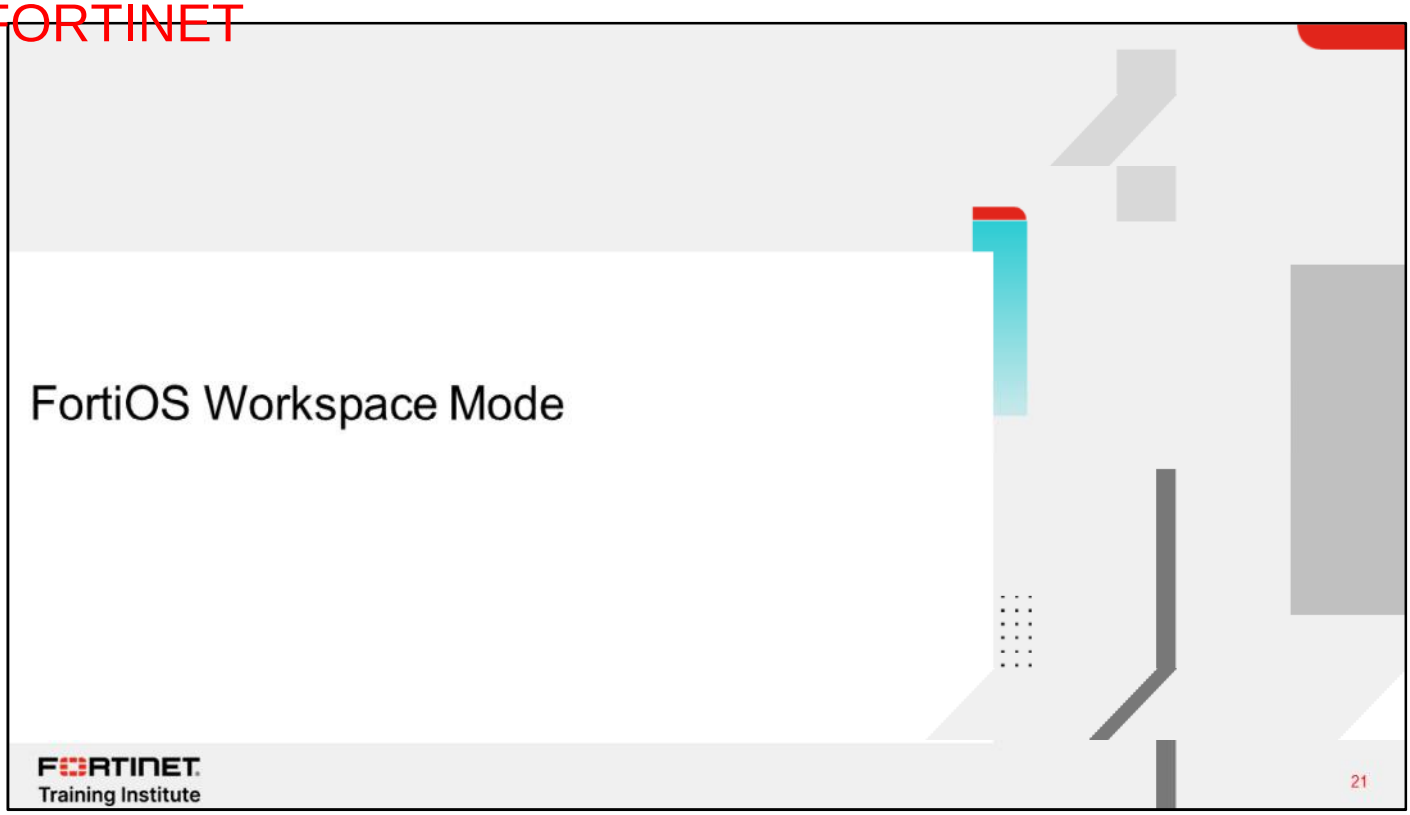
DCFW also allows you to meet growing business requirements with high availability and automation.

It also enables you to present a strong security posture with consistent and automated security policy.

DCFW is also environmentally responsible, which helps customers achieve sustainability goals.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



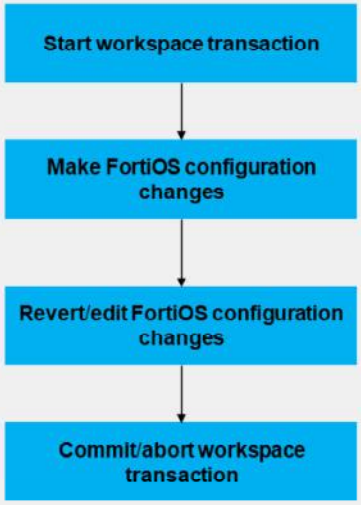
In this section, you will learn about FortiOS workspace mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Workspace Mode

- Start workspace mode:
  - `execute config-transaction start`
  - Configuration changes are made in a local CLI process that is not viewable by other processes
- Abort configuration changes:
  - `execute config-transaction abort`
  - If changes are aborted, no changes are made to the current configuration
- Commit configuration changes:
  - `execute config-transaction commit`
  - After committing, the changes are available for all other processes and the kernel



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Workspace mode allows administrators to make a batch of changes that are not implemented until they commit the transaction. Prior to committing, the administrator can revert or edit the changes as needed without impacting current operations.

When an administrator edits an object in workspace mode, it is locked, preventing other administrators from editing that object. A warning message is shown to let the administrator know that the object is currently being configured in another workspace transaction.

All administrators can use workspace mode; their permissions in workspace mode are the same as the permissions defined in their account profile.

A workspace mode transaction times out in five minutes if there is no activity. When a transaction times out, all changes are discarded. A warning message is shown to let the administrator know that a timeout is imminent, or has already happened.

Workspace mode is available only through the FortiGate CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Diagnosing Workspace Mode

```
# diagnose sys config-transaction status
The CLI is running config transaction (id=1)

# diagnose sys config-transaction show txn-info
txn id=1, expire=12 seconds, user='admin', userfrom='ssh(10.1.10.1)',
clicmd_fpath='/dev/cmdb/txn/4_Ede9G.conf
config transaction id=1 will expire in 10 seconds
config transaction id=1 has expired

# diagnose sys config-transaction show txn-cli-commands
  config system global
    set hostname "NewHostname"
  end
```

Transaction ID

Administrator

Changes are aborted if they are not committed before the transaction expires

Changes pending to be committed

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

The command `config-transaction status` shows if the current administrator is working on a workspace that is pending being committed. If that is the case, the output shows the transaction ID for the workspace.

To view information about all the active workspace transactions (from multiple concurrent administrators), use the command `config-transaction show txn-info`. The output shows the identifier for each transaction and their expiration times. It also shows the usernames of the administrators working on each workspace, as well as information about how and from where those administrators are connecting.

You can list the CLI changes pending to be committed in your workspace using the command `config-transaction show txn-cli-commands`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe the enterprise firewall solution
- ✓ Explain the network security reference architecture and the Fortinet products it comprises
- ✓ Describe the roles of firewalls and their placement in the network
- ✓ Understand FortiOS workspace mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

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

By mastering the objectives covered in this lesson, you learned about the enterprise firewall solution and the network security reference architecture and the Fortinet products it comprises. You learned also about the roles of firewalls and their placement in the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

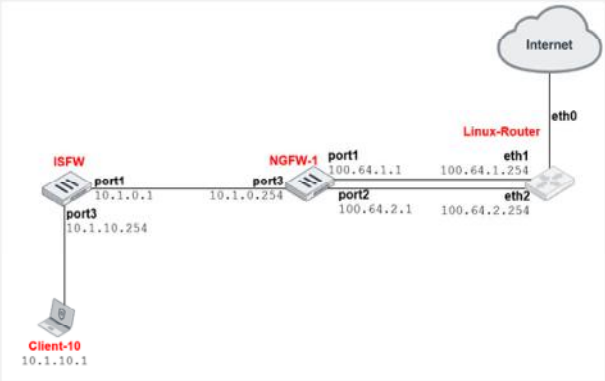
Now, you will work on *Lab 2–FortiOS Architechture*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lab 1—Introduction to Network Security Architecture

- Integrate ISFW port3 to a software switch
  - Migrate all port3 settings to the new interface
- Merge NGFW port1 and port2 to SD-WAN
  - Enable SD-WAN
  - Update firewall objects to point SD-WAN instead



FORTINET Training Institute

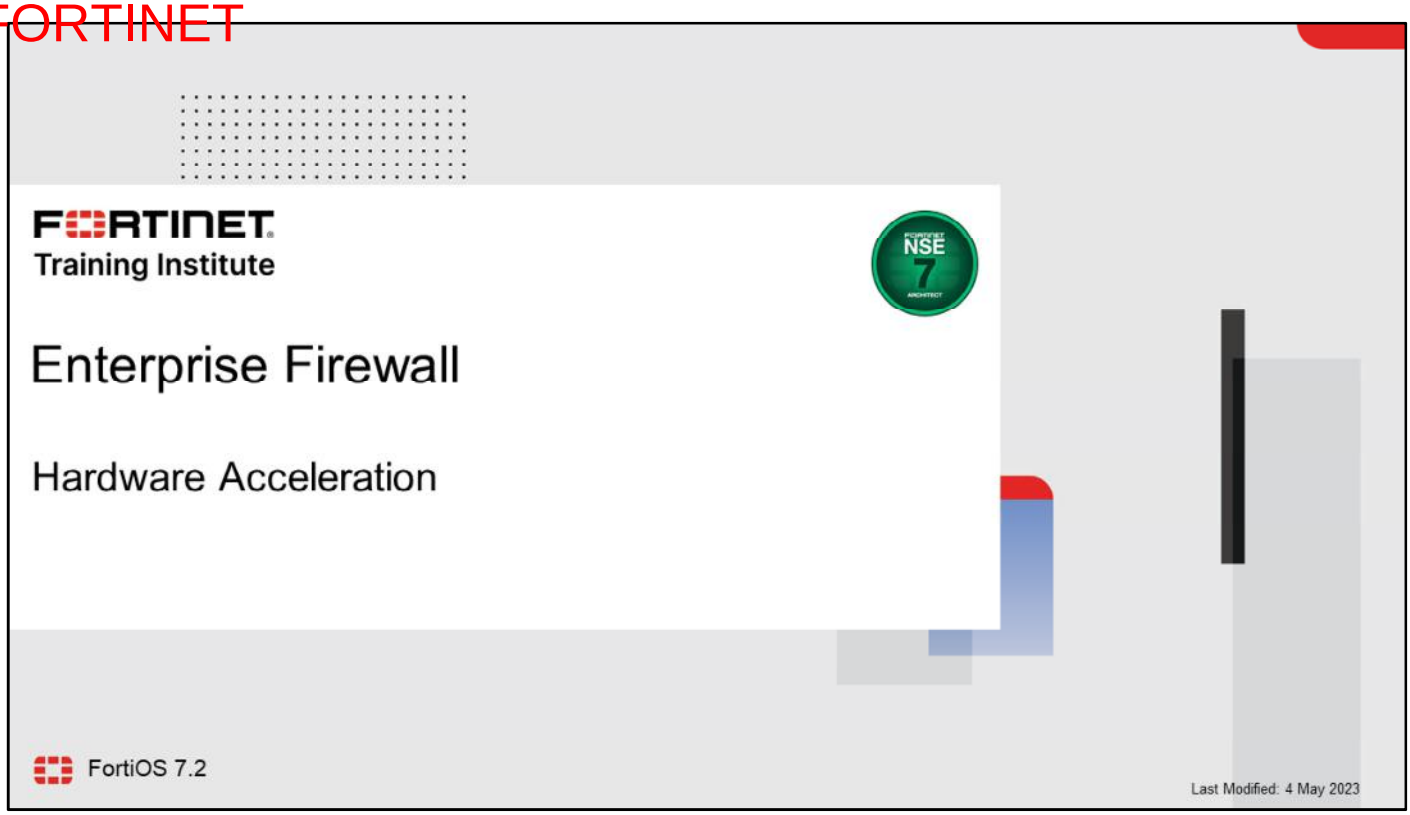
© Fortinet Inc. All Rights Reserved.

26

In this lab, you will integrate existing interfaces on ISFW and NGFW to the new interfaces on each FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about hardware acceleration on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Objectives

- Describe the architecture of hardware offload on FortiGate
- Explain NP7, NP6, NTurbo, SoC4, and CP9 processors and their features
- Describe how traffic is offloaded from kernel to NP
- Describe the limitations of offloading the traffic
- Configure hardware acceleration

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

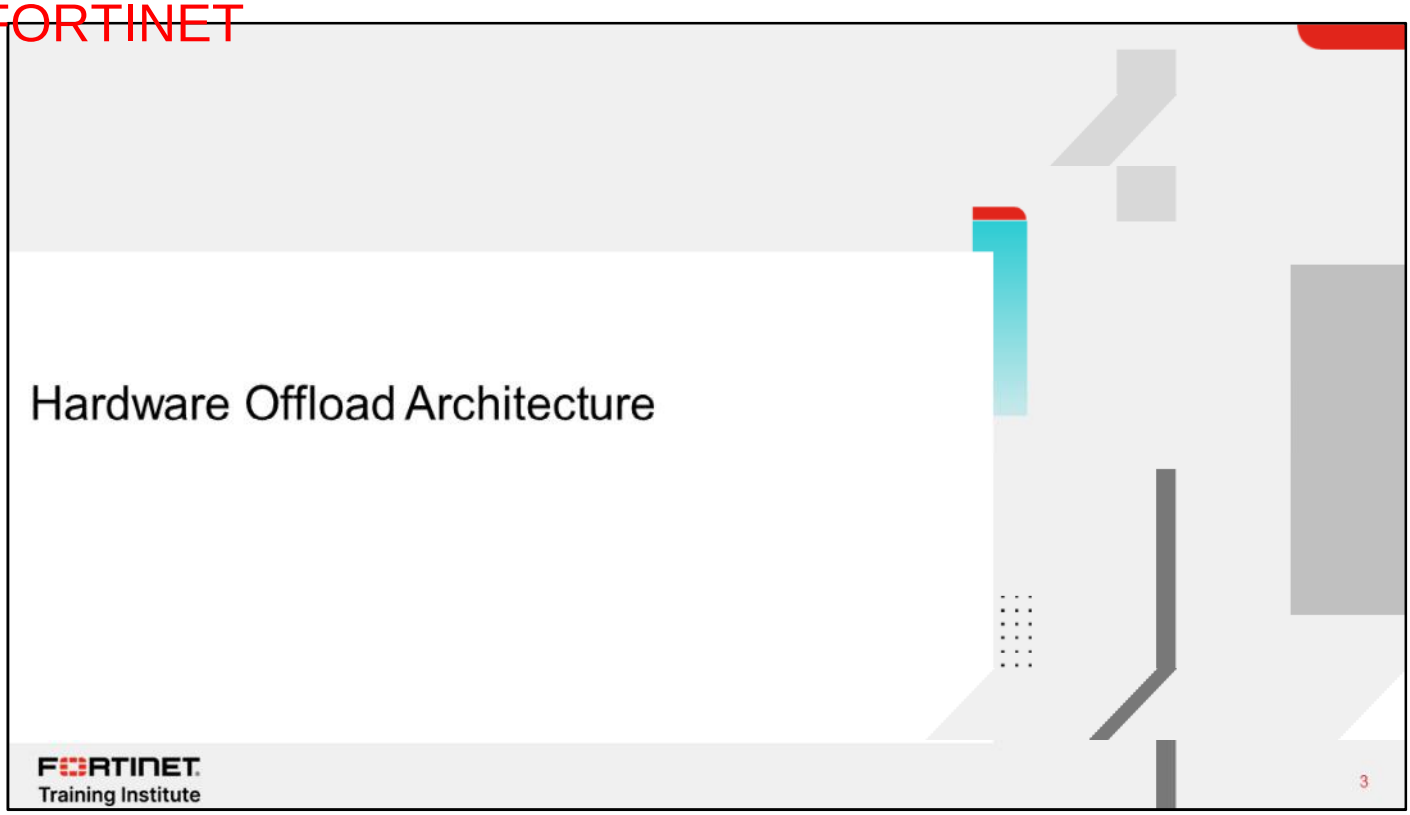
2

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

By demonstrating competence in hardware acceleration on FortiGate, you will be able to understand the design aspect of hardware acceleration on FortiGate and explore the different security processing units available on FortiGate as well as their features.

Vouchers & Dumps are Available | WhatsApp +201224560923

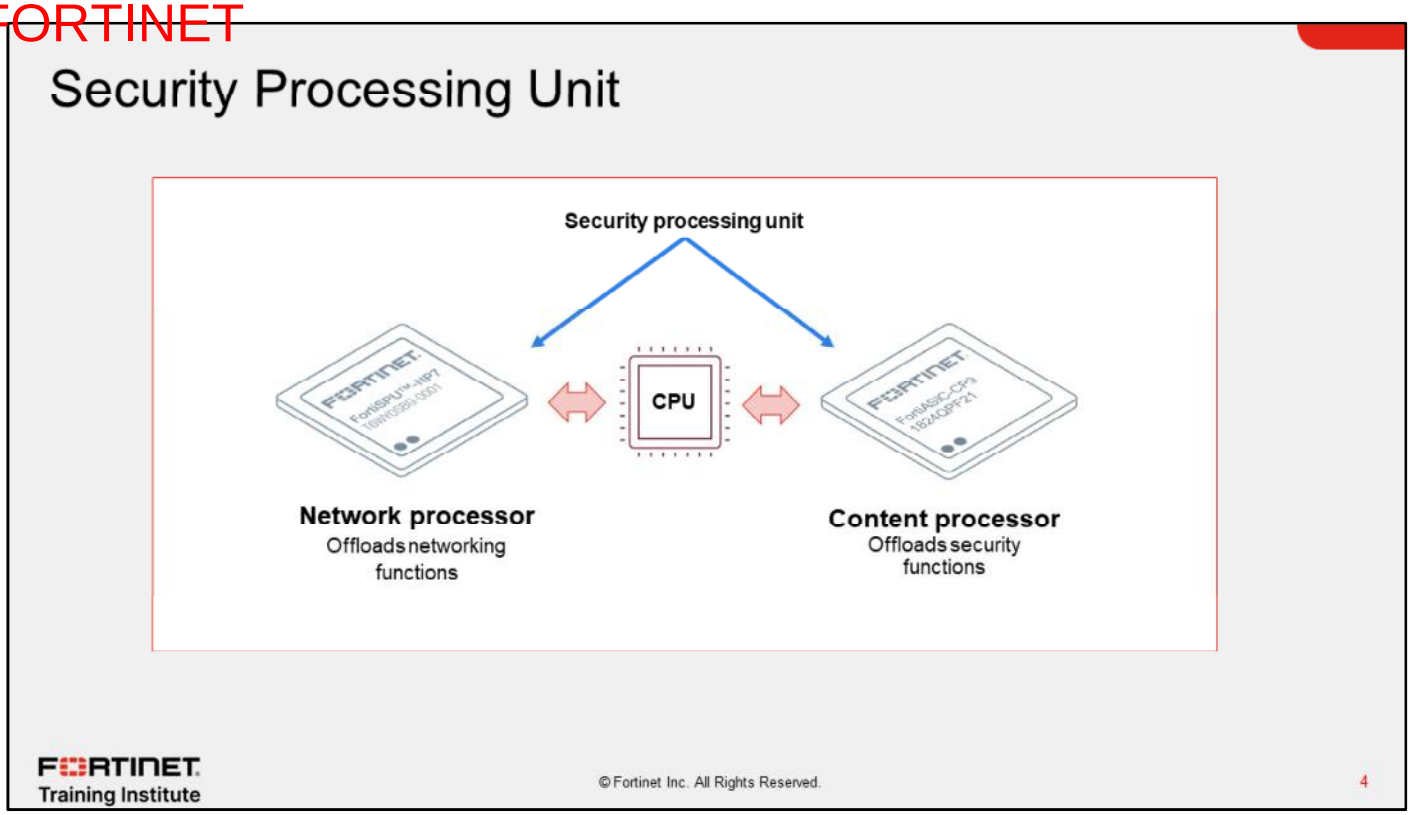
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the architecture of hardware offload on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

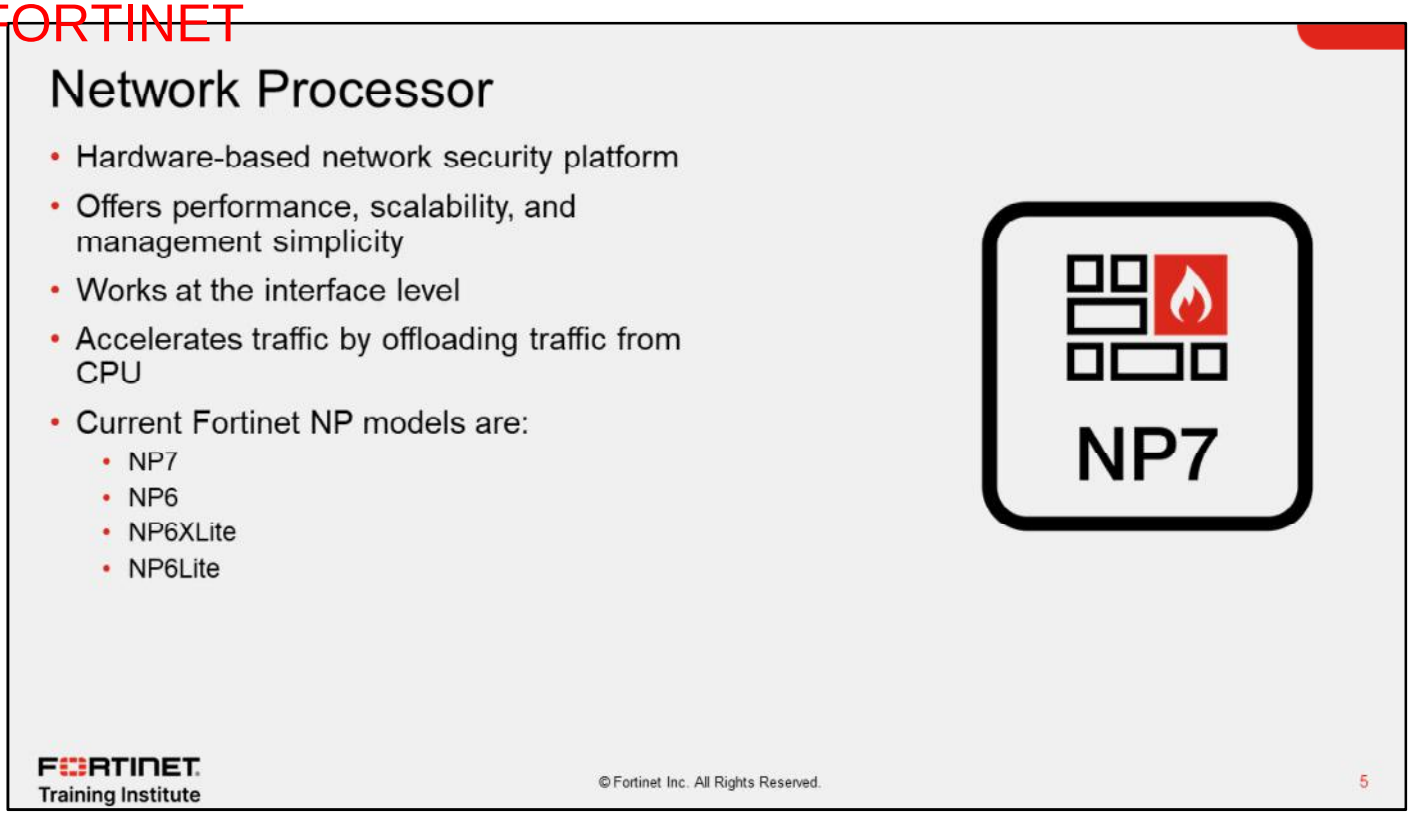


Fortinet hardware acceleration technology refers to the use of specialized hardware devices, such as network security processors, to offload certain security-related tasks from the main CPU in Fortinet security appliances. This allows for improved performance and higher processing speeds for certain functions, such as encryption and decryption, packet inspection, and others. By using hardware acceleration, Fortinet devices can handle more traffic and provide more efficient processing of network security functions, resulting in better network performance and scalability.

The specialized acceleration hardware on most FortiGate models, also referred to as the security processing unit (SPU) or an application-specific integrated circuit (ASIC), can offload resource-intensive processing from the main processing unit (CPU) on FortiGate. On FortiGate, an SPU can be a network processor (NP), a content processor (CP), or both. Depending on the FortiGate model, both processors can work simultaneously while traffic is passing through to be offloaded and/or accelerated.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The FortiGate network processor (NP) is a hardware-based network security platform. The NP allows for real-time, high-speed processing of network traffic for security and optimization purposes. This results in improved network performance, scalability, and simplified network management.

The FortiGate NP includes hardware acceleration capabilities, which offload specific security functions to dedicated hardware to further improve performance and reduce the load on the main CPU.

The NP works at the interface level to accelerate network traffic by offloading it from the CPU. The current Fortinet models available on most FortiGate devices are:

- NP7
- NP6
- NP6XLite
- NP6Lite

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Processor

- A component of a FortiGate device
- Accelerates common resource-intensive security-related processes
- Works at the system level and receives offloaded tasks from the CPU
- Security tasks accelerated are offloaded to the CP based on the assignment of CPU tasks
- Current Fortinet CP models are:
  - CP9
  - CP9XLite
  - CP9Lite

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

Content processors (CPs) are components on FortiGate devices that accelerate network traffic and scan traffic for potential security threats. The CP accelerates the common resource-intensive security processes and offloads them from the main CPU. The CPU determines which security tasks gets accelerated and offloaded to the CP.

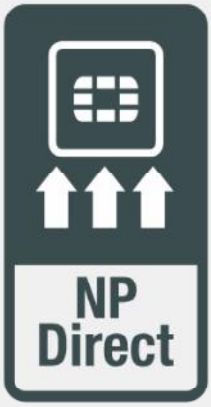
The current Fortinet CP models available on most FortiGate devices are:
- CP9
- CP9XLite
- CP9Lite

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP Direct Architecture

- Available on FortiGate devices that have two or more NP6 processors
- Hardware architecture that has a FortiASIC network processor directly connected to the interfaces
- Reduces forwarding latency
  - Eliminates ISF
- Physical topology must ensure that all traffic passes through the offloaded interfaces of one NP6 processor



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

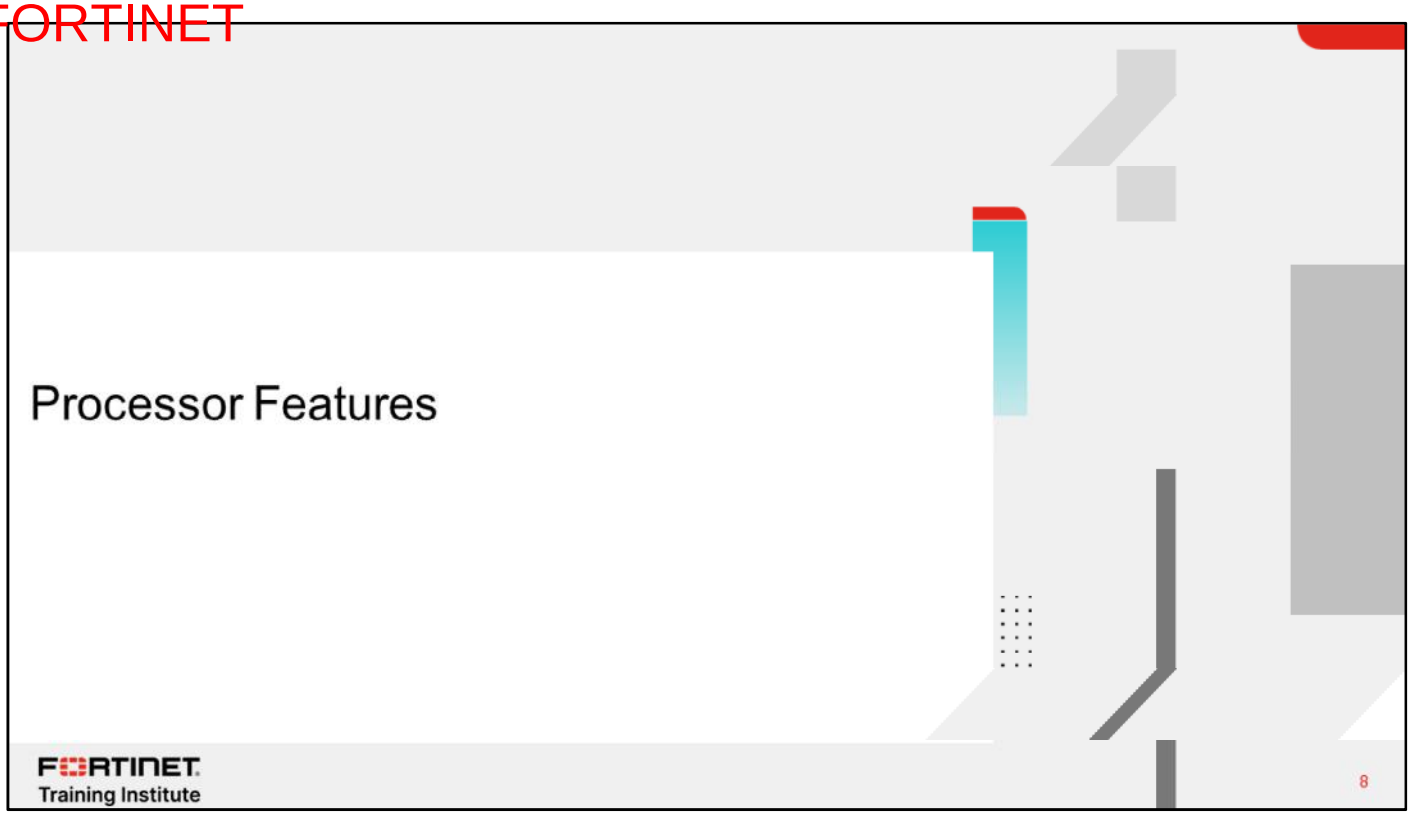
7

NP direct architecture offers access to the NP by removing the use of the internal switch fabric (ISF), which is the hardware chip switch that is attached to the FortiGate physical interfaces. NP direct architecture is available on FortiGate devices equipped with two or more NP6 processors. This allows access between the interfaces directly to the NP for lowest-latency forwarding.

Part of the requirement for implementing NP direct architecture is to ensure that the offloaded traffic enters and exits FortiGate through interfaces connected to the same NP6 processor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the NP7, NP6, NTurbo, SoC4, and CP9 processors and their features

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP7 Processor

- 1 channel of 8 PCIe host interfaces
- Maximum 200 Gbps forwarding throughput
  - Two 100-Gbps interfaces
- Accelerated session setup and logging
- Hyperscale services
  - License required for high-end devices
  - GCNAT and hardware logging support
  - Volumetric DDoS protection
- IPsec VPN improvement
  - Higher throughput
  - Suite B IPsec acceleration with ESN support
  - GTP load balancing

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

The NP7 processor operates inline to deliver unmatched performance for network functions and hyperscale for stateful firewall functions.

The NP7 processor has a maximum throughput of 200 Gbps using two 100-Gbps interfaces. Some FortiGate devices with NP7 processors support the configuration of NP7 port mapping. You can map data interfaces to specific NP7 100 Gbps interfaces, which allows you to balance traffic between the NP7 interfaces.

The NP7 processor offers single IPsec encrypted tunnel throughput of at least 75 Gbps, which allows FortiGate to encrypt high-speed data on data center connections.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP6 Processor

- Available in two versions:
  - Four 10-Gbps connections
  - Three 10-Gbps and 16 1-Gbps connections
- Provides bandwidth and connectivity to the CPU to achieve improved CP direct support for the latest Intel chip
- Supports the latest multicore CPU
- Adds stronger support for IPsec cryptography

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

The NP6 processor is available in two versions:

- Four 10-Gbps connections, which is tailored for high-end FortiGate devices where the 10-Gbps ports are attached to an ISF
- Three 10-Gbps connections and 16 1-Gbps connections, which is available on mid-range FortiGate devices and allows direct connection of the FortiGate ports to the NP6 processor, without ISF

With higher bandwidth and connectivity to FortiGate CPU, the NP6 processor supports multicore CPUs that aid in higher flow to security and SSL inspection performance. The NP6 processor also enhances IPsec encryption and decryption and adds additional layers of security to VPN tunnels.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NTurbo Processor

- The NTurbo processor offloads traffic inspected by the security profiles in flow-based mode
  - The NP cannot offload traffic inspected by the security profiles
- The FortiOS kernel runs the NTurbo driver to handle incoming traffic
  - The NTurbo processor runs on a dedicated CPU and is not shared with other tasks
- The NTurbo processor receives packets from the ISF through the CPU and NP
- For a new session, the NTurbo processor sends packets to the IPS engine
  - The IPS engine processes the required security action
  - The IPS engine then sends the packet back to the NTurbo processor
- The NTurbo processor continues to send processed packets back to the NP and then to the ISF

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

The NTurbo processor offloads traffic that the NP cannot offload due to the security profiles used to inspect the traffic.

FortiGate runs the NTurbo driver on a CPU that is dedicated to processing traffic that the NP sends and that requires a security inspection in flow-based mode. The FortiGate CPU processes proxy-based inspections.

When packets from the NP and CPU pass through the NTurbo processor, it sends the packets to the IPS engine to complete the security task required. Then, the NTurbo processor sends the processed packets to the ISF through the NP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SoC4 Processor

- Integrates the following components in one chip:
  - CPU
  - NP6XLite
  - CP9XLite
- Available on some entry-level FortiGate devices
- Does not require binding interfaces to specific NPs
- Accelerates all sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

The system-on-a-chip (SoC) processor consolidates network and content processing, and delivers fast application identification, steering, and overlay performance.

The SoC4 processor combines the main CPU of FortiGate with acceleration technologies such as NP6XLite and CP9XLite. This combination delivers a high-performance application experience on entry-level FortiGate devices.

FortiGate devices that have the SoC4 processor do not require binding interfaces to dedicated NPs because the SoC4 processor combines all the SPUs on one chip. Therefore, the SoC4 processor accelerates the traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

CP9 Processor

- Offloads tasks and performs hardware encryption
- Performance enhancement dependent on CPU architecture and speed
- Supports content processing in the following areas:
  - VPN
  - SSL offloading
  - Flow-based UTM
- Improves dynamic signatures and hashes on AV
- Allows configurable TTTD

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

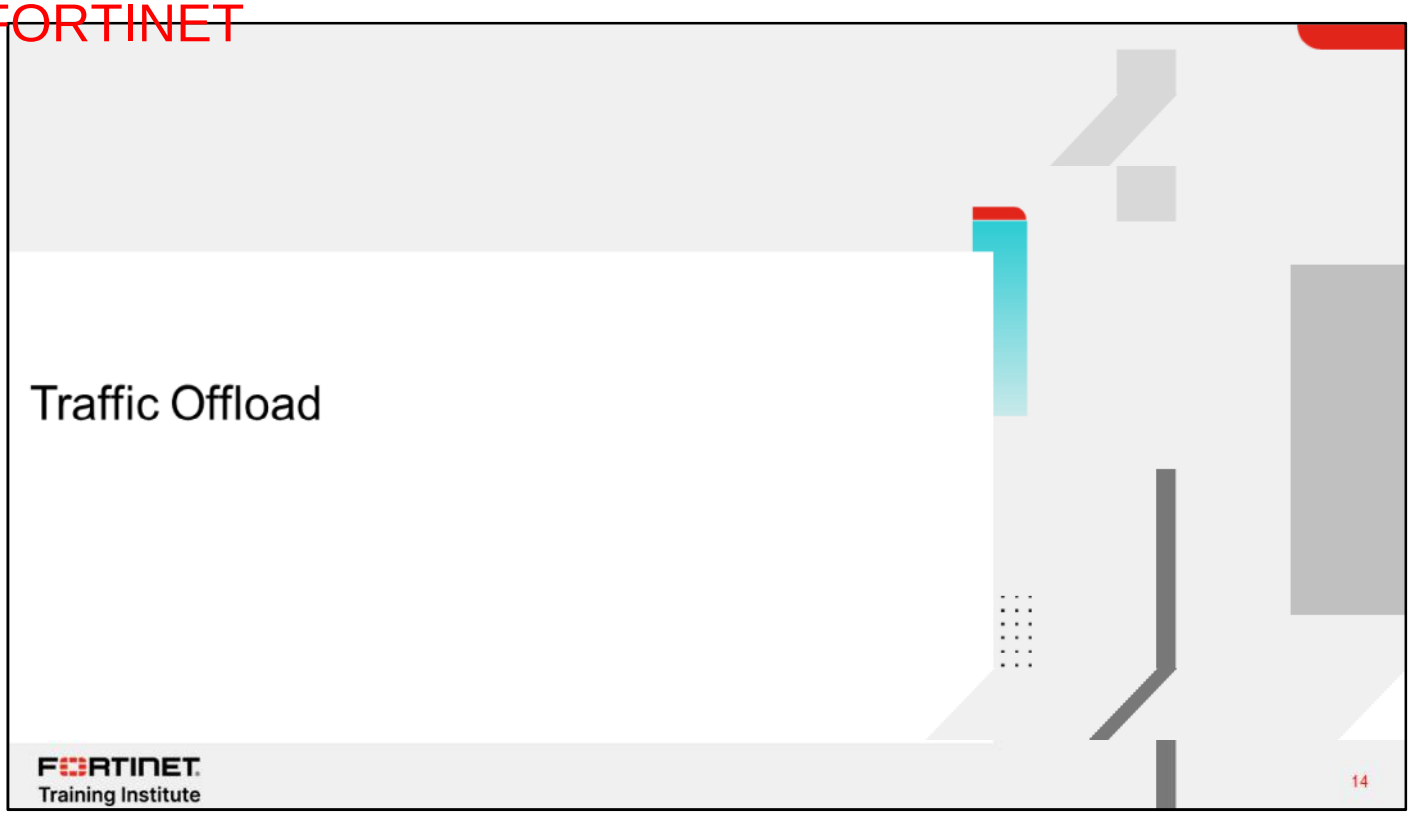
The CP9 processor increases performance by accelerating many common security resources. The CP9 processor offloads tasks and performs hardware encryption, relying on the FortiGate CPU architecture and speed.

As a coprocessor to the main CPU, the CP9 processor offloads resource-intensive processing and drives content inspection to accelerate security functions, VPN, and SSL offloading.

The CP9 processor improves dynamic signatures and hashes on the AV engine, and it allows configurable two thresholds two divisors (TTTD) content chunking for data loss prevention (DLP) inspection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn about how FortiGate offloads traffic from the kernel to an NP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP Offloading Packet Flow

- The NP alters traffic when offloading packets
- The packets initiating a session pass to the CPU
- FortiGate verifies if the packets matches session offloading requirements
  - The requirements depend on the type of NP
  - The assessment determines only whether to fast-path packets
- If the packets meet requirements, the session key or IPsec SA pass to the NP
- The NP continues to match packets on ingress ports
  - The NP accepts packets, or drops them if further anomaly checks are required
  - IPS anomaly checks are separate from the NP checks
- The NP checks the session key or IPsec SA
  - If it finds a match, packet acceleration continues, and the NP offloads the packets from the FortiGate CPU
- If the session doesn't match or meet requirements, the NP cannot offload it and sends the packets to the FortiGate CPU

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

The NP offloading process alters traffic when it arrives on FortiGate. The packets that initiate a session are passed to the FortiGate CPU, which verifies whether the packets match the offloading requirements. The requirements vary based on the type of NP.

The checking process verifies only whether packets should continue the acceleration process based on the requirements used in the original session.

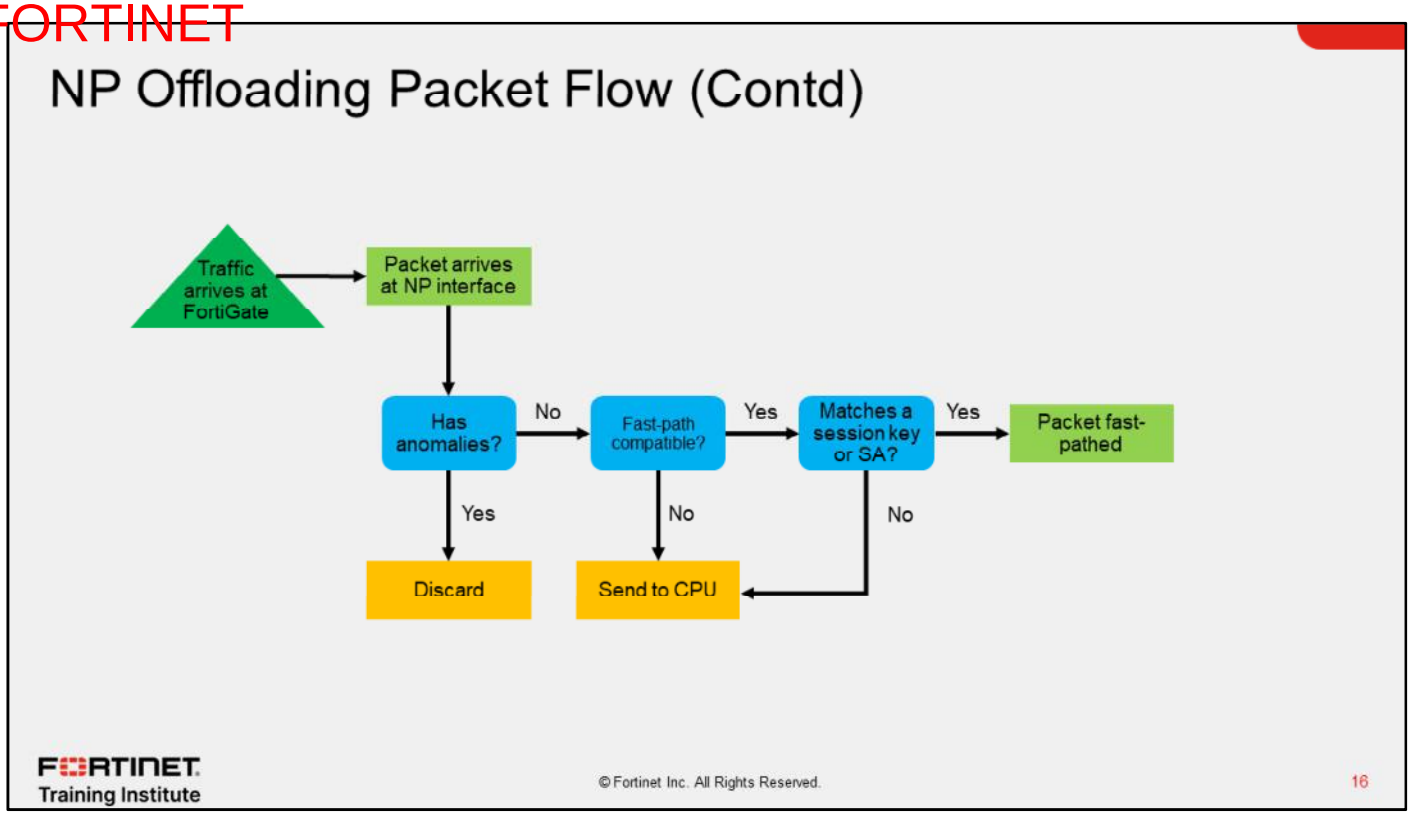
After the first phase of checking, and if the session key or IPsec SA matches the original traffic, FortiGate sends the packets to the NP. The NP continues to match packets on ingress ports and determines whether to accept them, or drop them if anomalies are detected. These NP checks are not the same as the IPS anomaly checks.

Next, the NP checks the session key or the IPsec SA. If it finds a match, the acceleration continues for the packets, and they are offloaded from the FortiGate CPU.

If the packets do not pass the checks, the NP sends them to the FortiGate CPU.

Vouchers & Dumps are Available | WhatsApp +201224560923

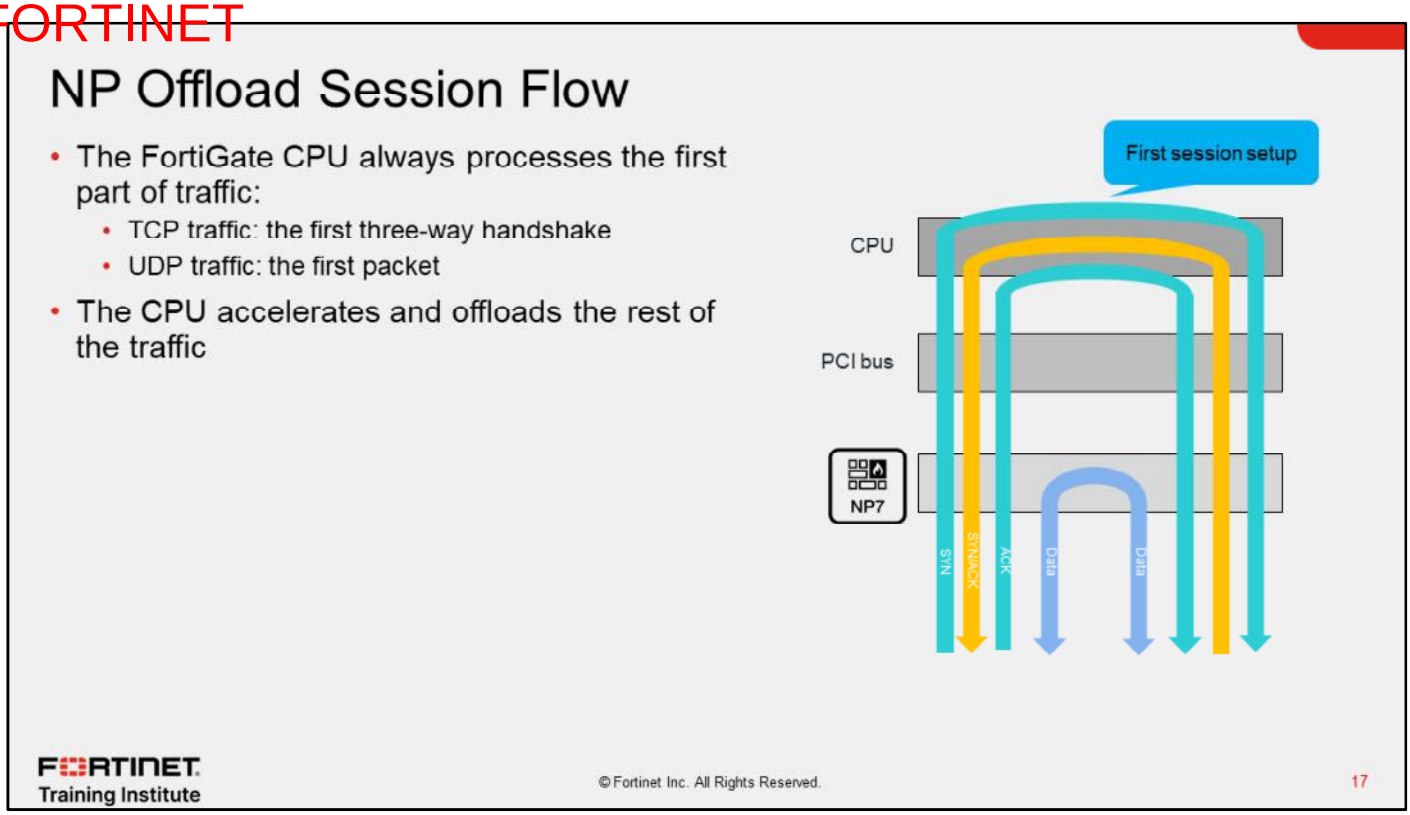
DO NOT REPRINT Brave-dumps.com
© FORTINET



The flow chart on this slide illustrates the process a packet goes through from arriving at the FortiGate device to completing the NP acceleration checklist.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



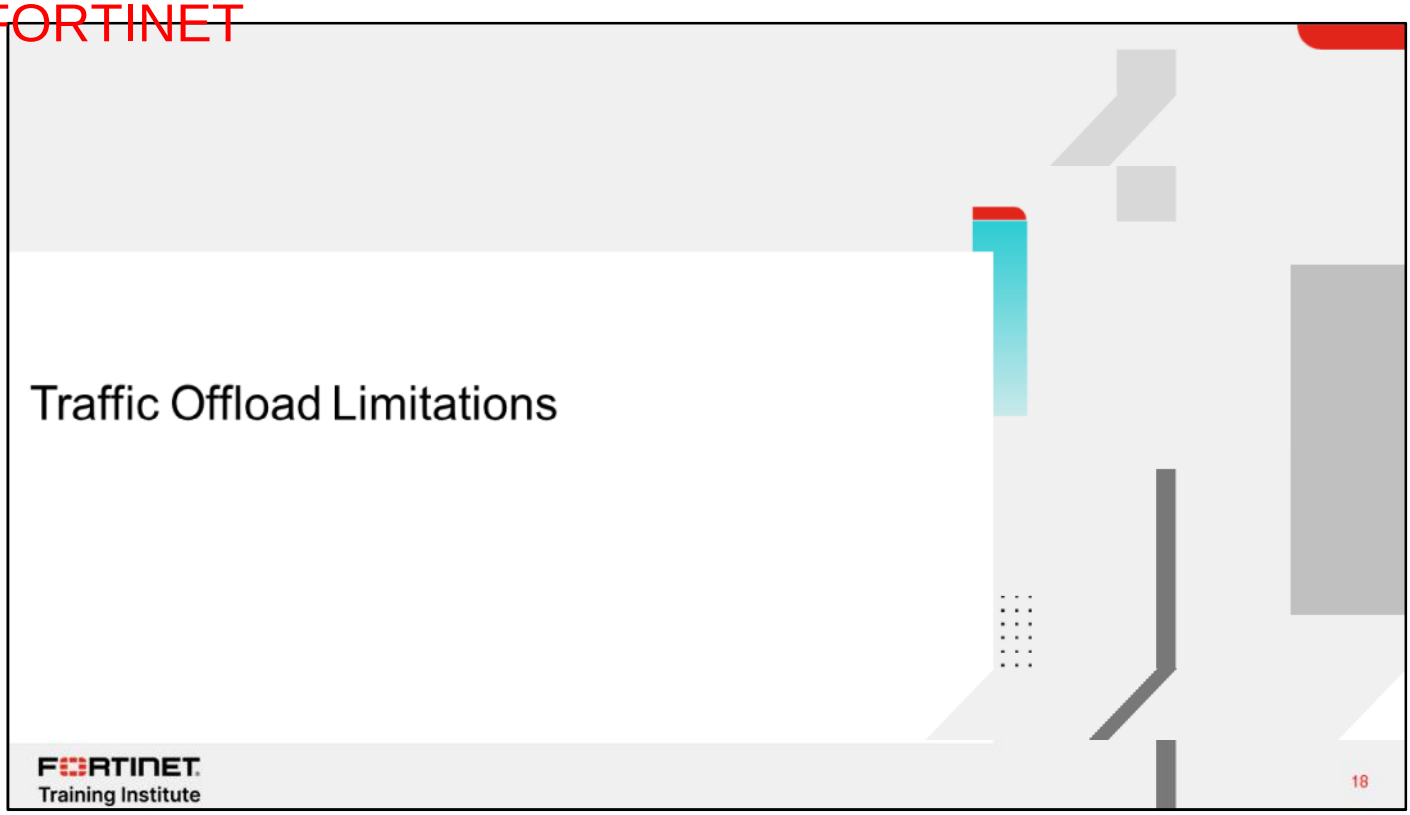
For NP processing, the traffic first passes through the FortiGate CPU to perform the required checks to determine whether the packets can be accelerated and offloaded to the NP processor.

For TCP traffic, the first packets of the three-way handshake must first go to the FortiGate CPU. For UDP traffic, only the first packet must pass through the FortiGate CPU.

If the FortiGate CPU determines that the conditions are met for the first part of the traffic, then the CPU accelerates and offloads the rest of the traffic to the NP6 processor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn about the limitations of offloading traffic on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP7 Processor—Sessions Limits

- The NP7 processor supports a maximum of 12 million sessions
- If it exceeds the maximum, the processor does not offload further new traffic and the main CPU takes control
- To prevent this issue, distribute incoming sessions evenly among available NP7 processors

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

One NP7 processor can support up to 12 million sessions. This number is limited by the processor's memory. Once an NP7 processor hits its session limit, sessions that are over the limit are sent to the CPU. You can avoid this problem by distributing incoming sessions evenly among multiple NP7 processors. To be able to do this you need to be aware of which interfaces connect to which NP7 processors and distribute incoming traffic accordingly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP7 Processor—Supported Traffic Protocols

- The NP7 processor accelerates the following list of protocols:

Name	Protocol
TCP	Transmission control protocol
UDP	User datagram protocol
IP-in-IP	IPv4 IP-in-IP encapsulation
ICMP	Internet control message protocol
RDP	Reliable data protocol
IPv6	IPv6 encapsulation
GRE	Generic routing encapsulation
ESP	Encapsulating security payload
ETHERIP or EoIP	Ethernet over IP
SCTP	Stream control transmission protocol

These protocols are accelerated only in pass-through mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

This slide shows the protocols that the NP7 processor can offload and accelerate. Note that the NP7 processor accelerates tunneling protocols in pass-through mode, which means that traffic does not originate from and is not sent to the processing FortiGate device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NP7 Processor—Supported Tunneling Protocols

- The NP7 processor offloads the following list of tunneling protocols:

Name	Protocol
ESP used for IPsec VPN	IPsec VPN tunneling
CAPWAP	Communication between wireless access points and wired LANs or between different wireless access points
VXLAN	VXLAN and VXLAN over IPsec. Provides secure communication between data centers over public networks

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

This slide shows the tunneling protocols that the NP7 processor supports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

CP9 Processor—Limitation

- The CP9 processor does not accelerate security inspection on unencrypted IPsec traffic on FortiGate
  - For example, IPsec VPN using phase1 proposal AES-GMAC
- Use the CLI to configure and IPsec phase1 proposals with supported proposals

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

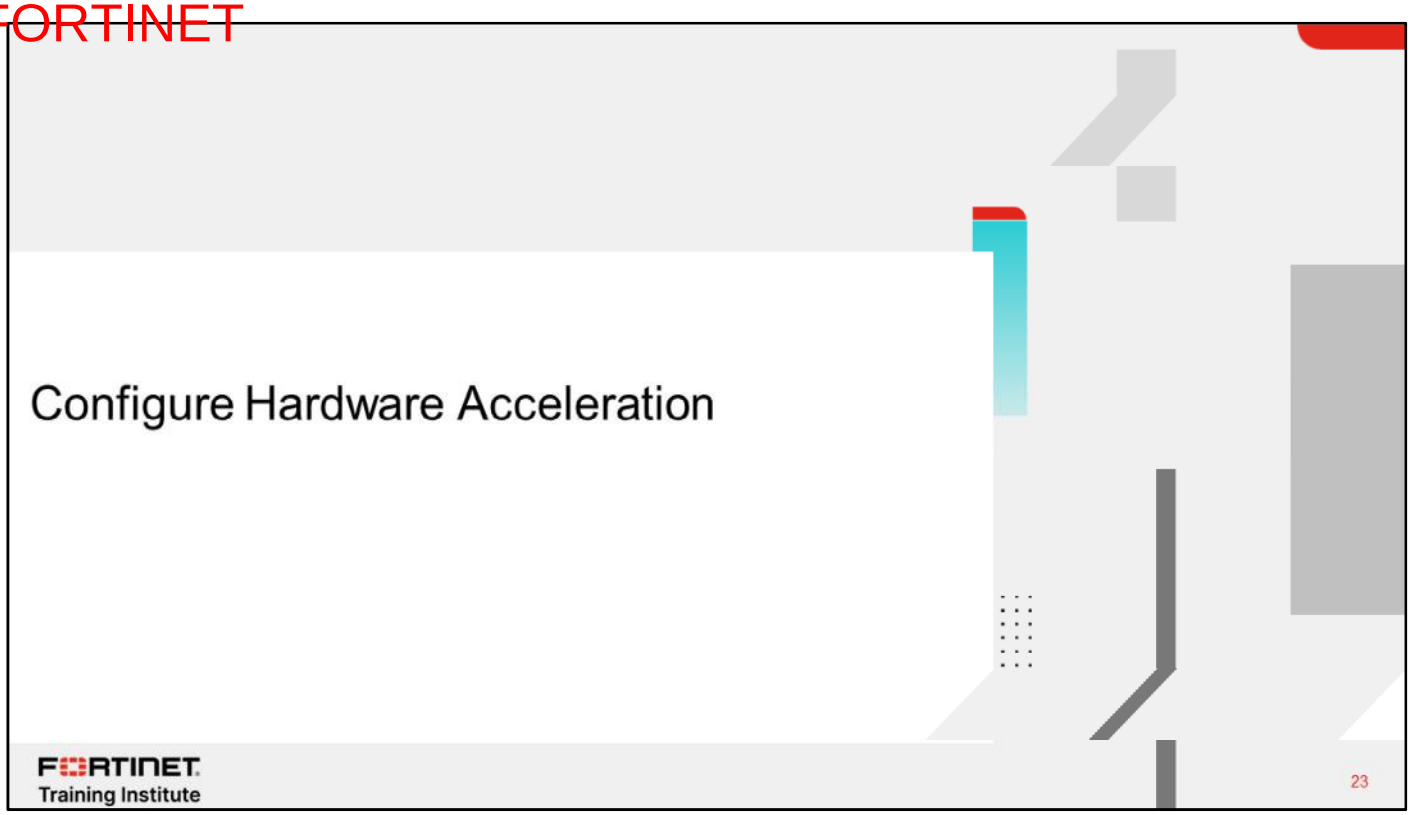
22

IPsec VPNs may not support some less commonly used proposals such as AES-GMAC. If you use an unsupported phase1 proposal, the CP9 processor does not accelerate security inspection on unencrypted IPsec traffic on FortiGate.

To ensure that the CP9 processor accelerates IPsec VPN tunnel traffic, update IPsec phase1 proposals to use a supported encryption algorithm.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about how to configure hardware acceleration

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Strict Header Checking

- You can disable hardware acceleration to enforce header checking
- `check-protocol-header strict` disables all NPs and CPs

```
config system global
    set check-protocol-header [loose|strict]
end
```

- Header checking looks at the following header parameters:
  - L4 header length
  - IP header length
  - IP version
  - IP checksum
  - IP options
  - ESP and SPI correct values
  - Data length

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

You can disable hardware acceleration for NPs and CPs, to cause FortiGate to apply strict header checking and verify that traffic is part of a session that should be processed.

The command checks the packet header and verifies the following parameters:
- Layer-4 protocol header length
- IP header length
- IP version
- IP checksum
- IP options
- ESP correct sequence number
- SPI
- Data length

If the packet fails header checking, FortiGate drops it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

CPU Interface Binding

- Port CPU mapping
- Enable NTurbo and IPSA

```
config system npu
    config port-cpu-map
        edit <interface>
            set cpu-core {string}
        next
    end
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

In some cases, FortiGate may forward fragmented packets in a multicast traffic stream in the wrong order. This can happen if different CPU cores are processing packets from the same multicast stream.

You can use the CLI command to configure the FortiGate to send all traffic received by an interface to the same CPU core.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NTurbo and IPSA

- Configure NTurbo and IPSA acceleration for firewall policy sessions:
  - Firewall policy with security profiles enabled
  - Firewall policy with flow-based inspection mode
- Set NTurbo and IPSA modes

```
config ips global
    set np-accel-mode {none | basic}
    set cp-accel-mode {none | basic | advanced}
end
```

Acceleration mode for IPS processing

Set it to advanced to offload more pattern matching

- Disable NTurbo on a firewall policy for testing purposes

```
config firewall policy
    edit <policy_id>
        set np-acceleration {disable | enable}
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

You can set NTurbo and IPSA acceleration modes in IPS global settings. By setting the NTurbo mode to `basic`, you can disable NTurbo on a security firewall policy. This can be helpful if you want to troubleshoot or test hardware acceleration for specific traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IPsec Diffie-Hellman Offloading

- FortiGate accelerates the Diffie-Hellman key exchange for IPsec traffic
- If issues arise with IPsec ESP traffic, you can disable ASIC offloading using the following command:

```
config system global
    set ipsec-asic-offload disable
end
```

- By default, FortiGate uses Diffie-Hellman for hardware offloading to accelerate IPsec traffic

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

You can run the CLI command on this slide in the system global settings on FortiGate to disable ASIC offloading to accelerate the IPsec Diffie-Hellman key exchange for IPsec ESP traffic. By default, FortiGate uses IPsec Diffie-Hellman hardware offloading.

For debugging purposes or other reasons you can disable offload in config system global.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Determine SPU information

- To check the NP model available on FortiGate:

```
# diagnose hardware lspci | grep 1a29
...
9b:00.0 Class 1000: Device 1a29:NPID
```

1a29 is the vendor ID for Fortinet

  - If NPID is 4e36, it is NP6
  - If NPID is 4e37, it is NP7

- To determine the CP model available on FortiGate:

```
# get hardware status
Model name: FortiGate-100D
ASIC version: CP8
...
```

ASIC version represents CP version available on FortiGate

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

To check the SPU information on FortiGate, you can run the CLI command `lspci` and review the hexadecimal value that comes after the vendor ID for Fortinet which is `1a29`.

For information about CP on FortiGate, you can run the command `get hardware status` and review the `ASIC version` value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Describe the architecture of hardware offload on FortiGate
- ✓ Explain the NP7, NP6, NTurbo, SoC4, and CP9 processors and their features
- ✓ Describe how traffic is offloaded from kernel to NP
- ✓ Describe the limitations of offloading the traffic
- ✓ Configure hardware acceleration

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

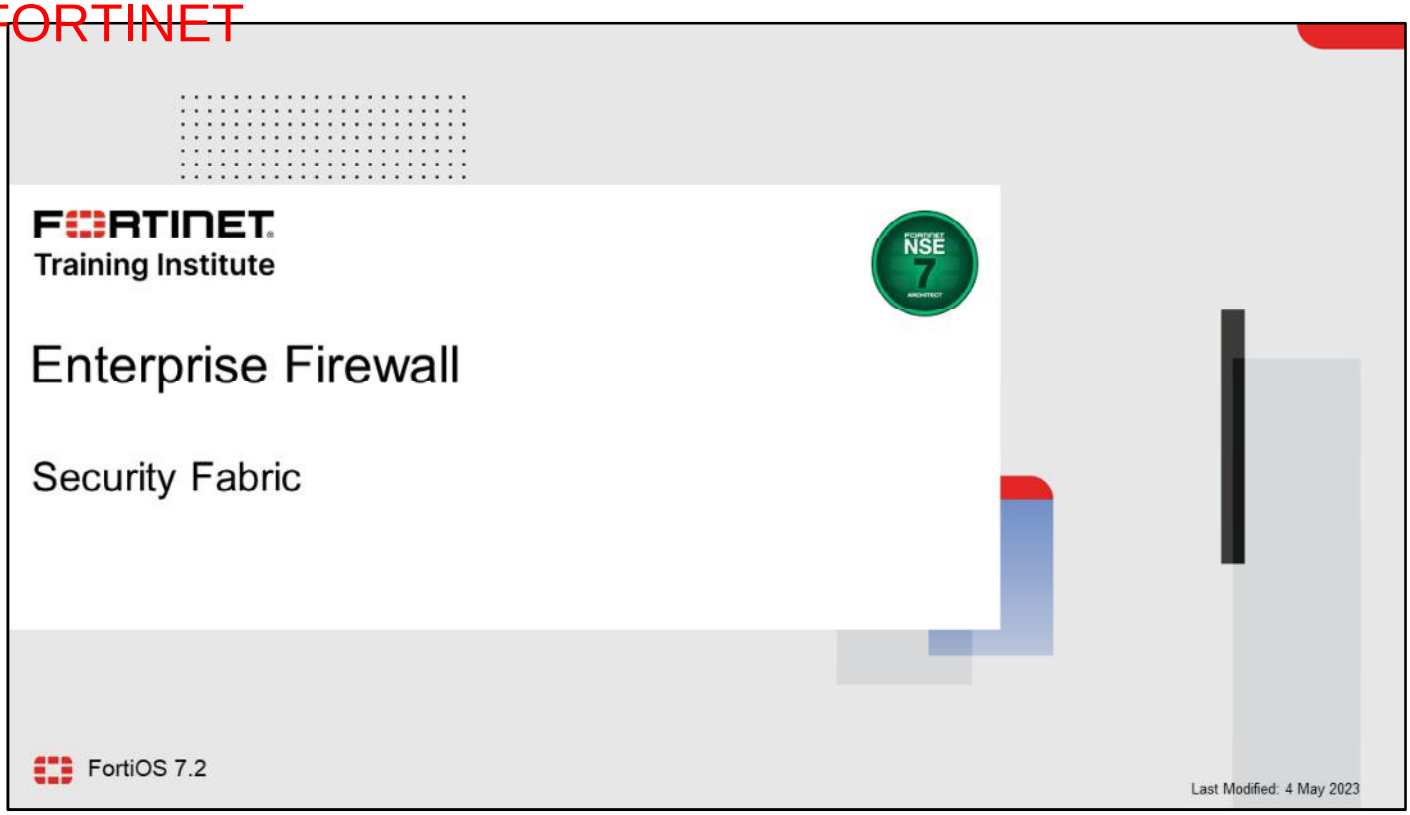
29

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

By mastering the objectives covered in this lesson, you learned about the design aspect of hardware acceleration on FortiGate and explored the different security processing units available on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the Fortinet Enterprise Firewall solution and the Fortinet Security Fabric.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Configure the Fortinet Security Fabric
- Configure automation stitches
- Identify Security Fabric use cases based on different scenarios

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating a competent understanding of the Fortinet Security Fabric, you will be able to configure the Fortinet Security Fabric, perform a security rating audit of your Security Fabric, and configure automation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Devices That Comprise the Security Fabric

- Core:
  - Two or more FortiGate devices + FortiAnalyzer
- Recommended – adds significant visibility or control:
  - FortiManager, FortiAP, FortiSwitch, FortiClient, FortiSandbox, FortiMail
- Extended – integrates with fabric, but may not apply to everyone:
  - Other Fortinet products and third-party products using the API

FORTINET Training Institute

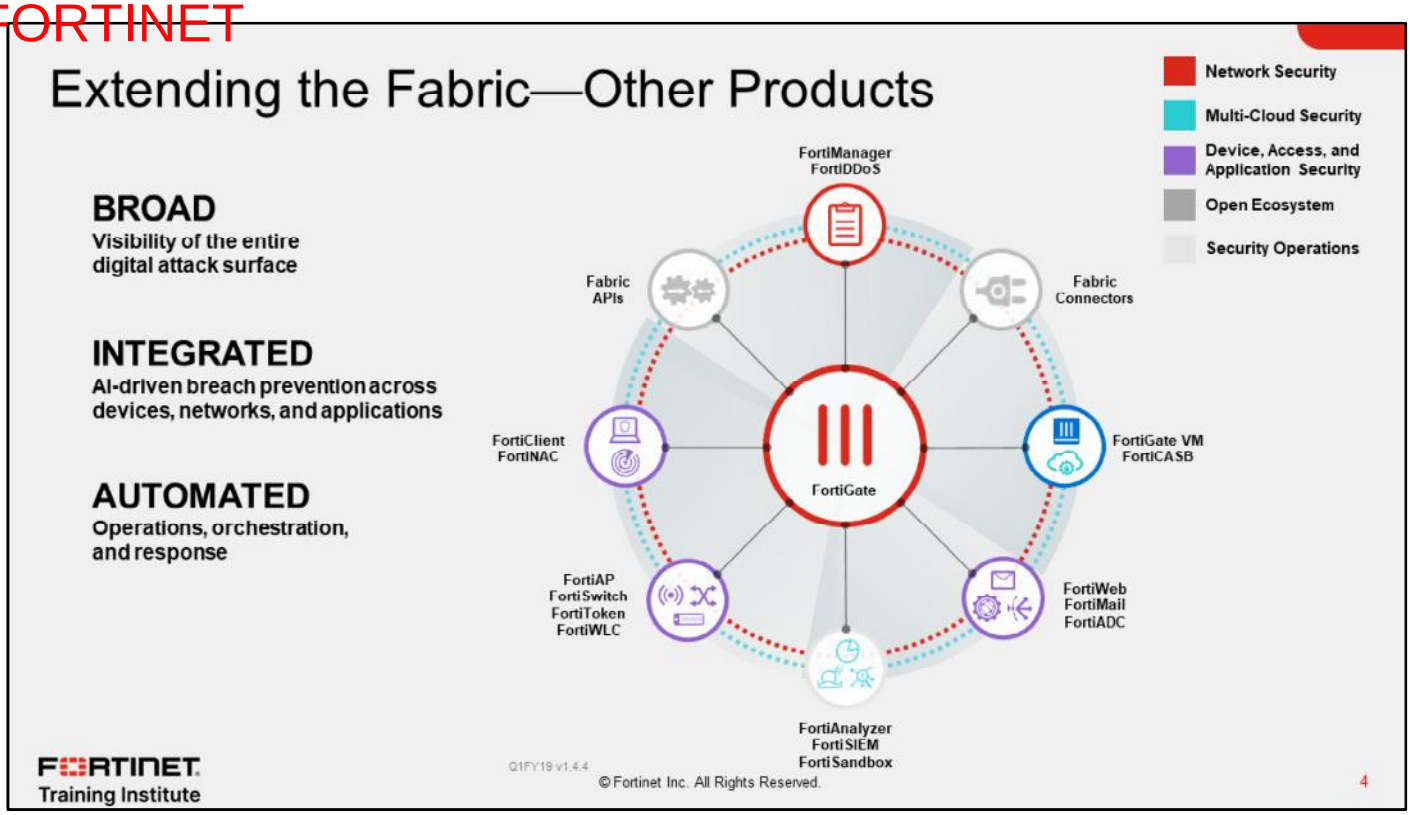
© Fortinet Inc. All Rights Reserved.

3

Two or more FortiGate devices and FortiAnalyzer are the mandatory products at the core of the solution. To add more visibility and control, Fortinet recommends adding FortiManager, FortiAP, FortiClient, FortiSandbox, FortiMail, and FortiSwitch. You can extend the solution by adding other network security devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



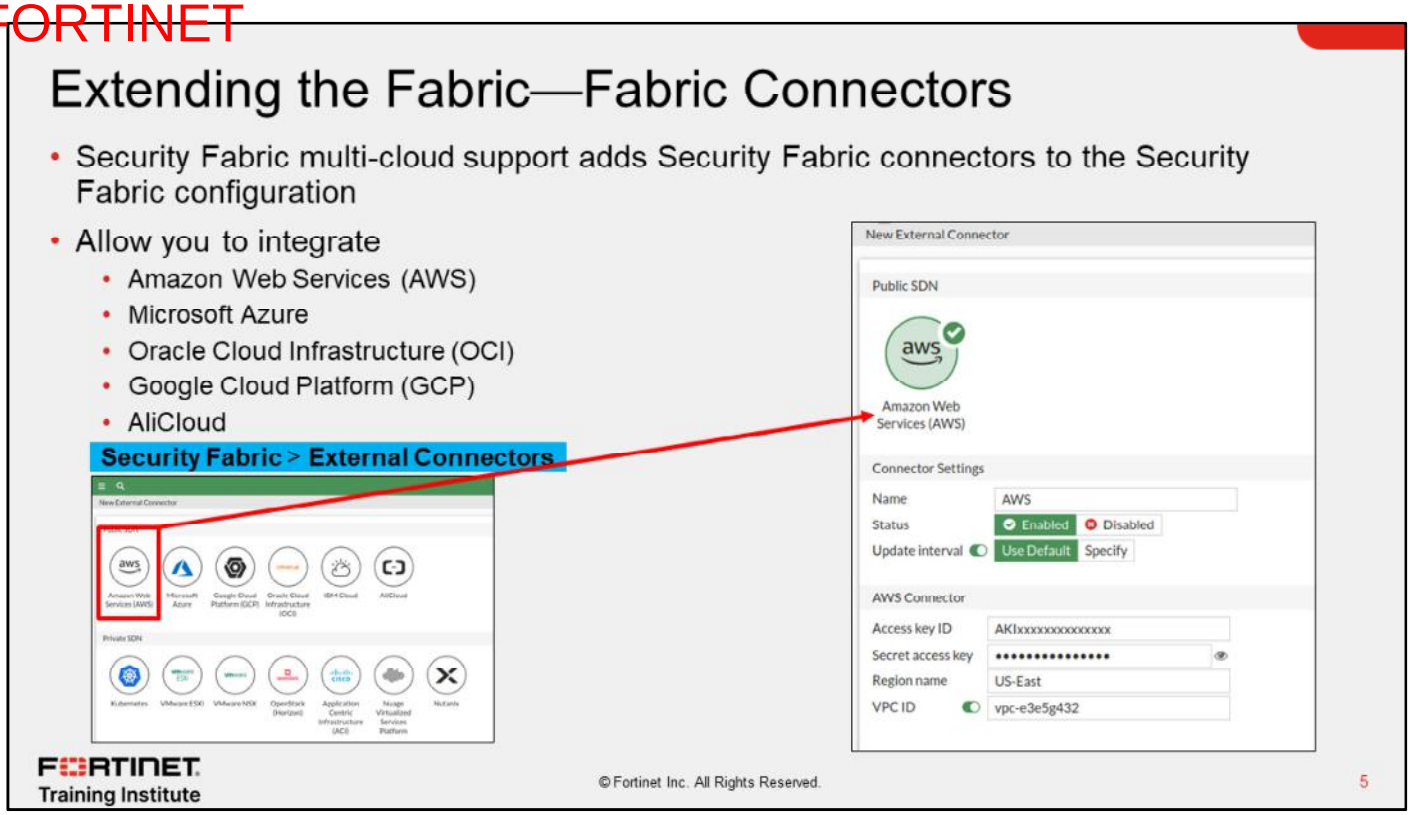
Fortinet recommends using FortiManager for centralized management of all FortiGate devices, and access devices in the Security Fabric. You can integrate FortiSwitch devices, and FortiAP devices to extend the Security Fabric down to the access layer.

You can also extend the Security Fabric by integrating FortiMail, FortiWeb, FortiSandbox, and FortiClient EMS.

The Security Fabric is open. The API and protocol itself is available for other vendors to join and for partner integration. This allows for communication between Fortinet and third-party devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



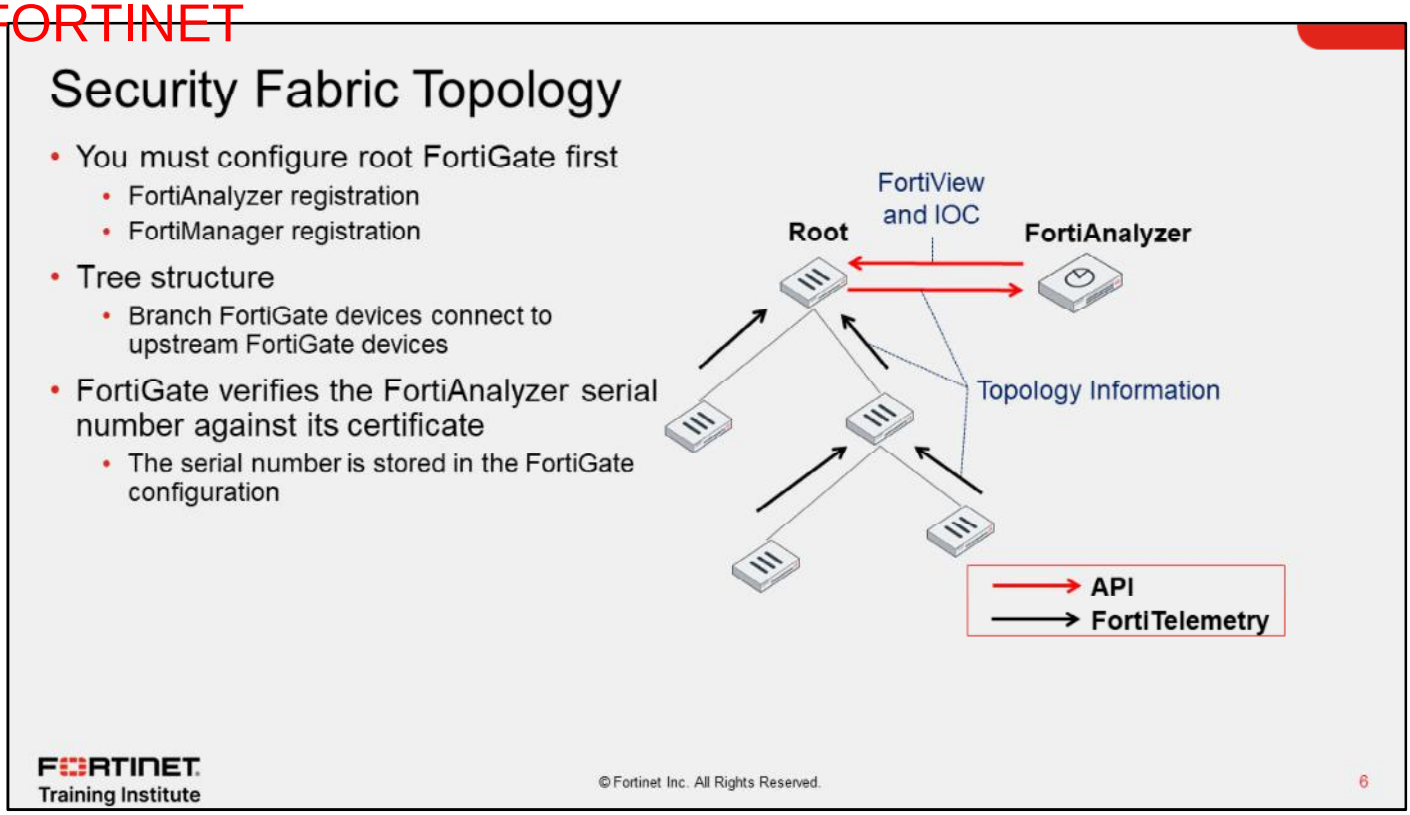
Fabric connectors allow you to integrate multi-cloud support, such as ACI and AWS, to name a few.

In an application-centric infrastructure (ACI), the SDN connector serves as a gateway bridging SDN controllers and FortiGate devices. The SDN connector registers itself to APIC in the Cisco ACI fabric, polls interested objects, and translates them into address objects. The translated address objects and associated endpoints populate on FortiGate.

FortiGate VM supports cloud-init and bootstrapping in various cloud providers, such as Microsoft Azure and Google Cloud Platform (GCP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The Security Fabric follows a tree model. You must configure the root FortiGate first. This includes FortiAnalyzer registration and, if any, FortiManager registration. The branch FortiGate devices connect to upstream FortiGate devices to form the Security Fabric tree. The root FortiGate is typically the NGFW device at the edge of the enterprise network that provides connectivity to service providers, but this is not a requirement for deployment.

All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity. FortiTelemetry uses TCP port 8013. FortiGate uses the FortiTelemetry protocol to communicate with other FortiGate devices and distribute information about the network topology. FortiGate also uses FortiTelemetry to integrate with FortiClient.

The root FortiGate collects the network topology information and forwards it to FortiAnalyzer using the FortiAnalyzer API. FortiAnalyzer combines that information with the logs received from all FortiGate devices to generate different topology views, as well as indicators of compromise (IOC), in cases when endpoints get compromised. FortiAnalyzer sends the topology views and the IOC events to the root FortiGate. You can configure FortiGate to take automatic actions any time it receives an IOC from FortiAnalyzer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Upstream and Downstream FortiGate

```
# diagnose sys csf upstream
Upstream Information:
Serial Number:FGVM010000077649
IP:10.1.0.254
Connecting interface:port1
Connection status:Authorized

# diagnose sys csf downstream
 1:     FGVM010000077646 (10.1.0.1) Management-IP: Management-port:0 parent:
FGVM010000077649
        path:FGVM010000077649:FGVM010000077646
        data received: Y downstream intf:port1 upstream intf:port3 admin-port:443
        authorizer:FGVM010000077649
```

Port connected to root FortiGate

LAN (device detection) port on the downstream FortiGate

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

If a FortiGate device is not the Security Fabric root, you can see which upstream or downstream FortiGate it is connected to, using the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Security Fabric Configuration Synchronization

- FortiAnalyzer, FortiManager, and FortiSandbox configuration is pushed from the root FortiGate:
  - All members send logs to a single FortiAnalyzer
  - All members are managed by the same FortiManager
  - All members use the same FortiSandbox for file inspection where antivirus is applied
- You can disable the configuration synchronization on the downstream devices:

```
config system csf
  set configuration-sync local
end
```

- All fabric members maintain their own security fabric map
  - MAC and IP address of all the connected FortiGate devices and their interfaces

```
# diagnose sys csf neighbor list
   Interface                MAC
------------------------------------
port3                 00:50:56:b6:ad:29
port3                 00:50:56:9f:07:84
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

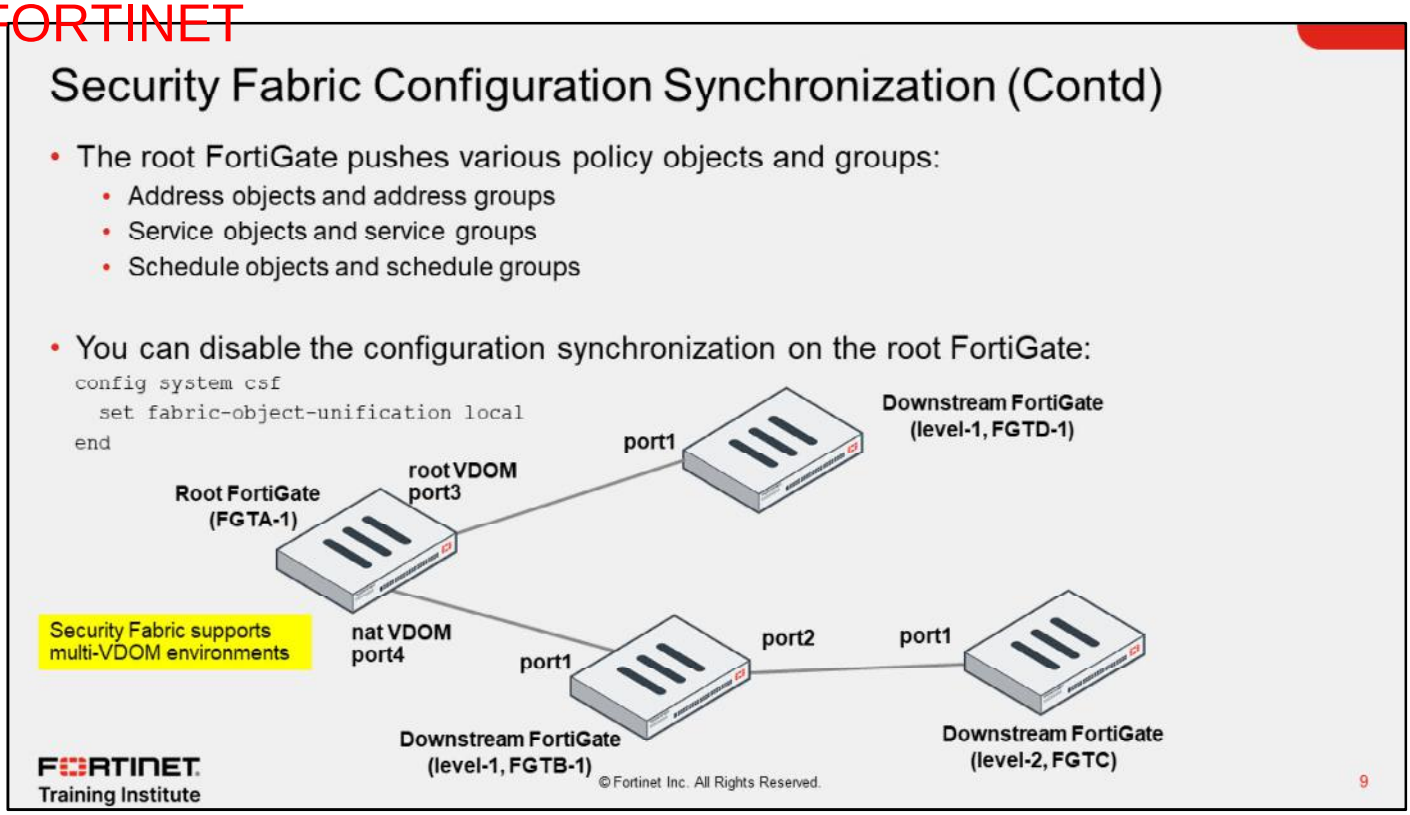
8

By default, in a Security Fabric, all FortiGate devices send logs to a single FortiAnalyzer. FortiAnalyzer is configured on the root FortiGate, which is pushed to all downstream FortiGate devices as they join the Security Fabric. In a similar way, the FortiManager and FortiSandbox configuration is also pushed from the root to all other FortiGate devices. So, all Security Fabric members are managed by the same FortiManager. On the downstream devices, you can disable this configuration and the fabric objects synchronization using the setting `configuration-sync` under `config system csf`.

All FortiGate devices in the Security Fabric maintain their own Security Fabric map. Security Fabric maps include the MAC address and IP address of all connected FortiGate devices and their interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



By default, in a Security Fabric, the root FortiGate pushes global CMDB firewall address objects, address groups, service objects, service groups, schedule objects, and schedule groups to all downstream FortiGate Security Fabric members. This synchronization simplifies policy configuration within the Security Fabric by eliminating the need to create the same objects many times on various FortiGate devices. On the root FortiGate, you can disable this configuration synchronization using the setting `fabric-object-unification` under `config system csf`.

A Security Fabric can be enabled in multi-VDOM environments. This allows access to all of the Security Fabric features, including automation, security rating, and topologies, across the VDOM deployment. In the multi-VDOM setup, downstream FortiGate devices must connect to the upstream FortiGate from its management VDOM.

In the example topology shown on this slide, there is a root FortiGate with three FortiGate devices connected through two different VDOMs. The root (FGTA-1) sends its global CMDB objects to FGTB-1, which has `configuration-sync` set to `local`, so FGTB-1 will not import objects sent by the root. However, FGTB-1 will still forward these messages downstream to FGTC, which has `configuration-sync` set to `default`, so FGTC will receive and synchronize the objects sent from the root FortiGate (FGTA-1).

On the root FortiGate, you can configure individual objects and groups to be locally scoped, the default setting, or global CMDB objects. You can set this option either on the GUI for the object, or on the CLI using the `set fabric-object enable` configuration option. Setting objects or groups to `enable` will make them global CMDB objects, to be distributed to downstream Security Fabric members.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Security Fabric Logging

- Traffic logs are always enabled in all firewall policies
- The Security Fabric, as a whole, logs each session once
  - The first FortiGate that handles a session in the Security Fabric logs the session
  - Any upstream FortiGate that is a member of the Security Fabric does not create duplicate traffic logs for sessions coming from another member's MAC address with the following exceptions:
    - If an upstream FortiGate performs NAT, FortiGate generates another log on that device
    - Upstream FortiGate devices still log UTM events, if configured
- FortiAnalyzer does UTM and traffic log correlation, so that session details, UTM events, reporting and automation in the Security Fabric work correctly

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

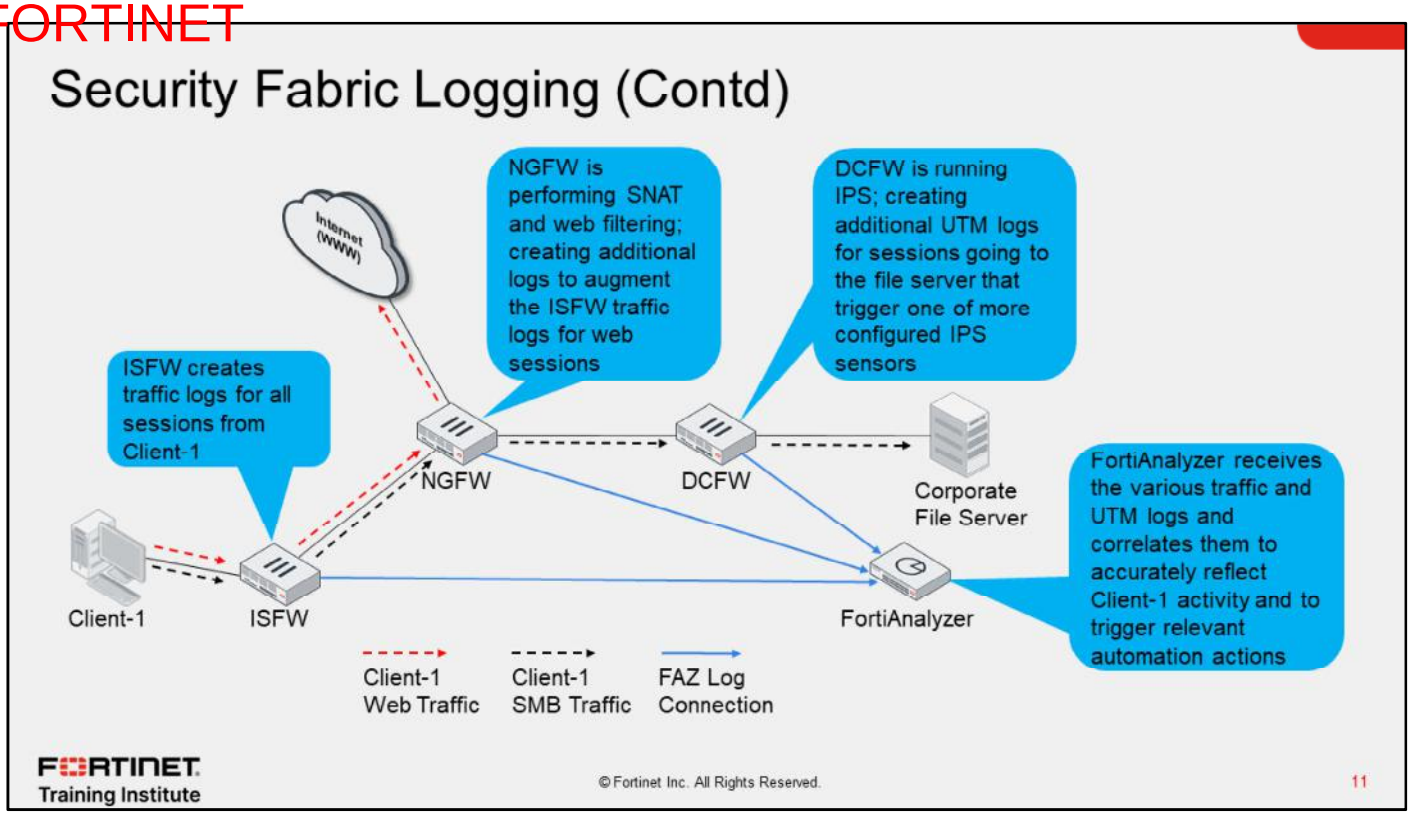
A session's traffic logging is always done by the first FortiGate that handled it in the Security Fabric. FortiGate devices in the Security Fabric know the MAC addresses of their upstream and downstream peers. If FortiGate receives a packet from a MAC address that belongs to another FortiGate in the Security Fabric, it does not generate a new traffic log for that session. This helps to eliminate the repeated logging of a session by multiple FortiGate devices. One exception to the behavior is that if upstream FortiGate performs NAT, then another log is generated. The additional log is needed to record NAT details such as translated ports and/or addresses.

Upstream devices complete UTM logging, if configured, and FortiAnalyzer performs UTM and traffic log correlation for the Security Fabric, in order to provide a concise and accurate record of any UTM events that may occur. No additional configuration is required for this to take place because FortiAnalyzer performs this function automatically.

Note that each FortiGate in the Security Fabric logs traffic to FortiAnalyzer independent of the root or other leaf devices. If the root FortiGate is down, logging from leaf FortiGate devices to FortiAnalyzer continues to function.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows how logging functions in the Security Fabric to give full visibility while eliminating duplicate logs throughout the environment. There are three FortiGate devices configured in a Security Fabric along with a FortiAnalyzer device.

- ISFW is installed in the access layer providing device detection, breach isolation and basic DoS protection from the attached end-user LANs.
- NGFW is installed between the corporate network and their internet service provider where it performs SNAT on outbound communications for RFC-1918 hosts, as well as web filtering for HTTP/HTTPS sessions.
- DCFW is installed in the data center where it runs IPS for all inbound communications to the servers behind it.

All traffic from Client-1 is received by ISFW and it creates traffic logs for the initial session.

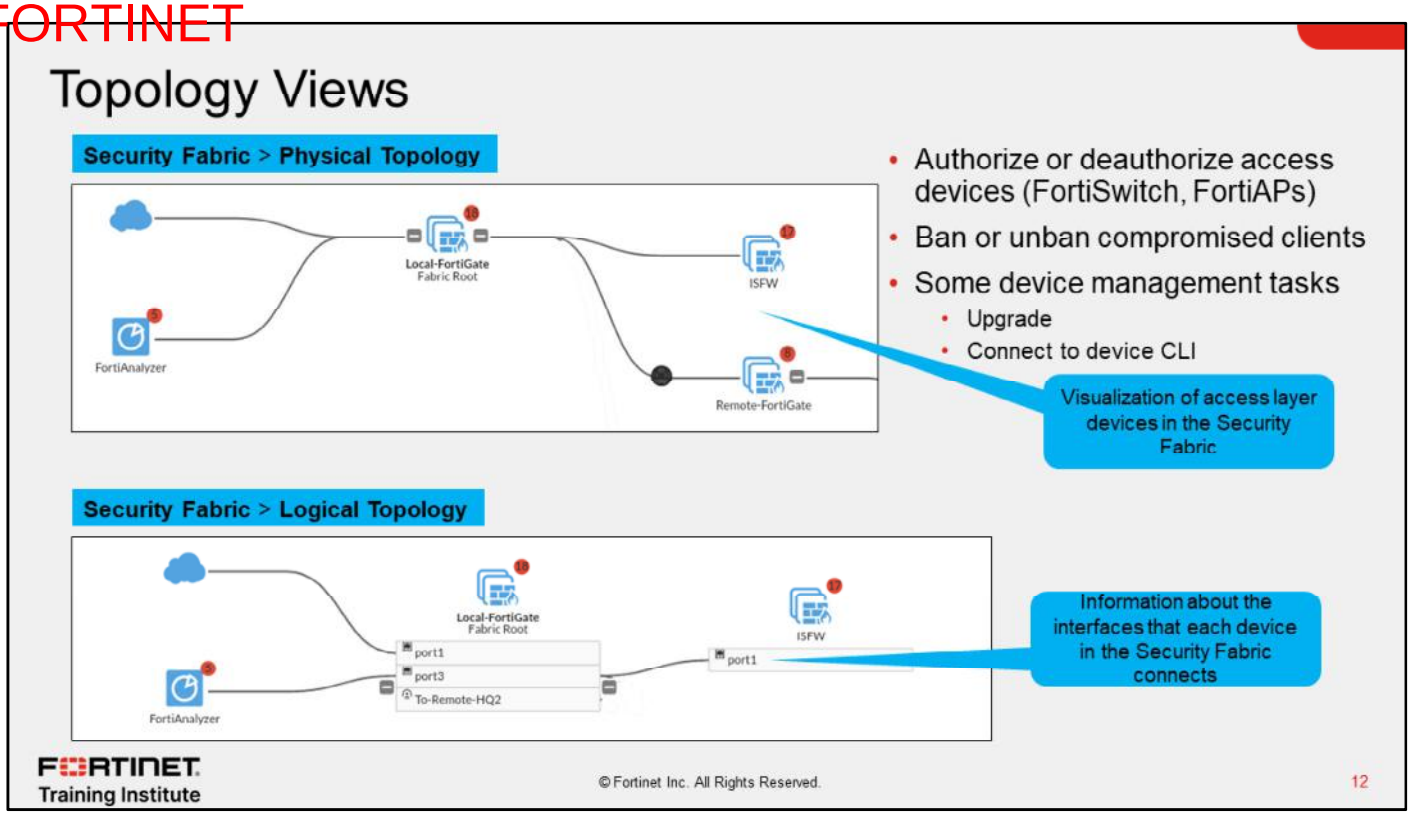
The web session is forwarded to NGFW, which doesn't duplicate the initial traffic log but does generate a traffic log as a result of SNAT being applied to the session. Additionally, NGFW applies a web filtering policy to this session and generates the relevant UTM logs, if appropriate.

The SMB session is forwarded to NGFW, which does not duplicate the initial traffic log. NGFW doesn't need to perform NAT or apply web filtering, so it forwards the traffic to DCFW. DCFW also does not generate a duplicate traffic log, but it performs IPS inspection based on its configuration and, should a signature match be triggered that results in an action generating a log, logs the event.

FortiAnalzyer receives the various traffic and UTM logs, and correlates them automatically so that they are linked for proper viewing, reporting, and automation actions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can view the Security Fabric topology on the root FortiGate GUI. There are two options: **Physical Topology** view and **Logical Topology** view.

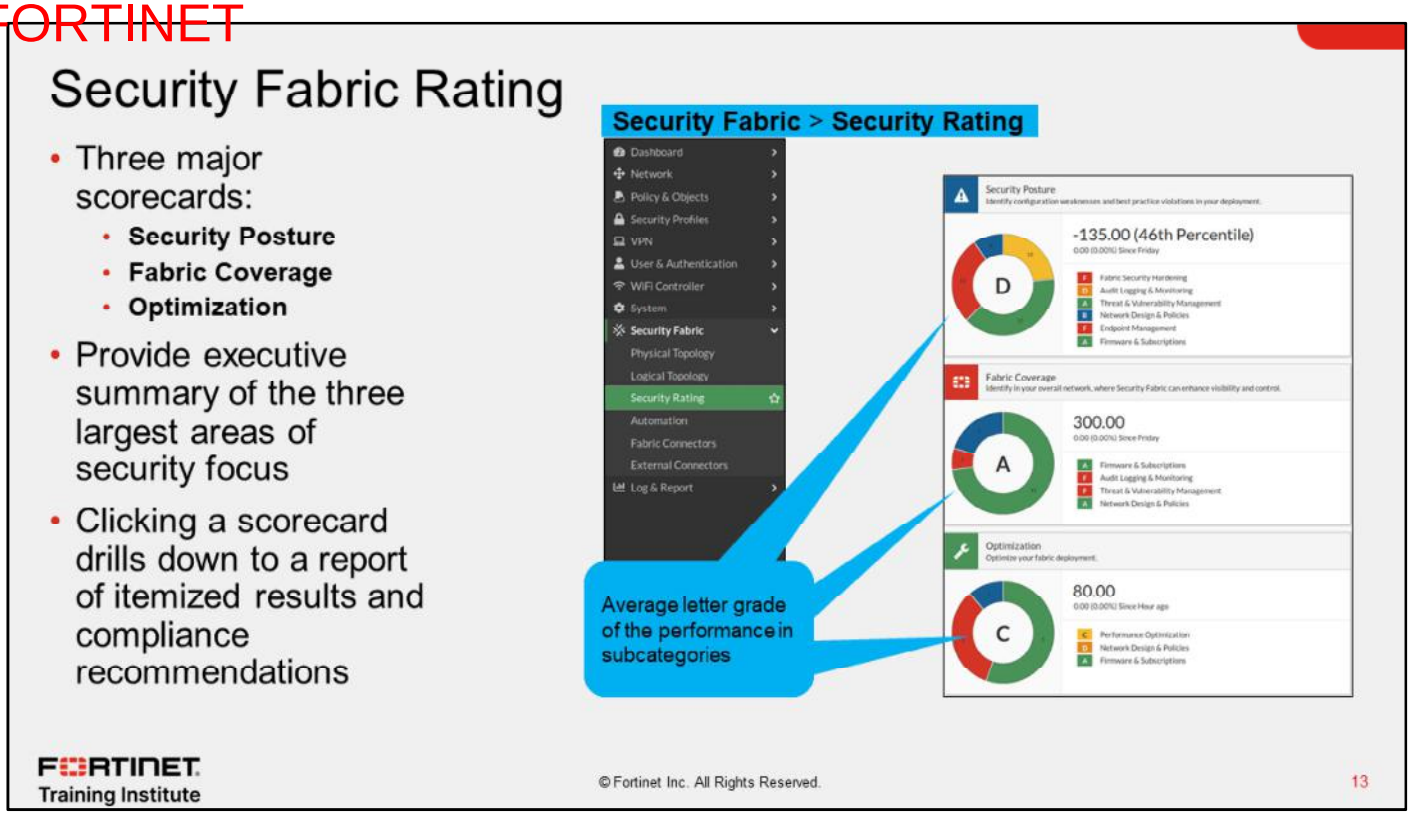
The **Physical Topology** view displays the physical structure of your network, by showing the devices in the Security Fabric and the connections between them. The **Logical Topology** view displays the logical structure of your network, by showing information about logical and physical network interfaces in the Security Fabric and the interfaces that connect devices in the Security Fabric.

The topology views are interactive. You can authorize, and deauthorize access devices, such as FortiSwitch and FortiAP. You can ban or unban compromised clients. You can also perform some device management tasks directly in the topology view, such as device upgrades, or connect to a specific device CLI.

Only Fortinet devices are shown in the topology views.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Security rating is a subscription service that requires a security rating license. This service now provides the ability to perform many *best practices*, including password checks, to audit and strengthen your network security. The **Security Rating** page is separated into three major scorecards:

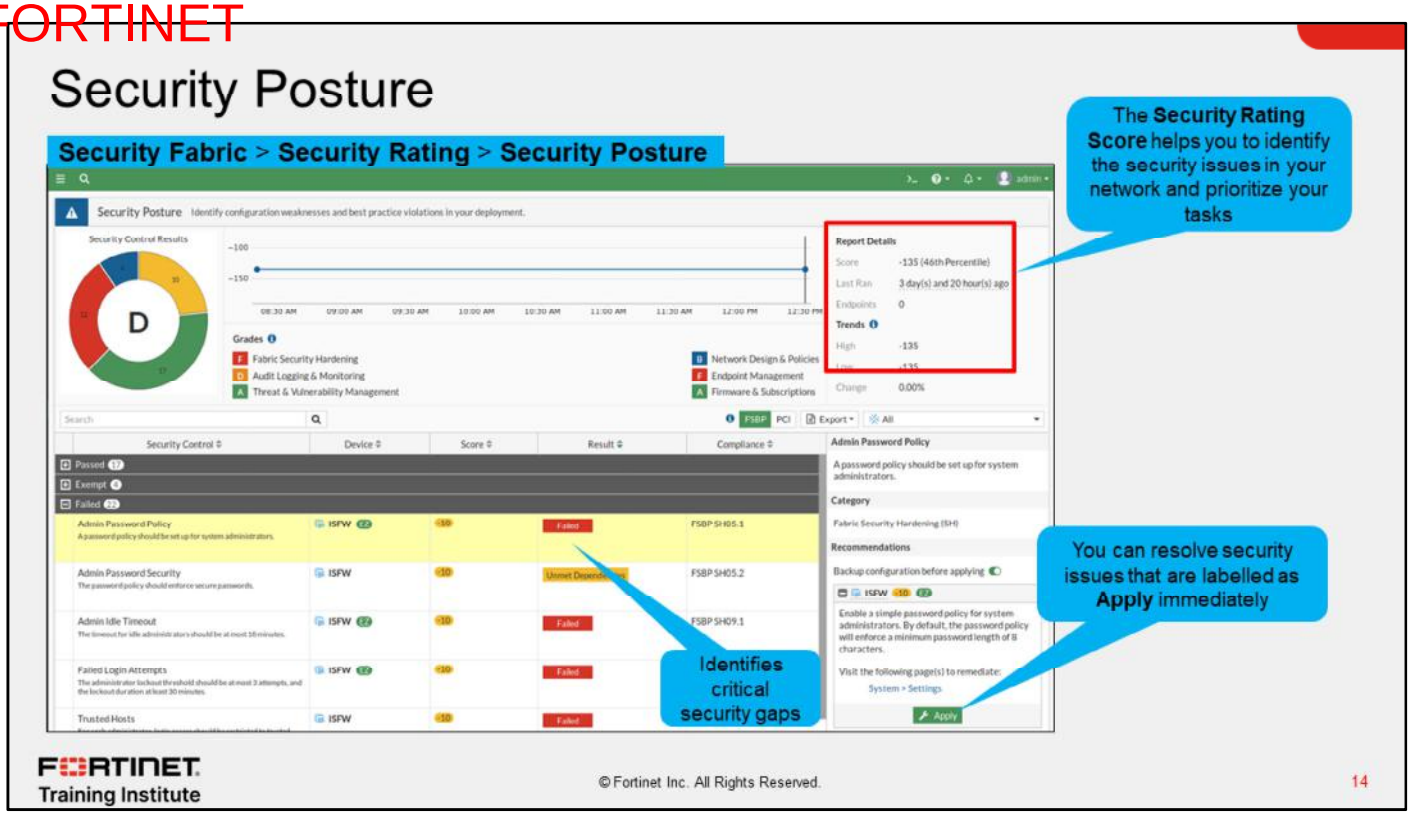
- **Security Posture**
- **Fabric Coverage**
- **Optimization**

These scorecards provide an executive summary of the three largest areas of security focus in the Security Fabric.

The scorecards show an overall letter grade and breakdown of the performance in subcategories. Clicking a scorecard drills down to a detailed report of itemized results and compliance recommendations.
The point score represents the net score for all passed and failed items in that area. The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies. You can click the FSBP and PCI buttons to reference the corresponding standard.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



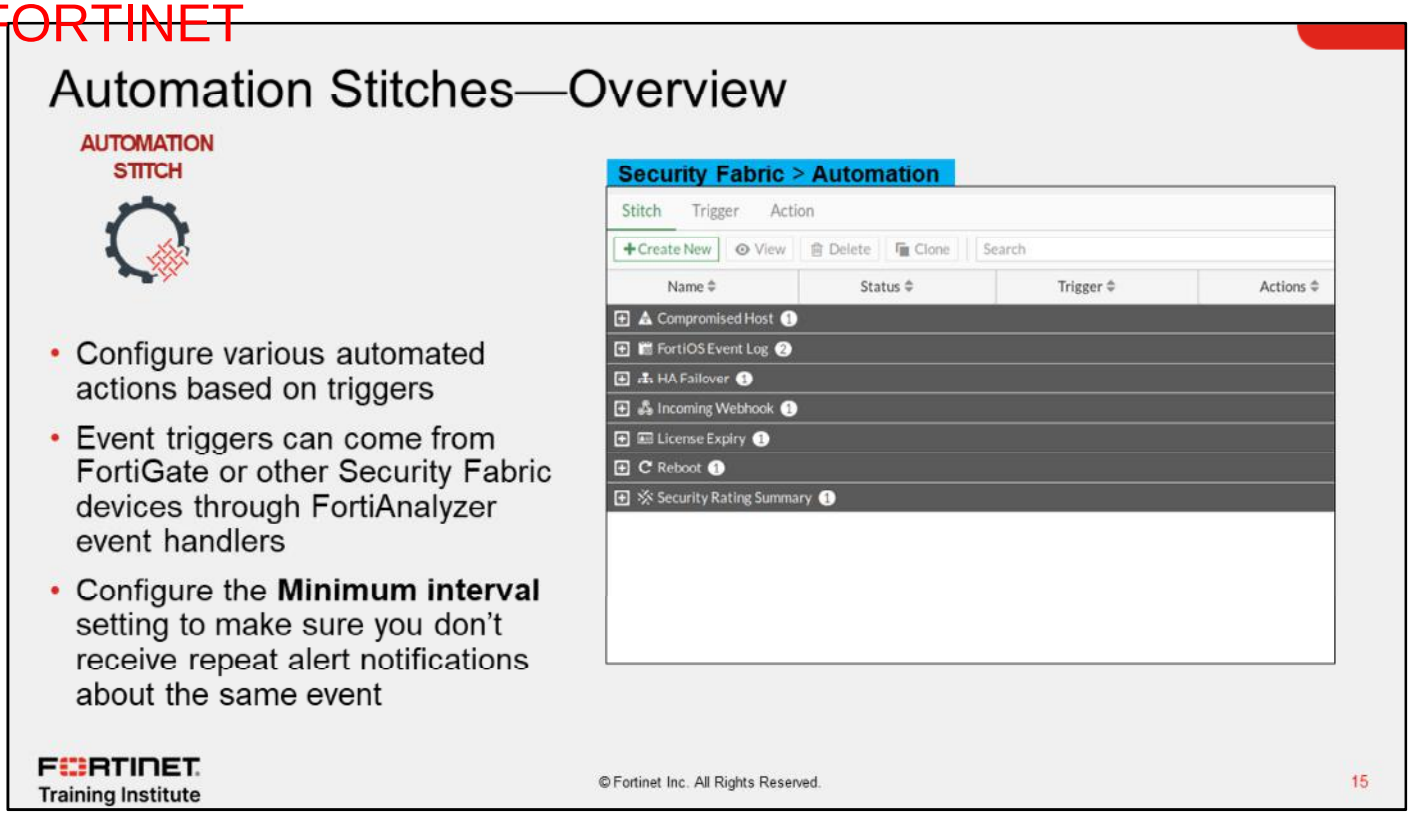
On the **Security Rating** page, click the **Security Posture** scorecard to expand it and see more details.

The security posture service now supports the following:

- Customer ranking based on the security audit information. FortiGuard data is used to provide customer ratings. A customer rating is presented as a percentile. The rating is based on results sent to FortiGuard and statistics received from FortiGuard.
- Security audits running in the background, not just on demand, when an administrator is logged into the GUI. When you view the security audit page, the latest saved security audit data is loaded. From the GUI, you can run audits on demand and view results for different devices in the Security Fabric. You can also view all results or just-failed test results.
- New security checks that can help you make improvements to your organization's network. These checks include enforcing password security, applying recommended login attempt thresholds, encouraging two-factor authentication, and more.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



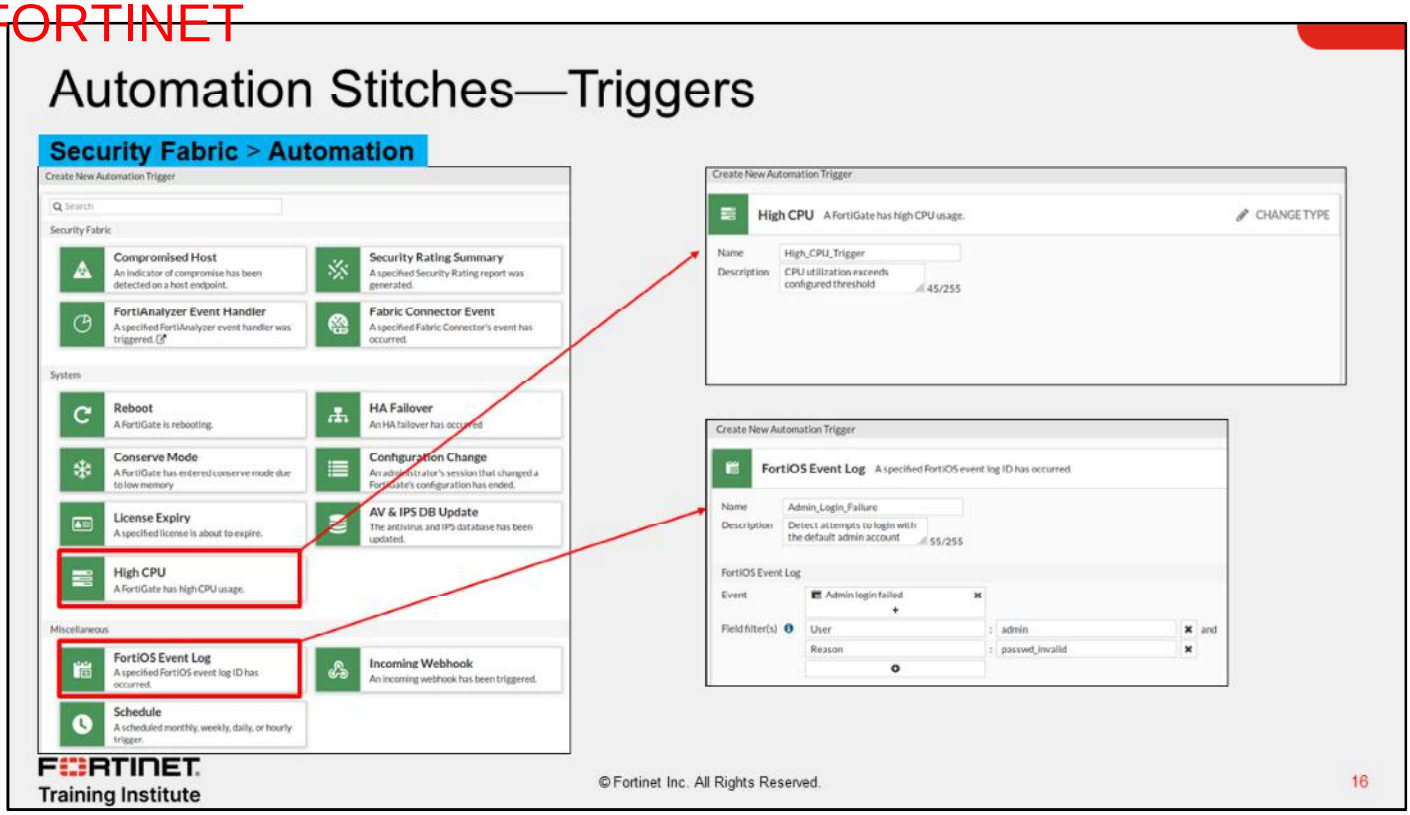
Administrator-defined automated workflows (called stitches) use if/then logic to cause FortiOS to automatically respond to an event in a preprogrammed way. Because this workflow is part of the Security Fabric, you can set up stitches for any device in the Security Fabric. However, a Security Fabric is not a requirement to use stitches. If you configure stitches in a Security Fabric, you must configure them on the root FortiGate. You configure stitches to run on all FortiGate devices in the Security Fabric or a subset of FortiGate devices. Stitches configured on the root FortiGate are pushed to the relevant leaf FortiGate devices. The root FortiGate does not need to be operational for previously configured stitches to function on leaf FortiGate devices.

Each automation stitch pairs an event trigger and one or more actions, which allows you to monitor your network and take appropriate action when the Security Fabric detects a threat or other actionable event. You can use automation stitches to detect events from many sources. Some examples include high CPU, conserve mode, HA failover, reboot, FortiOS event logs with customizable filters, IoCs, and event handlers from FortiAnalyzer.

You can configure the **Minimum interval (seconds)** setting to make sure you don't receive repeat notifications about the same event.

Vouchers & Dumps are Available | WhatsApp +201224560923

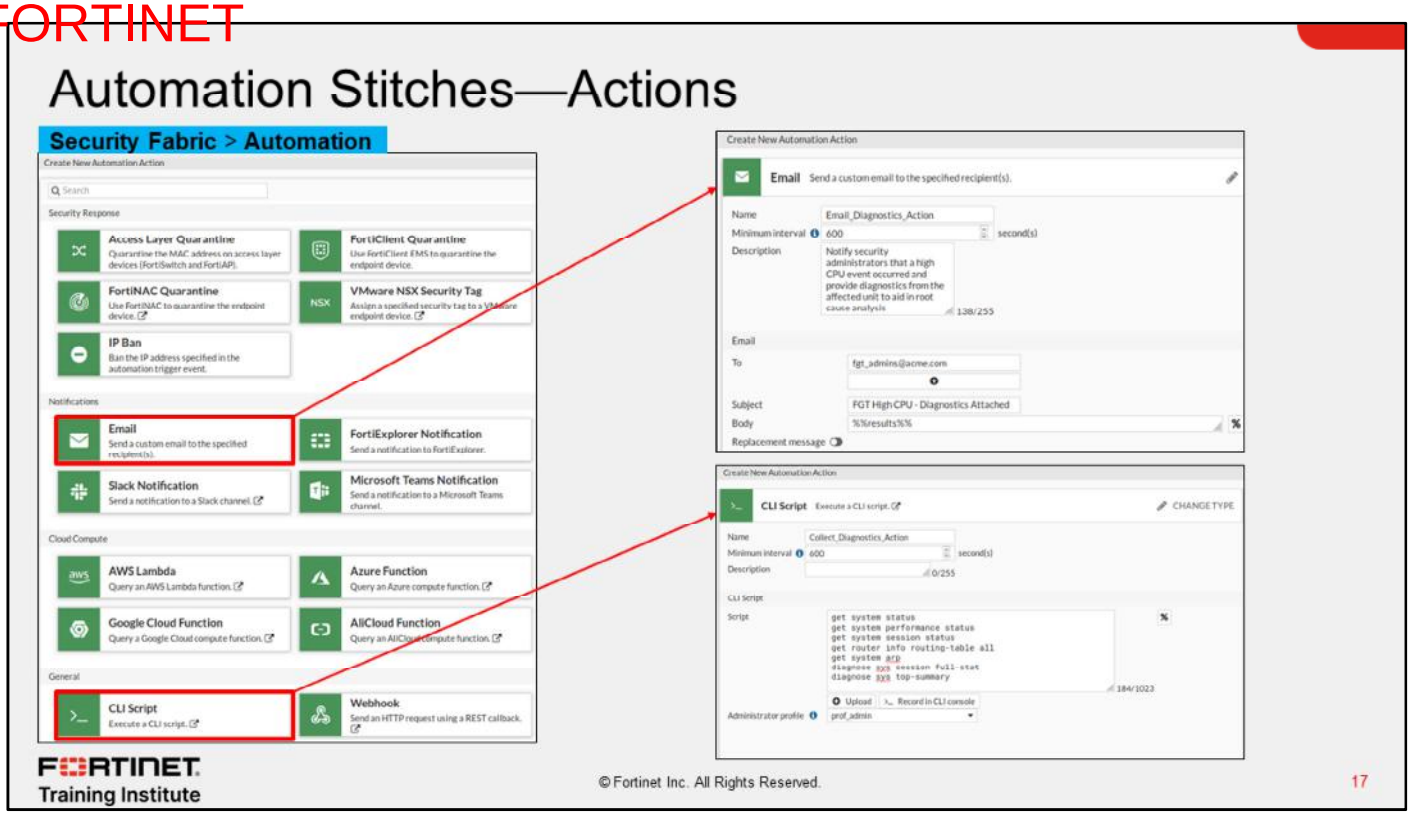
DO NOT REPRINT Brave-dumps.com
© FORTINET



Automation stitches require you to either select a preconfigured or custom automation trigger to define the event that instructs FortiOS to take one or more actions. In the example shown on this slide, two custom automation triggers are being created. One custom trigger, **High_CPU_Trigger**, identifies when the FortiGate exceeds the CPU utilization threshold configured with the `set cpu-usage-threshold` CLI command—which, by default, is 90%. The other custom trigger, **Admin_Login_Failure**, identifies when a user attempts to log in to FortiGate using the default administrator account with an invalid password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



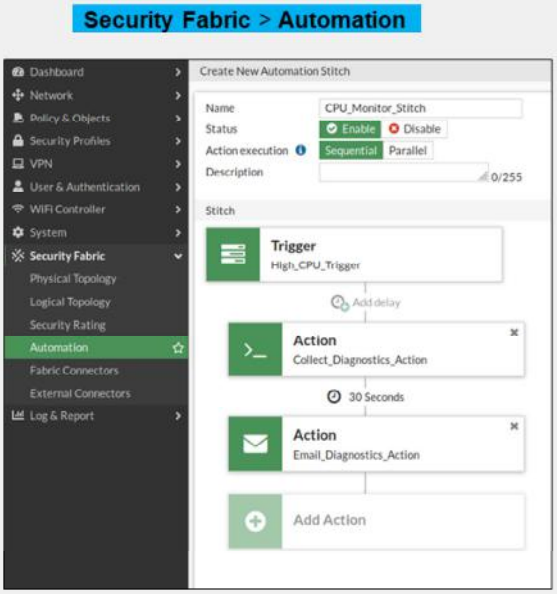
Automation stitches also require you to specify either preconfigured or custom automation actions that define what FortiOS should do based on the defined automation trigger occurring. In the example shown on this slide, two custom automation actions are being created. One custom automation action, **Collect_Diagnostics_Action**, tells FortiOS to run a custom CLI script consisting of various diagnostic commands that help to identify the cause of performance issues on FortiGate. The second automation action, **Email_Diagnostics_Action**, sends an email message to staff to notify them that a FortiGate device has experienced a period of high CPU utilization, and to provide the output of the **Collect_Diagnostics_Action** in the email body so they have the relevant details needed for troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Automation Stitches

- After you define the automation triggers and automation actions, you can create your automation stitch
- You can use multiple automation actions in your stitch.
- There are two types of execution for actions:
  - Sequentially
  - Parallel



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

After you define the automation trigger and actions, you can create the stitch on FortiGate. You must specify a single trigger, then you can add one or more actions to the stitch. The FortiGate GUI displays this as a visual workflow, so you can see the order of operations. When adding multiple actions, you must decide whether the actions should be executed sequentially or in parallel. Sequential execution allows you to configure a delay between actions to allow for tasks to be completed before proceeding to the next action. This is important because when using sequential execution, you can take action parameters from actions that have happened previously and use them as input for the action currently being executed. In the example shown on this slide, the automation stitch is going to execute actions sequentially. Once the **High_CPU_Trigger** occurs, the **Collect_Diagnostics_Action** runs, followed by a 30-second delay before proceeding to the **Email_Diagnostics_Action**. The **Collect_Diagnostics_Action** runs a series of CLI diagnostic commands so the 30-second delay allows time for the commands to finish. **Email_Diagnostics_Action** uses the output of these commands as a parameter, %%results%% , which forms the body of the email message to be sent.

Parallel execution executes all configured actions at the same time as soon as the stitch is triggered. You cannot use action parameters with parallel execution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Testing Stitches

- You can test stitches on the CLI

```
# diagnose automation test <stitch_name>
```

- When an automation stitch is triggered, FortiGate creates an event log

Log & Report > System Events

Add Filter | System Events | Details

Date/Time	Level	User	Message	Log Description
2020/04/27 19:14:39			stitch:AutoBan is triggered.	Automation stitch triggered
2020/04/27 19:14:39			Automation Stitch Test: IOC detected by FortiAnalyzer	Compromised host detected

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

You can test your automation stitch using the command shown on this slide. When an automation stitch is triggered, FortiGate creates an event log.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Use Case 1

- Security Fabric root device can link to FortiClient Endpoint Management System (EMS) for endpoint connectors and automation
- Telemetry and compliance data shared between FortiGate and FortiClient
- EMS helps enhance endpoint visibility, compliance control, vulnerability scanning, and automated response
- Implement ZTNA access control
- ZTNA method uses:
  - Client-device identification
  - Authentication
  - Zero-trust tags
- Provides flexibility to manage both on-fabric and off-fabric users

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

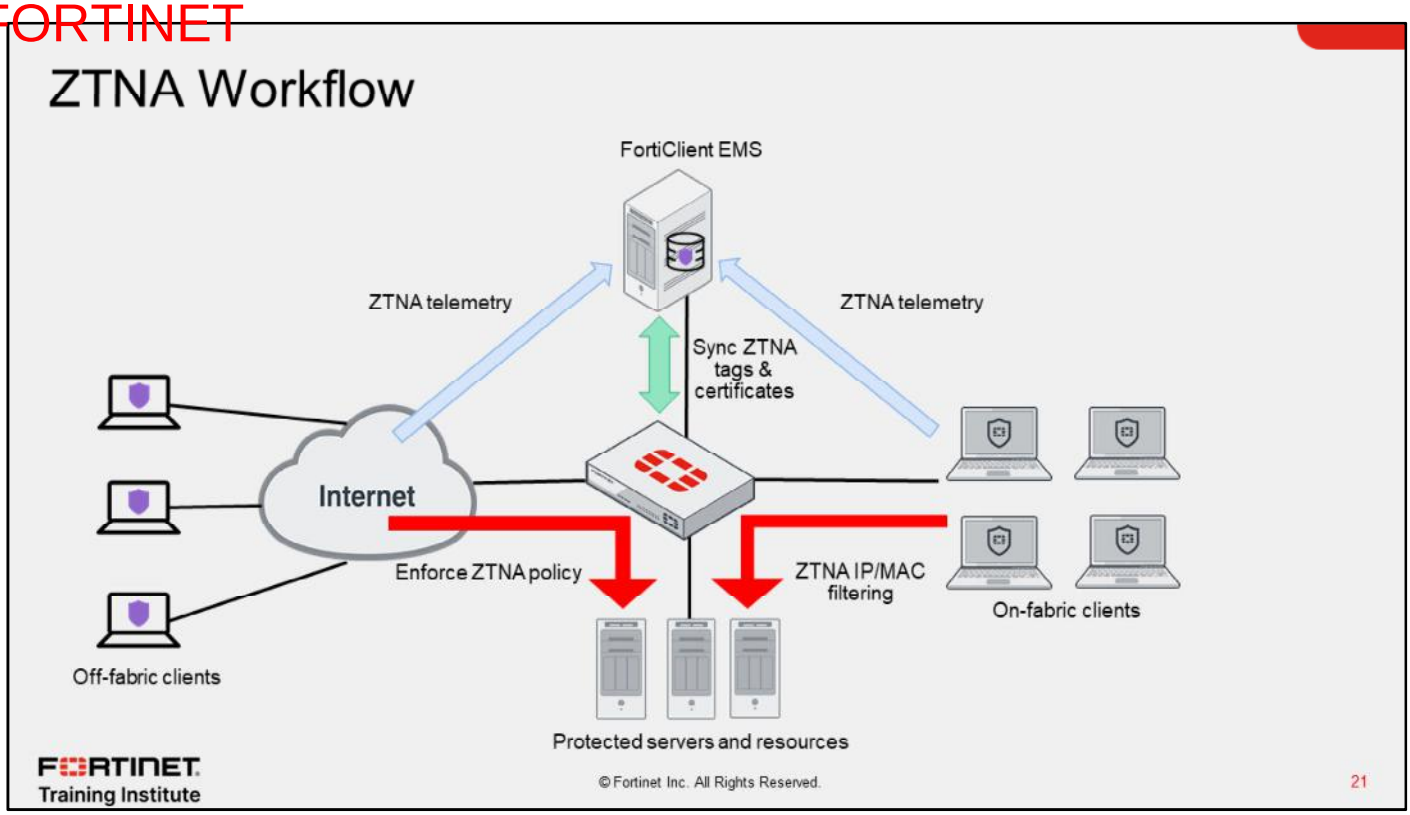
20

The FortiGate Security Fabric root device can link to FortiClient Endpoint Management System (EMS) and FortiClient EMS Cloud (a cloud-based EMS solution) for endpoint connectors and automation. Telemetry and compliance data, provided by FortiClient acting as a fabric agent, is shared between FortiGate and FortiClient EMS to help enhance endpoint visibility, compliance control, vulnerability scanning, and automated response. Using endpoint status information, a security fabric administrator can implement zero trust network access (ZTNA).

ZTNA is an access control method that uses client-device identification, authentication, and zero-trust tags to provide role-based application access. ZTNA gives administrators the flexibility to manage network access for on-fabric local users and off-fabric remote users. ZTNA grants access to applications only after verifying the device, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using zero-trust tags.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide demonstrates ZTNA telemetry, tags, and policy enforcement. You configure ZTNA tag conditions and policies on FortiClient EMS. FortiClient EMS shares the tag information with FortiGate through Security Fabric integration. FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry. FortiGate can then use ZTNA tags to enforce access control rules on incoming traffic through ZTNA access.

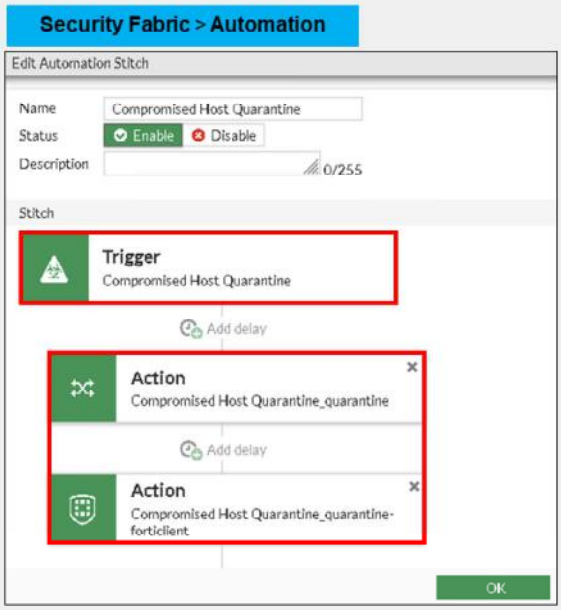
FortiOS also receive the dynamic endpoint groups from EMS. When a change to the dynamic endpoint groups occurs, such as an endpoint being added to or removed from a group, EMS sends the update to FortiOS, and FortiOS updates its dynamic policies accordingly, providing dynamic access control, based on endpoint status.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Quarantine Automation

- You can quarantine an endpoint from FortiOS using EMS using an API
- The following network components are required:
  - FortiGate
  - FortiAnalyzer
  - FortiClient EMS
  - FortiClient
- Security Fabric, which includes the above network devices, can automatically quarantine an endpoint on which an IoC is detected



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

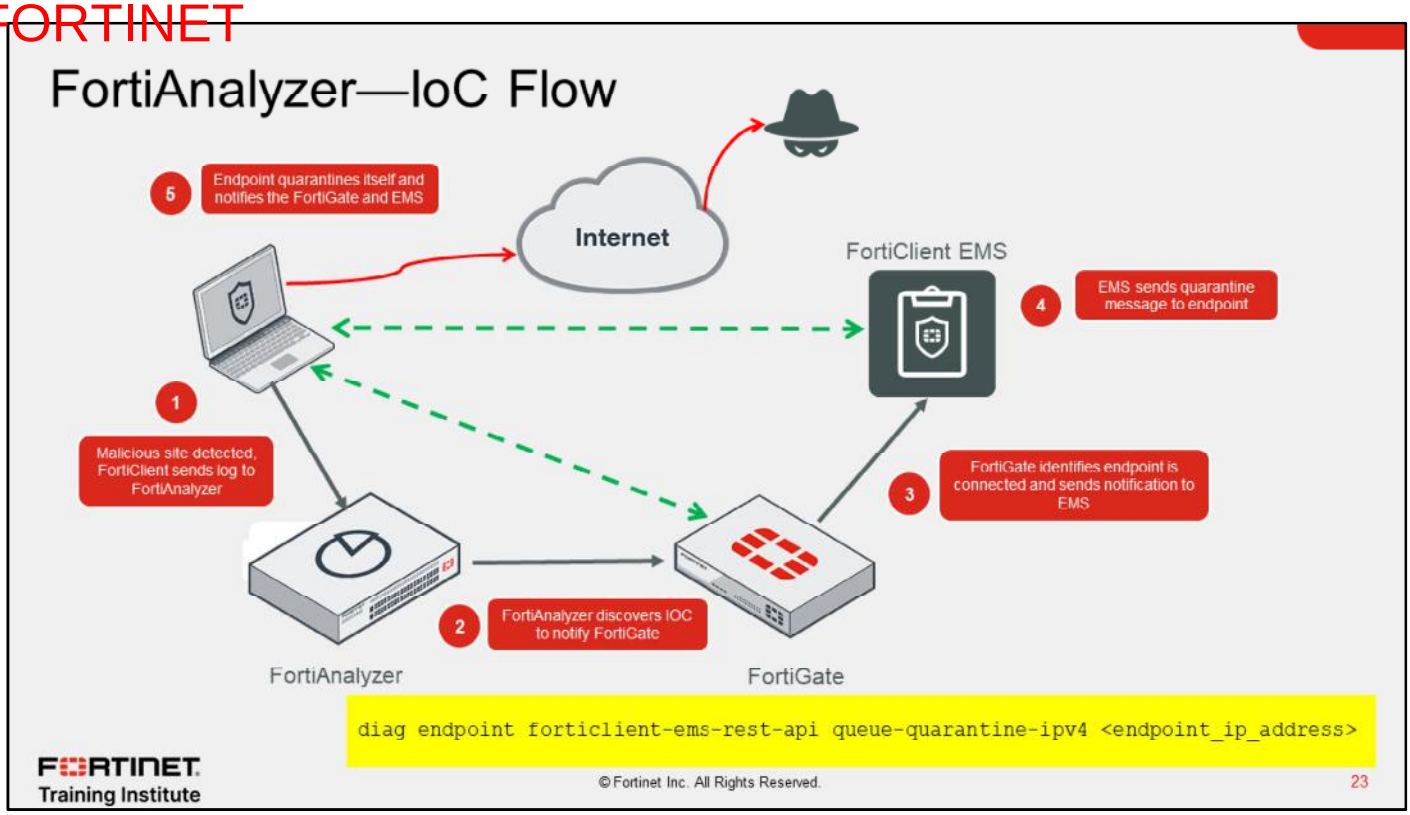
When the Security Fabric includes network devices listed here, you can configure the system to automatically quarantine an endpoint on which an IoC is detected. This requires the following network devices:

- FortiGate
- FortiAnalyzer
- FortiClient EMS
- FortiClient

You must connect FortiClient to both the EMS and FortiGate. FortiGate and FortiClient must both be sending logs to FortiAnalyzer. You must configure the EMS IP address on FortiGate, as well as administrator login credentials.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



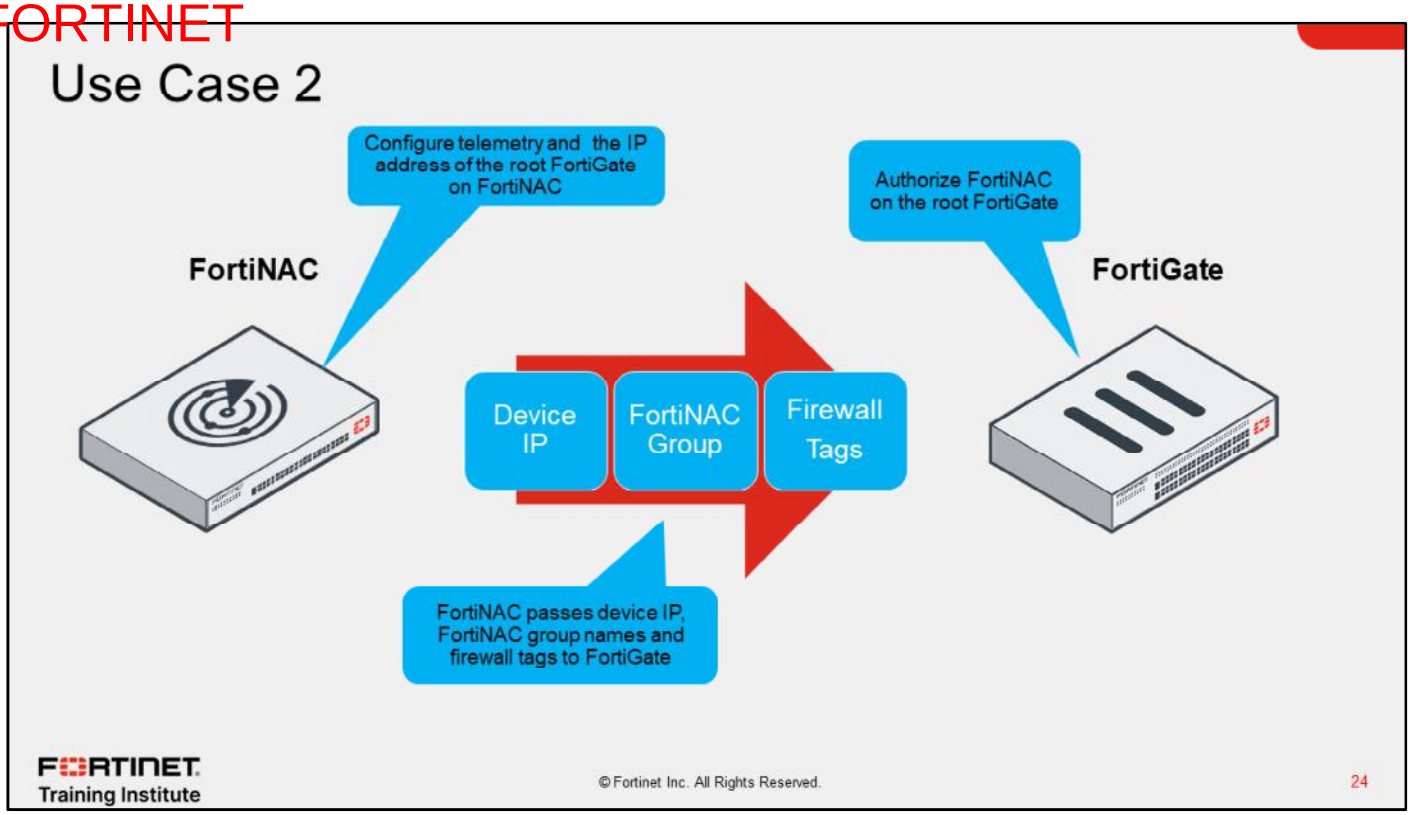
This configuration functions as follows:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies FortiGate.
3. FortiGate identifies if FortiClient is a connected endpoint, and if it has the login credentials for FortiClient EMS that FortiClient is connected to. With this information, FortiGate sends a notification to FortiClient EMS instructing it to quarantine the endpoint.
4. FortiClient EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies FortiGate and EMS of the status change.

The CLI command on the slide triggers the quarantine action on the endpoint at `endpoint_ip_address`: Note that this feature is not supported on FortiClient (Linux).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

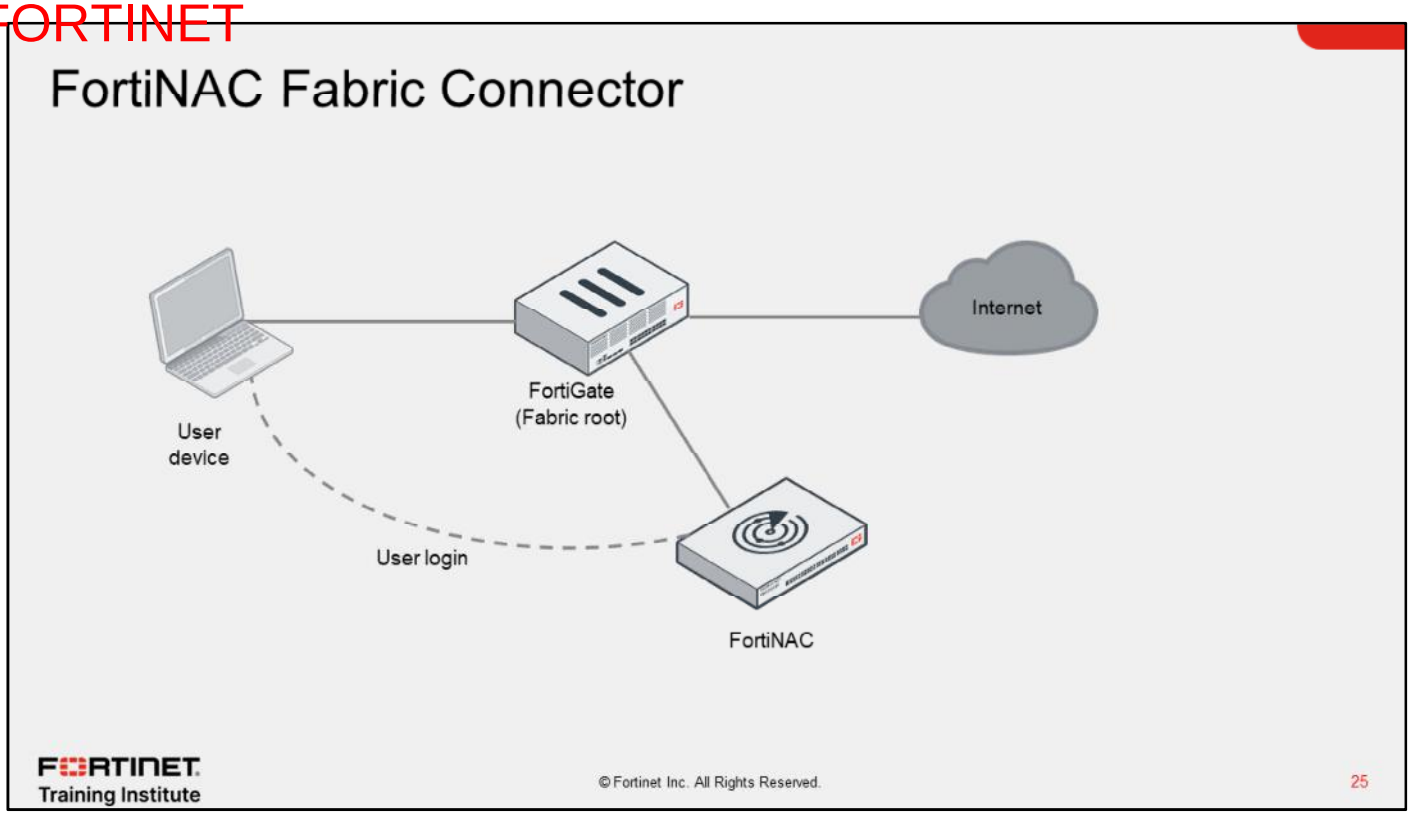


You can deploy FortiNAC as a physical device or as a virtual machine. FortiNAC communicates with infrastructure devices, such as wireless controllers, autonomous APs, switches, routers, and others. Because these infrastructure devices are inline, they can detect connected devices and connecting endpoints. They send this information back to FortiNAC, or FortiNAC gathers this information from them.

A FortiNAC device can be added to the Security Fabric on the root FortiGate. The FortiNAC tag dynamic firewall address type is used to store the device IP, FortiNAC firewall tags, and FortiNAC group information sent from FortiNAC by the REST API when user login and logout events are registered.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In the example on this slide, the user connecting to the network will be required to first log in to FortiNAC. When the login succeeds, the login information is synchronized to FortiGate using the REST API. FortiGate updates the dynamic firewall address object with the user and IP information of the user device. This firewall address is used in firewall policies to dynamically allow network access to authenticated users, thereby allowing SSO for the end user.

To use these FortiNAC tag dynamic firewall addresses, two user login events must trigger on FortiNAC. In FortiOS, you can view the newly created dynamic firewall address in the **FortiNAC Tag (IP Address)** section in **Policy & Objects** > **Addresses**. The dynamic firewall addresses that match the current user login status on FortiNAC have the current IP address of the user devices.

FortiNAC tag dynamic firewall address can be used as the source or destination addresses in the firewall policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case 3

- SSO fabric connectors integrate SSO authentication into the network
- Allows identified users access to multiple applications, without having to re-authenticate
- Users who are already identified can access applications, without being prompted to provide credentials
  - SSO software identifies a user's user ID, IP address, and group membership
  - FortiGate allows access based on membership in SSO groups configured on FortiGate
  - SSO groups can be mapped to individual users, user groups, organizational units (OUs), or a combination of them
- The following fabric connectors are available:
  - Fortinet single sign-on (FSSO) agent
  - Poll Active directory server
  - Symantec endpoint connector
  - RADIUS single sign-on agent
  - Exchange Server connector
- Each SSO method gathers login events differently

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

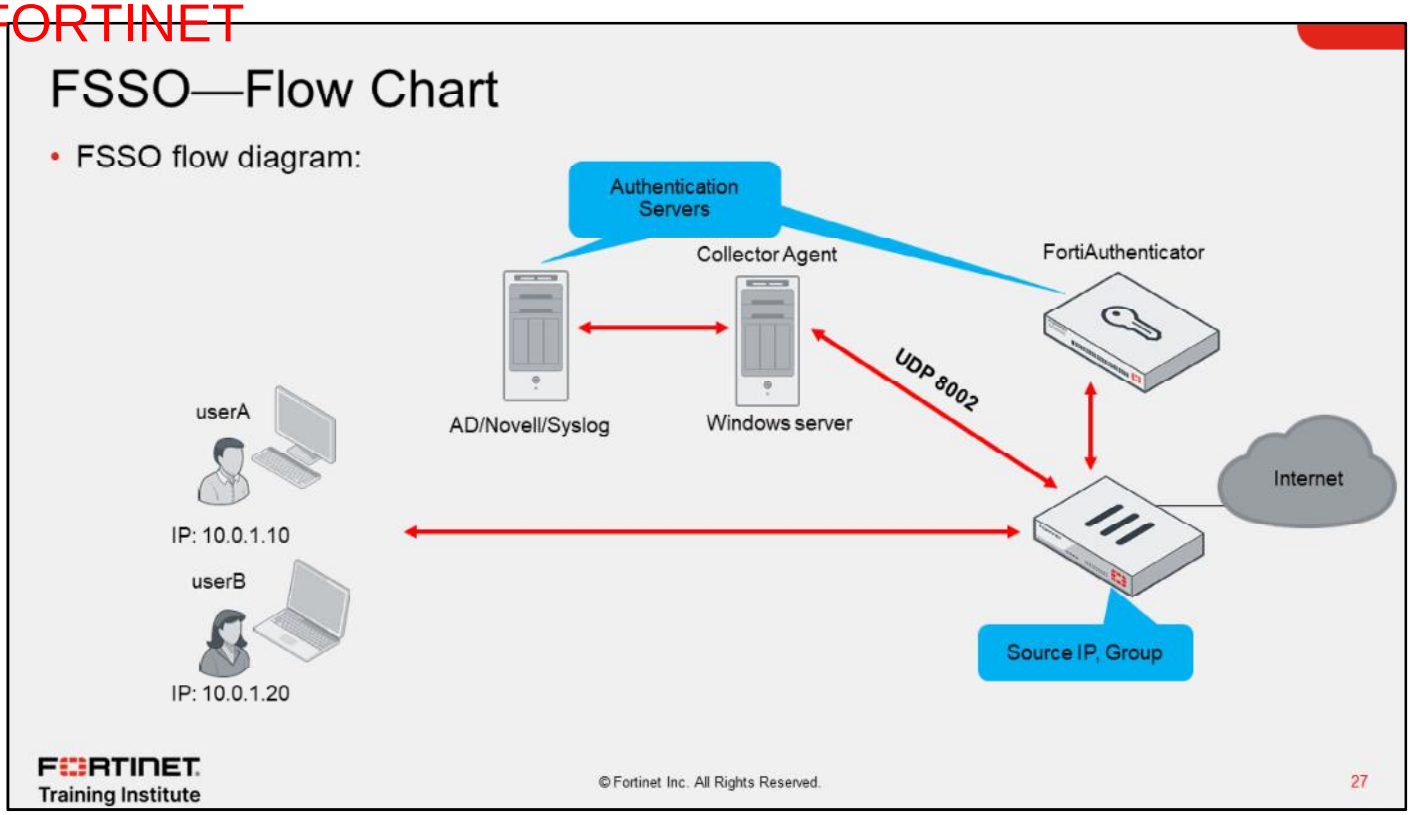
SSO fabric connectors integrate SSO authentication into the network. This allows users to be automatically logged in to every application after being identified, regardless of platform, technology, and domain.

The following fabric connectors are available:
- FSSO agent
- Poll active directory server
- Symantec endpoint connector
- RADIUS single sign-on agent
- Exchange server connector

When a user logs in to a directory service or connector, the SSO agent sends FortiGate the username, the IP address, and/or the list of groups that the user belongs to. FortiGate uses this information to maintain a local database of usernames, IP addresses, and group mappings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

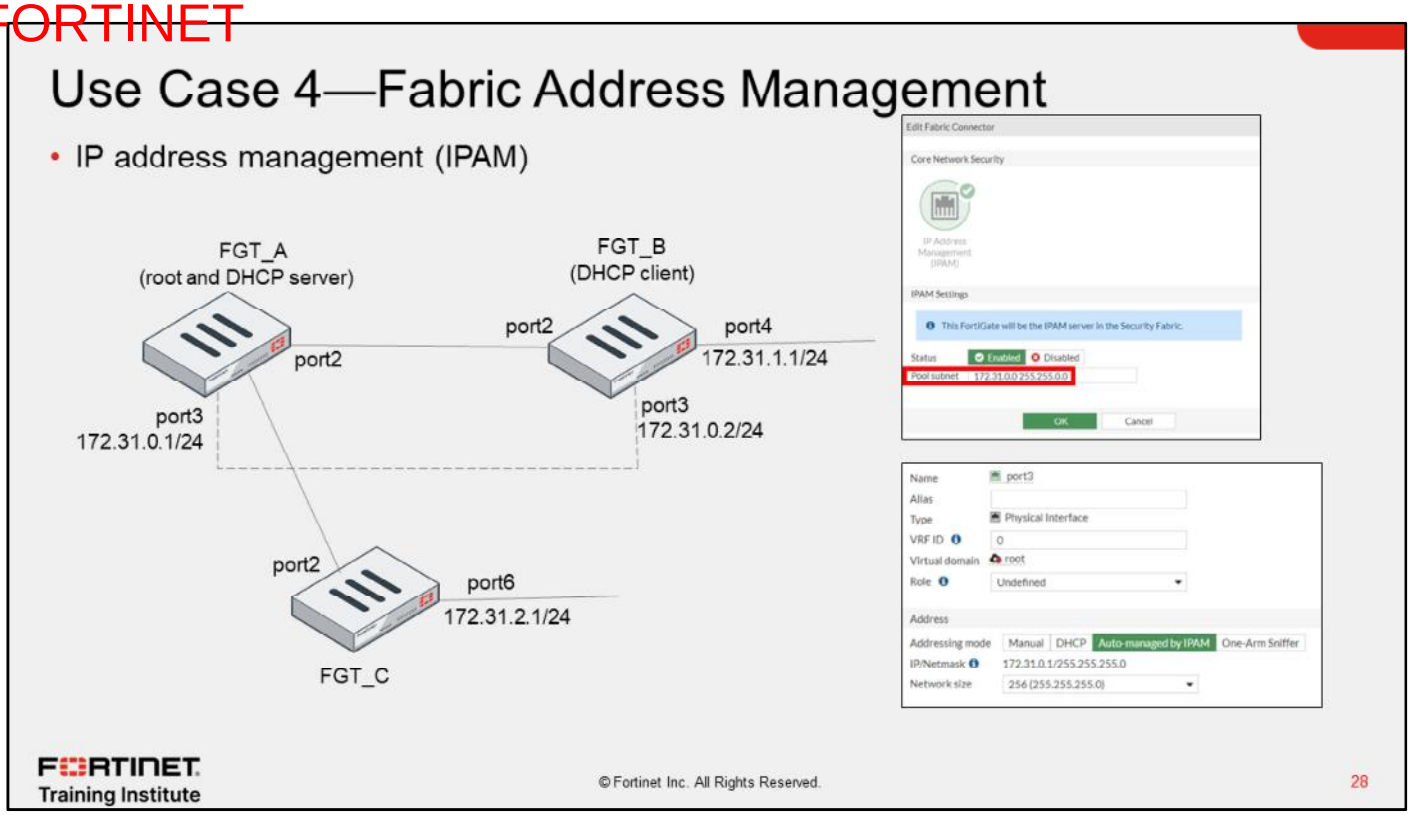


This slide shows the FSSO flow.

FSSO is typically used with directory service networks, such as Windows Active Directory or Novell eDirectory. Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



IPAM is available locally on FortiGate. A fabric root in the Security Fabric, can act as the IPAM server. Interfaces that are configured to be automanaged by IPAM will receive an address from the IPAM server's address/subnet pool. The DHCP Server is automatically enabled in the GUI, and the address range is populated by IPAM. Users can customize the address pool subnet and the size of a subnet that an interface can request.

In the example shown on this slide, FGT_A is the Security Fabric root with IPAM enabled. FGT_B and FGT_C are downstream fabric devices and retrieve IPAM information from FGT_A. The fabric interface on all FortiGate devices is port2. FGT_A acts as the DHCP server, and FGT_B and FGT_C acts as the DHCP client.

IPAM is managing a `172.31.0.0/16` network and assigns ports a /24 network by default, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Explore the Fortinet Security Fabric
- ✓ Diagnose the Security Fabric operation
- ✓ Perform a security rating audit
- ✓ Configure automation stitches
- ✓ Identify Security Fabric use cases based on different scenarios

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

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

By mastering the objectives covered in this lesson, you learned about the Fortinet Enterprise Firewall solution and the Fortinet Security Fabric.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

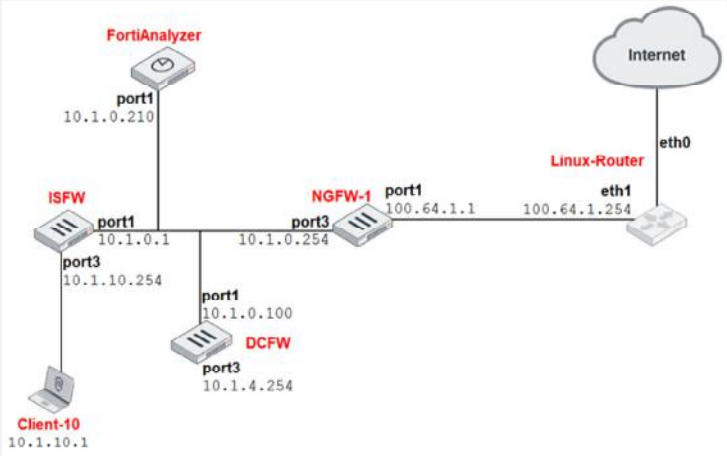
Now, you will work on *Lab 3–Security Fabric*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 3—Security Fabric

- The Security Fabric follows a tree topology
- NGFW-1 will be the root of the tree and ISFW and DCFW will be branches
- On NGFW-1, DCFW, and ISFW you will:
  - Enable device detection
  - Enable Security Fabric
  - Enable Security Fabric automation stitch



FORTINET Training Institute

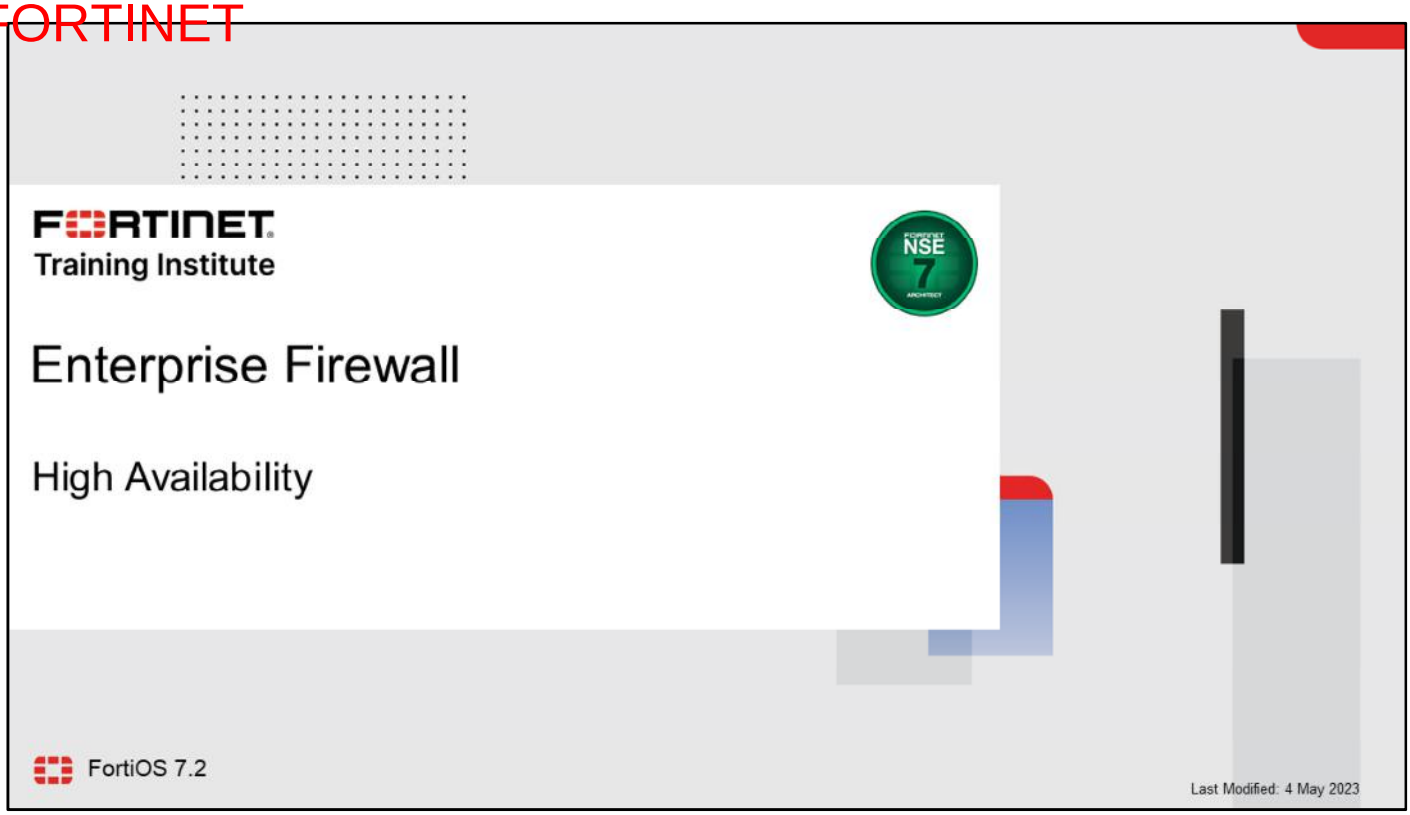
© Fortinet Inc. All Rights Reserved.

31

In the first exercise, you will configure the Security Fabric on NGFW-1 and DCFW. The Security Fabric follows a tree topology. NGFW-1 will be the root of the tree, and ISFW and DCFW will be branches.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to troubleshoot high availability (HA) issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Describe how HA virtual MAC addresses are assigned
- Monitor an HA cluster
- Check the status of the HA configuration and session synchronization
- Discuss FortiGate Clustering Protocol (FGCP) virtual clustering
- Discuss FortiGate Session Life Protocol (FGSP)
- Discuss VRRP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

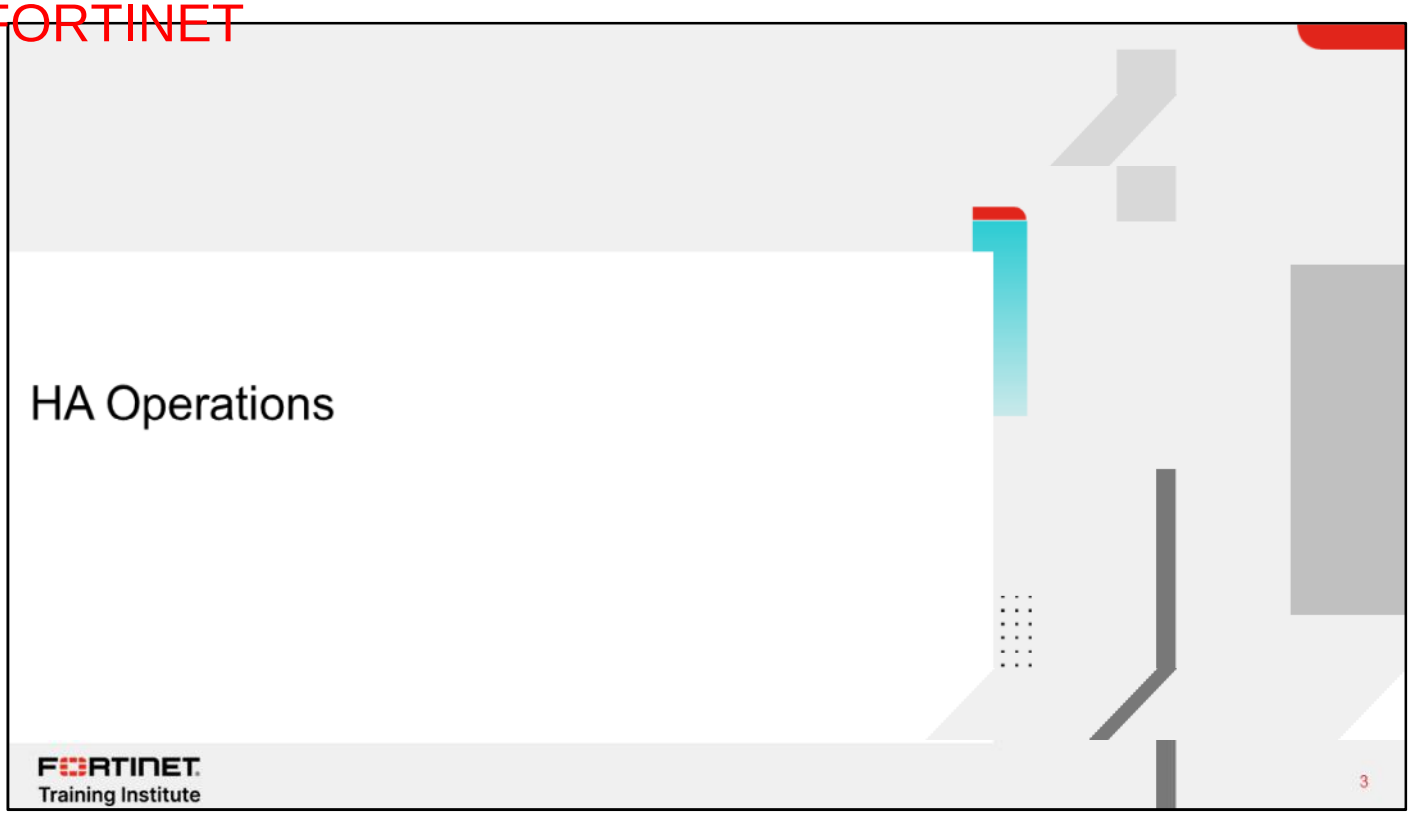
2

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

By demonstrating competence in HA, you will be able to monitor and troubleshoot common HA problems, unexpected reboots, and frozen devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



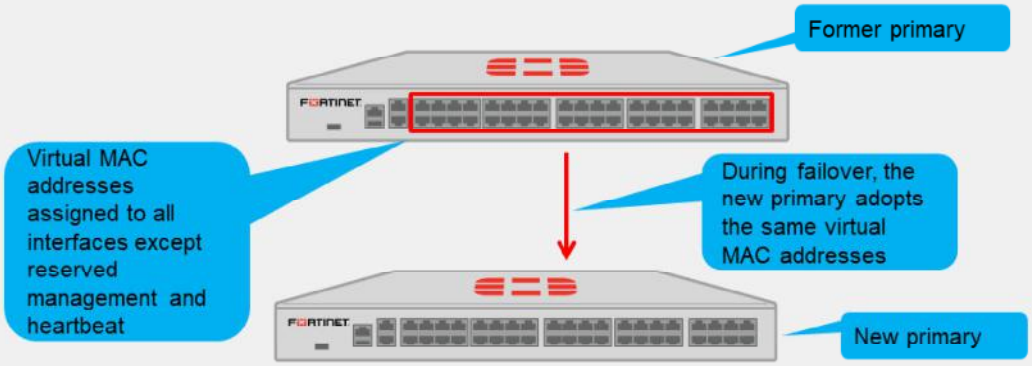
In this section, you will review HA operations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Virtual MAC Addresses and Failover

- On the primary device, each interface—except HA heartbeat interfaces and reserved management interfaces—is given a virtual MAC address
- Upon failover, the newly elected primary adopts the same virtual MAC addresses as the former primary



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses. When a primary joins an HA cluster, FortiGate gives each interface a virtual MAC address. The primary informs all secondary devices about the assigned virtual MAC addresses. Upon failover, a secondary adopts the same virtual MAC addresses for equivalent interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

How the Virtual MAC Addresses Are Assigned

- FortiGate determines the virtual MAC address using the following formula:
  `<group-prefix>:<group-id_hex>:(<vcluster_integer> + <idx>)`
  - `group-prefix` is determined by the set of group IDs:
    - Set 1: group IDs `0 - 255`: group prefix `00:09:0f:09`
    - Set 2: group IDs `256 - 511`: group prefix `e0:23:ff:fc`
    - Set 3: group IDs `512 - 767`: group prefix `e0:23:ff:fd`
    - Set 4: group IDs `768 - 1023`: group prefix `e0:23:ff:fe`
  - `Group-id_hex` is the HA group ID converted to hexadecimal
  - `vcluster_integer` is 0x00 for virtual cluster 1 and 0x80 for virtual cluster 2
  - `idx` is the interface index number
    - Interfaces are numbered from `0` to `x` (where `x` is the number of interfaces)
- Therefore, two or more HA clusters in the same LAN segment should use different HA group IDs, to prevent virtual MAC address conflicts

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

FortiGate determines the HA virtual MAC addresses assigned to each interface by the HA group prefix, group ID, the virtual cluster ID, and the interface index. Group prefix is determined by the set of group IDs as shown on this slide.

The `<vcluster_integer>` field is `00` for virtual cluster 1, and `80` for virtual cluster 2. If VDOMs are not enabled, HA sets the virtual cluster to 1 and by default all interfaces are in the root VDOM.

So, if you have two or more HA clusters in the same broadcast domain, and using the same HA group ID, you might get MAC address conflicts. For those cases, it is strongly recommended that you assign different HA group IDs to each cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Verifying the HA Virtual MAC Address

```
# diagnose hardware deviceinfo nic port1
Name:              port1
Driver:            vmxnet3
Version:           1.4.a.0-k-NAPI
Bus:               0000:03:00.0
Hwaddr:            00:09:0f:09:02:00
Permanent Hwaddr:00:0c:29:68:18:03
...
```

During HA operation, the current hardware address becomes the HA Virtual MAC address

Physical MAC address

FORTINET Training Institute

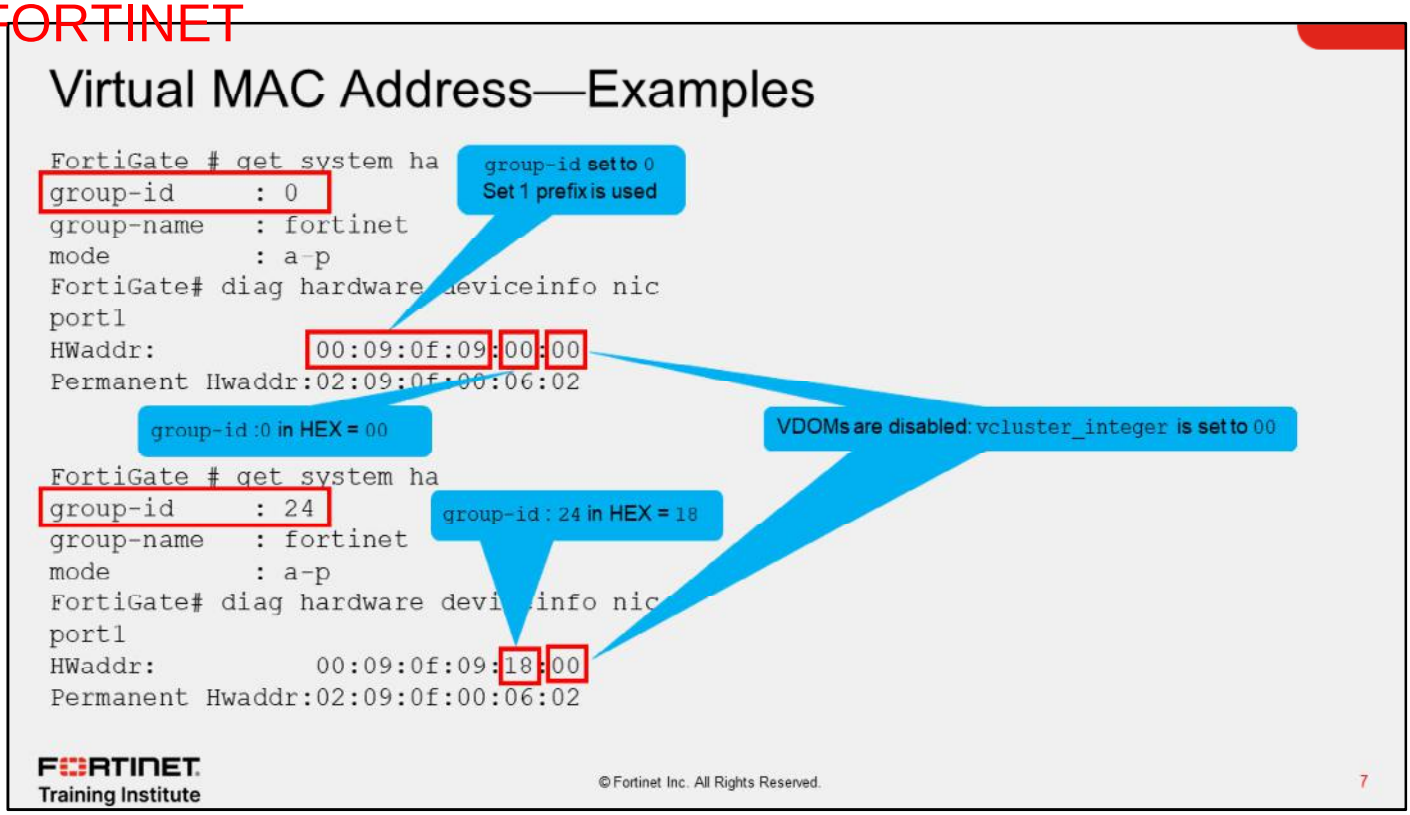
© Fortinet Inc. All Rights Reserved.

6

You can use the command shown on this slide to display the HA virtual MAC address assigned to an interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The examples on the slide show the difference between virtual MAC addresses based on `group-id`. As group ID `0` or `24` belongs to set 1, VMAC prefix is set to `00:09:0f:09`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Virtual MAC Address—Examples (Contd)

```
FortiGate # get system ha
group-id      : 256
group-name    : fortinet
mode          : a-p
FortiGate# diag hardware deviceinfo nic
port5
HWaddr:           e0:23:ff:fc:00:04
Permanent Hwaddr:02:09:0f:00:06:02

FortiGate # get system ha
group-id      : 256
group-name    : fortinet
mode          : a-p
FortiGate# diag hardware deviceinfo nic
port7
HWaddr:           e0:23:ff:fc:00:86
Permanent Hwaddr:02:09:0f:00:06:02
```

group-id set to 256
Set 2 prefix is used

VDOMs are enabled vcluster_integer is set to 00 as root vdom includes port5 with index number 4

VDOMs are enabled: vcluster_integer is set to 80 as other vdom includes port7 with index number 6

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

In this example, virtual MAC prefix has changed to `e0:23:ff:fc` as set 2 is used for the group ID. Also, VDOMs are enabled and the root VDOM contains port5(virtual cluster 1) and other VDOM contains port7(virtual cluster 2). Therefore, last octet of the MAC address includes `vcluster_integer` 0 for the port 5 and 80 for the port 7.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Virtual MAC Addresses and Failover

- After a failover, gratuitous ARP informs the network that the virtual MAC addresses are now reachable through a different device
- Some switches might not clear their MAC tables fast enough, so they would keep sending packets to the former primary device
- To shut down the interfaces of the former primary FortiGate (except the heartbeats and reserved management) for one second during failover, use the following commands:

```
config system ha
 set link-failed-signal enable
end
```

- Because of the link outage, all switches detect the failure and clear their MAC tables

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

After a failover, the new primary broadcasts gratuitous ARP packets, notifying the network that each virtual MAC address is now reachable through a different switch port.

In most networks, that's enough for the switches to update their MAC forwarding tables with the new information. However, some high-end switches might not clear their MAC tables correctly after a failover. So, they keep sending packets to the former primary even after receiving the gratuitous ARPs. In these cases, you should use the command shown on this slide to force the former primary to shut down all its interfaces for one second when the failover happens, excluding heartbeat and reserved management interfaces. This simulates a link failure that clears the related entries from the MAC table of the switches.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate Clustering Protocol

- Ethernet type 0x8890 (NAT/Route) or 0x8891 (transparent)
  - Heartbeats
  - Discover other FortiGate devices in the same HA group
  - Elect the primary
  - Synchronize other data
  - Detect when a device fails
- Ethernet type 0x8893
  - Configuration synchronization
- For example, to sniffer HA heartbeat packets for a NAT/route mode cluster:

```
# diagnose sniff packet any "ether proto 0x8890" 4
```

- Dedicated session synchronization interfaces
  - `set session-sync-dev <interface1> <interface2>`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

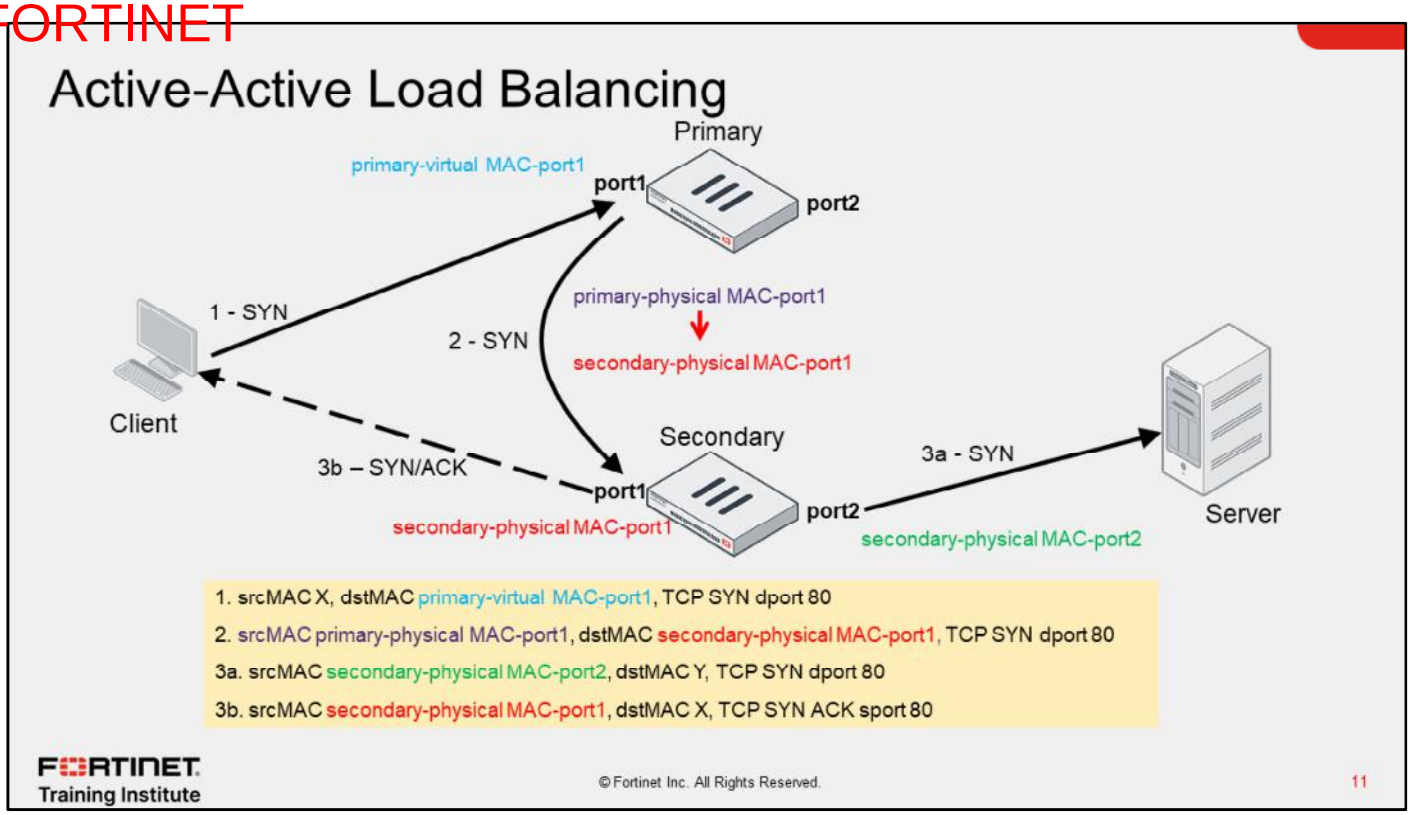
FortiGate HA uses the FGCP, for HA-related communications. FGCP travels among the clustered FortiGate devices over the links that you have designated as the heartbeats.

The FGCP traffic uses a different Ethernet type than the IP protocol. It actually uses three different Ethernet types, depending on the operation mode (transparent or NAT/route).

When session synchronization is enabled, you can also select dedicated interfaces in the HA setup for synchronizing sessions. By default, session synchronization occurs over the HA heartbeat link. Dedicated synchronization links reduce the bandwidth requirements of the HA heartbeat interface and improve the efficiency and performance of the cluster specifically false failover due to a larger number of sessions. If you select multiple interfaces, session synchronization traffic is load balance among the selected interfaces. If all of the session synchronization interfaces become disconnected, session synchronization falls back to using the HA heartbeat link.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



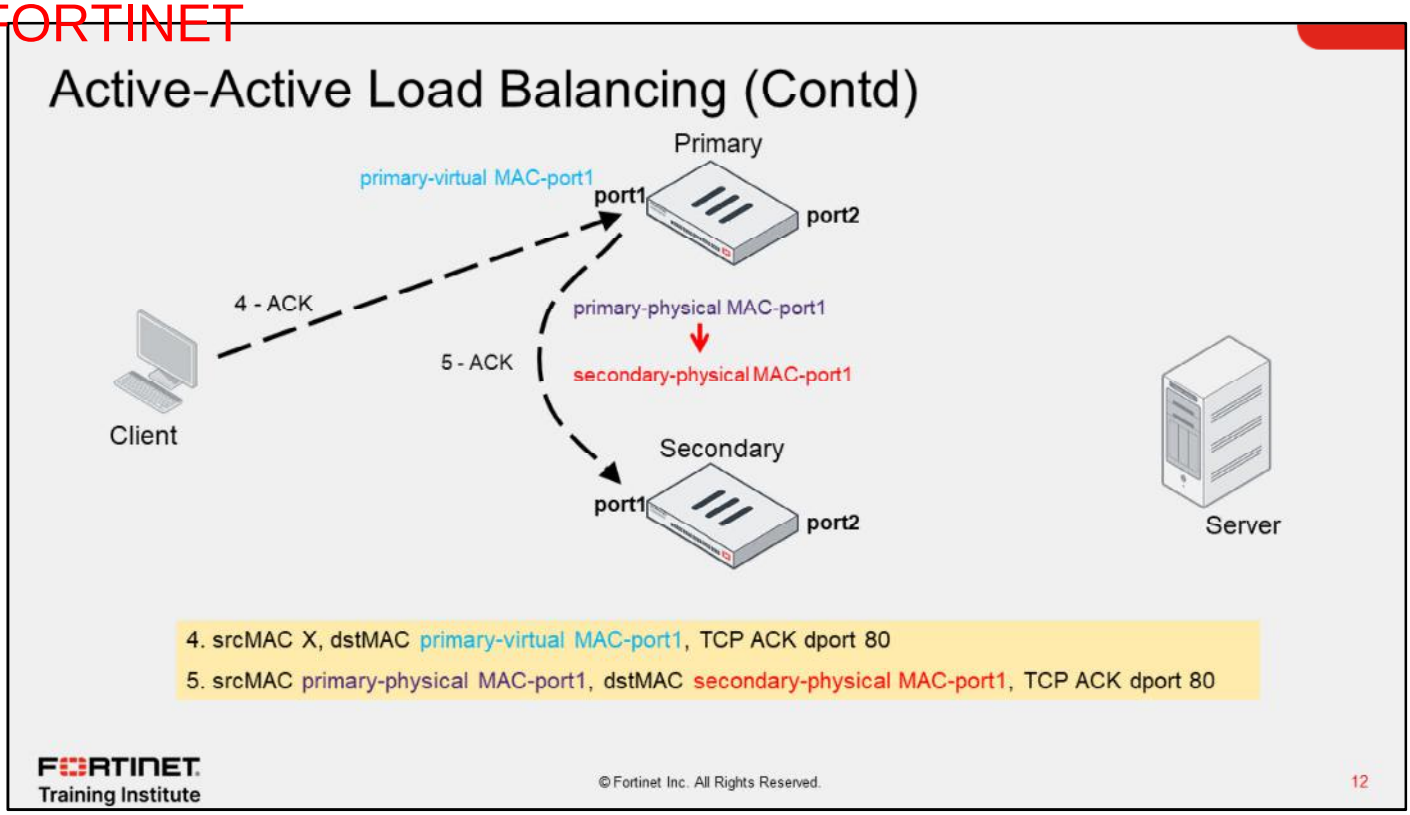
Take a look at how an HA cluster in active-active mode handles traffic.

First, the client sends a SYN packet, which is always forwarded to the primary FortiGate using the internal interface virtual MAC address as the destination. If the primary decides that the session is going to be inspected by a secondary, the primary forwards the SYN packet to the respective secondary.

In the example shown on this slide, the destination MAC address is the physical MAC address of the secondary FortiGate. The secondary responds with a SYN/ACK to the client and starts the connection with the server by directly sending a SYN packet.

Vouchers & Dumps are Available | WhatsApp +201224560923

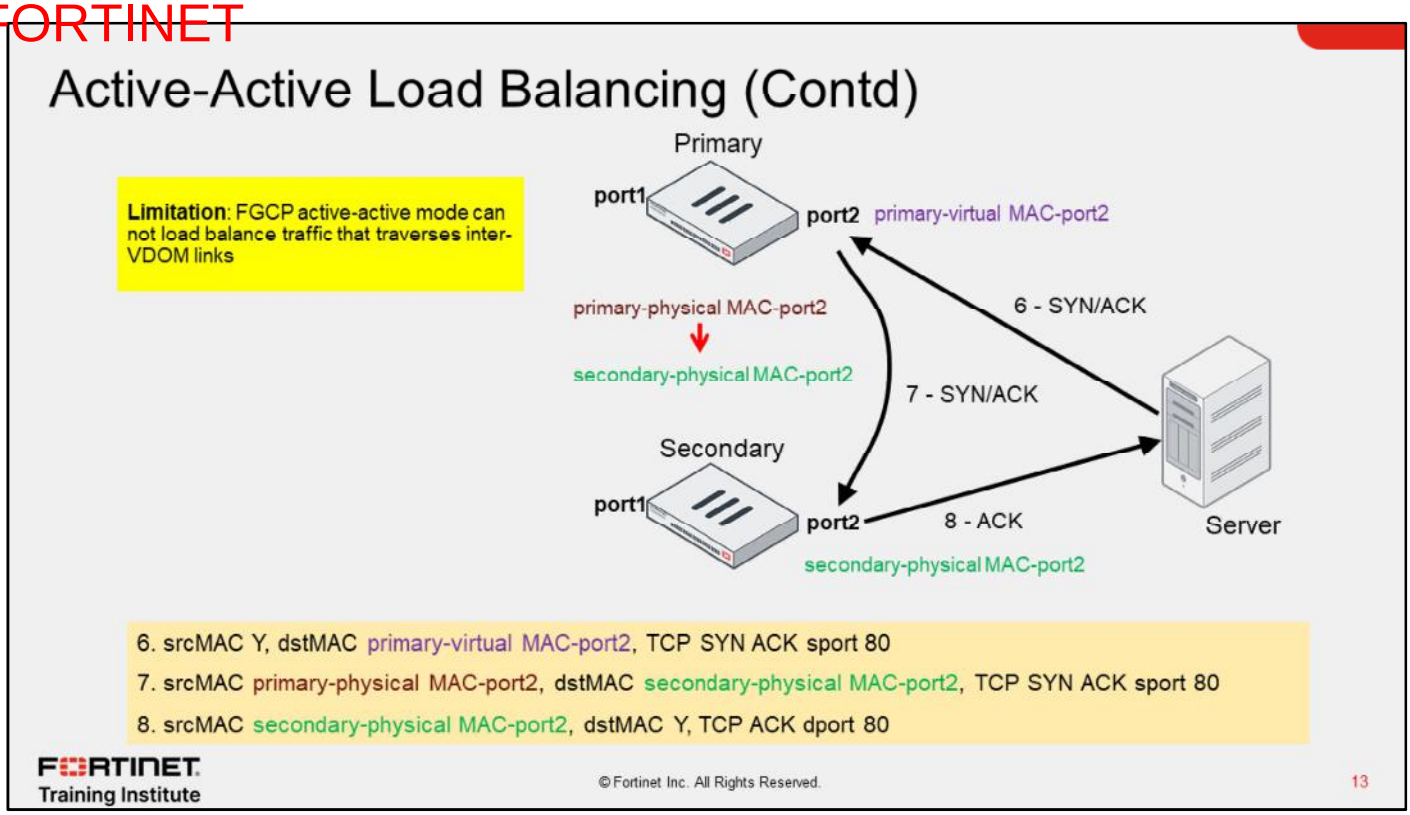
DO NOT REPRINT Brave-dumps.com
© FORTINET



Next, the client acknowledges the SYN/ACK. The client forwards to the primary using the virtual MAC address as the destination. The primary device forwards the packet to the secondary inspecting that session, using the secondary physical MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When the server responds to the TCP SYN, the packet is sent to the primary using the external interface virtual MAC. The primary signals the secondary, and it is the secondary that replies to the server.

As you can see in the example, the objective of active-active mode is not to load balance bandwidth. The traffic is always sent to the primary first. The main objective is to share CPU and memory among multiple FortiGate devices for traffic inspection.

Note that an FGCP in active-active mode cannot load balance any sessions that traverse inter-VDOM links. If you need an active-active load balancing of sessions between VDOMs, you must use an external router to handle the inter-VDOM routing

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Secondary Console Messages

- The console of a secondary device shows these messages when joining the cluster

```
secondary's external files are not in sync with primary, sequence:0. (type IDS)
secondary's external files are not in sync with primary, sequence:1. (type IDS)
secondary's external files are not in sync with primary, sequence:0. (type CERT_LOCAL)
secondary's external files are not in sync with primary, sequence:1. (type CERT_LOCAL)
secondary's external files are not in sync with primary, sequence:2. (type CERT_LOCAL)
secondary's external files are not in sync with primary, sequence:3. (type CERT_LOCAL)
secondary's external files are not in sync with primary, sequence:4. (type CERT_LOCAL)
secondary succeeded to sync external files with primary
secondary's configuration is not in sync with primary's, sequence:0
secondary's configuration is not in sync with primary's, sequence:1
secondary's configuration is not in sync with primary's, sequence:2
secondary's configuration is not in sync with primary's, sequence:3
secondary's configuration is not in sync with primary's, sequence:4
secondary starts to sync with primary
logout all admin users
secondary succeeded to sync with primary
```

FORTINET Training Institute

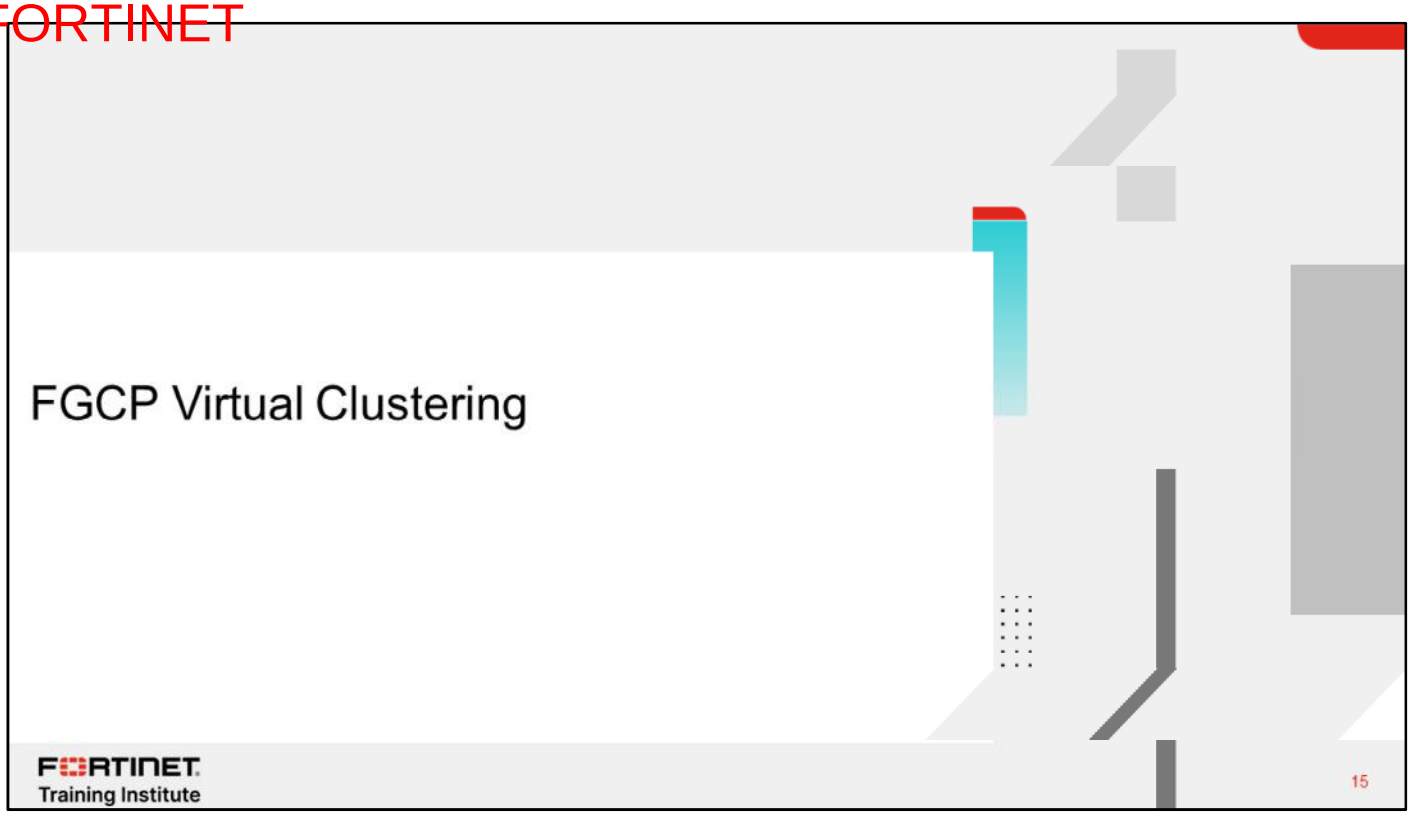
© Fortinet Inc. All Rights Reserved.

14

If you connect to the console port of a secondary device while it's joining an HA cluster, you should see the messages shown on this slide. First, the secondary tries to synchronize the *external files*. The external files include the FortiGuard databases and digital certificates. After that, the secondary synchronizes the configuration. The last message indicates that the secondary has successfully joined the cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



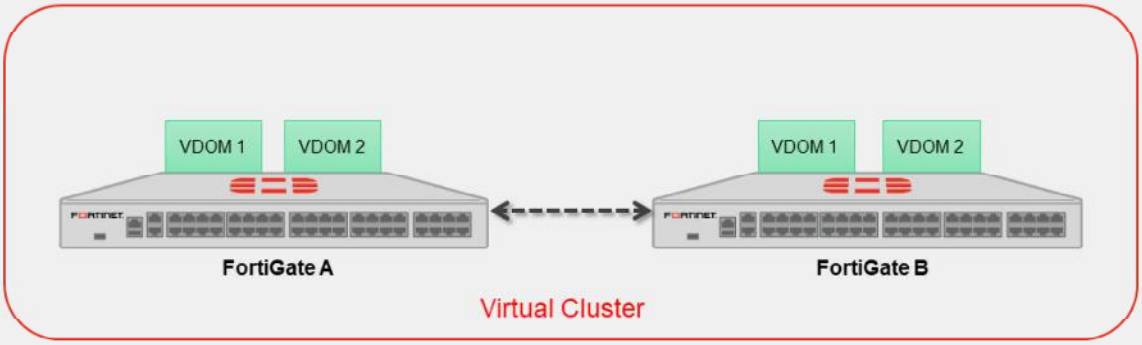
In this section, you will learn about FGCP virtual clustering.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

What Is Virtual Clustering?

- Extension of FGCP for a cluster of FortiGate devices with multiple VDOMs enabled
- Virtual clustering operates in active-passive mode
- FortiGate virtual clustering is limited to thirty virtual clusters



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

Virtual clustering is essentially a cluster of FortiGate devices operating with multiple VDOMs enabled.

In active-active mode, you can load balance sessions between two cluster devices. In active-passive mode, you can configure a virtual cluster to provide standard failover protection between two instances of a VDOM operating on two different devices. There is another way you can load balance sessions in a virtual cluster, which is VDOM partitioning.

Virtual clustering operates on a cluster of FortiGate devices. You can create up to thirty virtual clusters. If you want to create a cluster of more than two FortiGate devices operating with multiple VDOMs, you could also consider other solutions that either do not include multiple VDOMs in one cluster, or employ a feature, such as standalone session synchronization with FGSP.

Other requirements to configure virtual clustering are the same as in a standard HA configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VDOM Partitioning

- You must set HA mode to active-passive
- Uses VDOM partitioning to distribute traffic between both cluster devices
- Control the distribution of traffic between the devices in the cluster by adjusting which cluster device is the primary device for each VDOM

```
NGFW-1 #
config system ha
    set group-name "fortinet"
    set mode a-p
    set password ENC qg3xGg+sHoFBdoNqUM4qncLHuMf7
    set hbdev "port7" 0
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 200
            set vdom "VDOM1" "root"
        next
        edit 2
            set override disable
            set priority 50
            set vdom "VDOM2"
        next
    end
end
```

NGFW-1 firewall is primary device for 'VDOM1' and 'root' VDOMs

NGFW-1 firewall is secondary device for 'VDOM2'

```
NGFW-2 #
    config system ha
     set group-name "fortinet"
     set mode a-p
     set password ENC y22eaU3YlWXy3dO0wnw6QgLPqM9VS9TiPGCjWP
     set hbdev "port7" 0
     set session-pickup enable
     set vcluster-status enable
     config vcluster
         edit 1
             set override disable
             set priority 100
             set vdom "VDOM1" "root"
         next
         edit 2
             set override disable
             set priority 200
             set vdom "VDOM2"
         next
     end
end
```

NGFW-2 firewall is secondary device for 'VDOM1' and 'root' VDOMs

NGFW-2 firewall is primary device for 'VDOM2'

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

In VDOM partitioning, the HA mode is set to active-passive. To configure VDOM partitioning, you configure one cluster device as the primary for some VDOMs, and you set the other cluster device as the primary for other VDOMs. All traffic for a VDOM is processed by the primary device for that VDOM. You can control the distribution of traffic between cluster devices by adjusting which cluster device is the primary device for each VDOM.

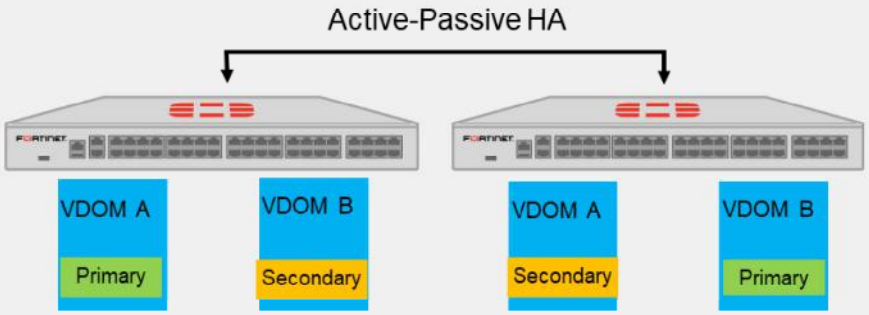
In this example, NGFW-1 is configured as primary cluster device for VDOM1 and root VDOMs, and NGFW-2 is primary cluster device for 'VDOM2'. The `set priority` command determines the role of the cluster device for each VDOM. The cluster device with the highest priority becomes the primary device for individual VDOMs in a VDOM partitioning setup.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VDOM Partitioning (Contd)

- If you have two VDOMs with high traffic volume then you can configure each cluster device to be the primary device for each VDOM
  - VDOM A and B with high traffic volume
  - Two FortiGate devices in a cluster, FortiGate1 and FortiGate2
  - For VDOM A, FortiGate1 is the primary device
  - For VDOM B, FortiGate2 is the primary device



FORTINET Training Institute

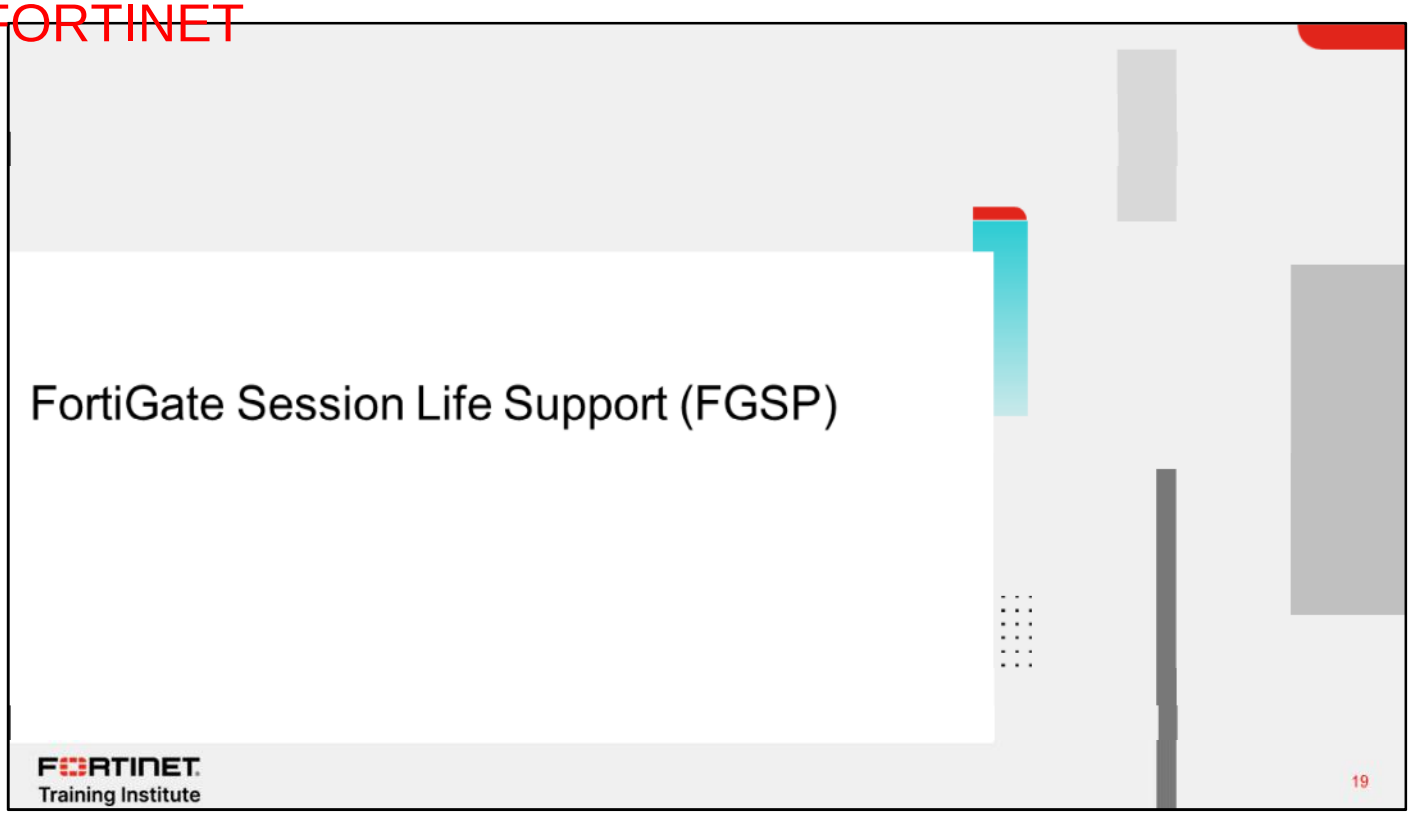
© Fortinet Inc. All Rights Reserved.

18

In the example shown on this slide, HA is configured in active-passive mode. FortiGate 1 processes all traffic for VDOM A, and FortiGate 2 processes all traffic for VDOM B. In case of a failover, one device in the cluster processes all traffic for all VDOMs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn about FortiGate Session Life Support (FGSP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate Session Life Support Protocol

- HA solution only for sharing sessions
- Peer-to-peer communication between:
  - Standalone FortiGate
  - FGCP cluster
- Load balancing and failover is performed by external network devices
  - VRRP can be used to support failover
- The following sessions can be synchronized:
  - IPv4 and IPv6 TCP
  - SCTP
  - UDP
  - ICMP
  - Expectation (EXP)
  - NAT
- By default, FGSP synchronizes all IPv4 and IPv6 TCP sessions, and IPsec tunnels

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

The FortiGate Session Life Support Protocol (FGSP) is another proprietary HA solution only for sharing sessions between standalone FortiGate devices or an FGCP cluster. Session sharing is based on peer-to-peer communications between FortiGate devices where traffic is load balanced by an upstream load balancer and scanned by downstream FortiGate devices. FGSP is also compatible with FortiGate VRRP.

FortiGate devices in FGSP operate as peers that process traffic and synchronize sessions. An FGSP deployment can include two to 16 standalone FortiGate devices, or two to 16 FortiGate FGCP clusters of two members each. Adding more FortiGate devices increases the CPU and memory required to keep all of the FortiGate devices synchronized, and it increases network synchronization traffic.

FGSP can perform session synchronization of IPv4 and IPv6 TCP, SCTP, UDP, ICMP, expectation, and NAT sessions, to keep the session tables synchronized on all FortiGate devices. If one of the FortiGate devices fails, the upstream load balancer should detect the failed member and stop distributing sessions to it. Session failover occurs and active sessions fail over to the peers that are still operating. Traffic continues to flow on the new peer without data loss, because the sessions are synchronized.

By default, FGSP synchronizes all IPv4 and IPv6 TCP sessions, and IPsec tunnels.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Requirements

- FGSP requires the same device model, firmware version, and licensing
- Each device should have a unique IP addresses
- Configuration:
  - Session synchronization and configuration synchronization must be configured separately
- A single device should receive both directions of traffic for UTM inspection (symmetric routing)
  - If inspected traffic experiences asymmetric routing, all packets for that session will be forwarded to the session owner (device that received the first packet)
- Standalone configuration synchronization is based on FGCP config sync
  - It requires layer 2 adjacency to form a cluster
  - Follow the same layer 2 segmentation requirements for active-passive mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

To form an FGSP cluster, the two devices must be of the same model, run the same firmware version, and have the same licensing. In addition, each device should have a unique IP address.

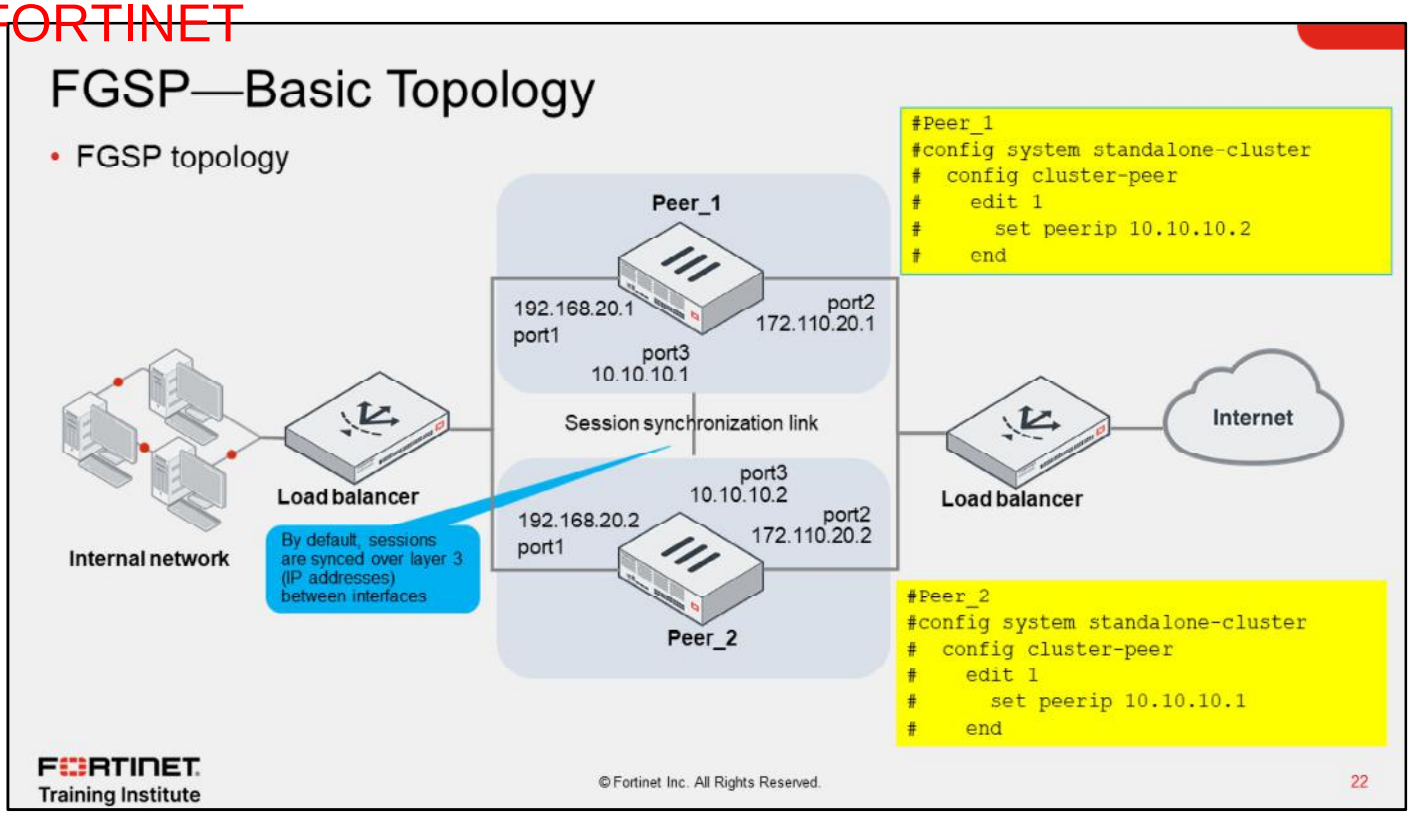
When configuring FGSP, you configure session synchronization and configuration synchronization separately.

For the best performance, it is recommended that you should enable UTM inspection only if the traffic is symmetric. However, if asymmetric routing occurs for UTM sessions, all packets for that session will be forwarded to the FortiGate device that owns the session.

In addition, standalone config sync is based on the config sync feature of FGCP, which requires layer 2 adjacency to work. This means that you need to follow the same layer 2 segmentation requirements needed for active-passive mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FGSP is primarily used instead of FGCP, when external load balancers are part of the topology and are responsible for distributing traffic amongst the downstream FortiGate devices. FGSP provides the means to synchronize sessions between the FortiGate peers, without needing a primary member to distribute the sessions, like you do in FGCP active-active mode. If the external load balancers direct all sessions to one peer, the effect is similar to active-passive FGCP HA. If external load balancers balance traffic to both peers, the effect is similar to active-active FGCP HA. The load balancers should be configured so that all packets for any given session are processed by the same peer, including return packets, whenever possible.

This slide shows a basic FGSP setup. This example uses two peer FortiGate devices. The load balancer is configured to send all sessions to Peer_1, and if Peer_1 fails, all traffic is sent to Peer_2. By default, FGSP peers use layer 3 connectivity to synchronize their sessions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Session Synchronization

Session Types	Syntax

To sync sessions with a particular source, destination, or source addresses/subnets, or a destination interface	`config session-syn-filter`
	`set srcintf <interface`
	`set dstintf <interface>`
	`set srcaddr <IPv4_address/subnet>`
	`set dstaddr <IPv4_address/subnet>`
	`set srcaddr6 <IPv6_address/subnet>`
	`set srcaddr6 <IPv6_address/subnet>`

To sync connectionless sessions (UDP & ICMP)	`config system ha`
	`set session-pickup enable`
	`set session-pickup-connectionless enable`

To sync expectation (EXT) sessions (pinholes open by firewall (SIP or FTP traffic)	`set session-pickup-expectation enable`
To sync NAT sessions	`set session-pickup-nat enable`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

By default, FGSP synchronizes all IPv4 and IPv6 TCP sessions, and IPsec tunnels. However, you can add other sessions to synchronize between peer FortiGate devices.

The table on this slide shows the CLI commands that you can use to enable and filter an additional sessions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

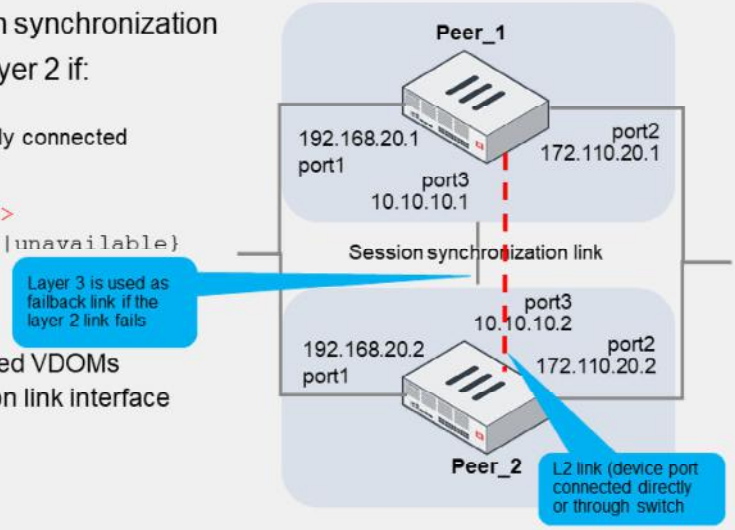
FGSP—Session Synchronization (Contd)

- Layer 2 connectivity can be used for session synchronization
- Session synchronization will happen over layer 2 if:
  - Session synchronization interface is configured
  - Peer session synchronization interfaces are directly connected

```
config system standalone-cluster
    set session-syn-dev <interface 1>
    set layer2-connection {available|unavailable}
end
```

- VDOM synchronization:
  - Can specify peer VDOM and the synchronized VDOMs
  - Peer VDOM contains session synchronization link interface

```
config system standalone-cluster
    config cluster-peer
        edit 1
            set peerip <IP address>
            set peervd <vdom>
            set synced <vdom1> [<vdom 2>] …[<vdom n>]
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

When peering over FGSP, by default, the FortiGate devices or FGCP clusters, share information over layer 3 between the interfaces that are configured with peer IP addresses. You can also specify the interfaces used to synchronize sessions in layer 2 instead of layer 3 using the `session-sync-dev` setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes unavailable.

If you are doing only session synchronization, and not configuration synchronization, no layer 2 connectivity is required.

When multi-VDOM mode is enabled on the FortiGate devices, you can specify the peer VDOM and the synchronized VDOMs. The peer VDOM contains the session synchronization link interface on the peer device. The synchronized VDOMs' sessions are synchronized using the session synchronization configuration shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Session Synchronization (Contd)

- Between different FortiGate models or firmware version
- Different FortiGate models:
  - FortiGate devices use the same 32-bit kernel or 64-bit kernel
  - FortiGate devices use the same type of CPU (such as ARM or x86)
  - For network interfaces:
    - The same type of physical interface should be used on each member
    - The physical interfaces should be capable of the same speed
  - The device memory should be similar in size
  - The configurations related to session tables should match
- Different firmware versions:
  - Firmware needs to have compatible data structures and session synchronization packet headers
  - Exceptions:
    - FortiGate devices running 7.0.2 or later, and FortiGate devices running 7.0.1 or earlier will not accept session synchronization
    - If the traffic uses a new feature only available in a newer FortiOS version
    - ForiOS 7.2.1 or later added `group-id` in to protocol header, which means that FortiGate cannot perform session synchronization with FortiGate devices running earlier versions.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

FGSP HA deployments are generally meant for interoperating between FortiGate devices with the same model and firmware version. However, situations may arise where individual members or FGCP clusters running over FGSP use different models or firmware versions. For example, to avoid downtime while upgrading the members, some FGSP members or clusters may be upgraded first, and then rejoin the FGSP peers after a successful upgrade. Or while performing maintenance, sessions may need to be offloaded to a temporary member or FGCP cluster of a different model.

When considering FGSP session synchronization between two FortiGate devices, ensure that:

- The FortiGate devices use the same 32-bit kernel or 64-bit kernel.
- The FortiGate devices use the same type of CPU (such as ARM or x86).
- For network interfaces:
  - The same type of physical interface should be used on each member.
  - The physical interfaces should be capable of the same speeds.
- If the FortiGate devices have vastly different memory sizes, their performance may be different if one device supports more sessions than the other.
- The configurations related to session tables should match. For example, the logical names used in firewall policies, IPsec interface names, VDOM names, firewall policy tables, and so on, should match. Note that virtual clusters and asymmetric routing are not supported.

When operating in FGSP, the firmware needs to have compatible data structures and session synchronization packet headers. The firmware is generally able to handle different data structures between old and new FortiOS sessions, but there are some exceptions:

- FortiOS 7.0.2 added support for widening the HA virtual MAC address range. This change updated the session synchronization packet header structure and hence doesn't support session synchronization with older firmware versions.
- A new feature in a newer FortiOS version, may not work when synchronized to an older FortiOS version.
- FortiOS 7.2.1 or later added `group-id` in to protocol header. This means FortiGate cannot perform session synchronization with earlier firmware versions

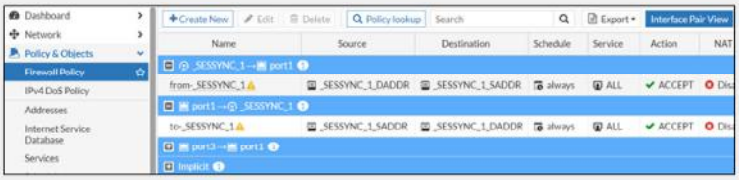
Vouchers & Dumps are Available | WhatsApp +201224560923

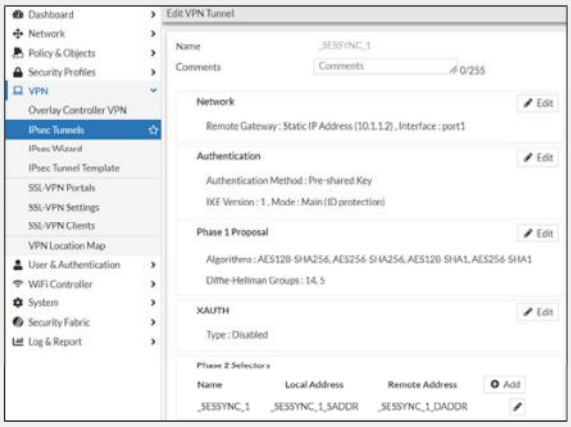
DO NOT REPRINT Brave-dumps.com
© FORTINET

Session Synchronization Encryption

- Session synchronization can be encrypted using an IPsec tunnel
  - Layer 3 connections
- Enable `encryption` and set the `psksecret`

```
config system standalone-cluster
    set encryption enable
    set psksecret fortinet
end
```





- Useful for securing session sync data when sent between data centers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

Encryption in the form of an IPsec tunnel can be enabled for session synchronization. This is achieved by enabling `encryption` and setting the `psksecret` under `config system standalone-cluster`.

When enabled, the IPsec VPN and policies are automatically created. This is useful for securing the session synchronization data, especially if it is travelling between data centers. Note that, encryption is supported for layer 3 connections only.

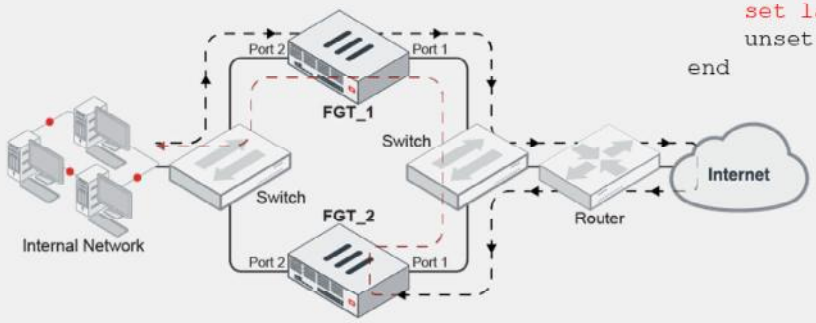
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Inspection with Asymmetric Traffic—Layer 2

- Security inspection is supported with asymmetric traffic by passing all packets for a session back to the device that processed the first packet
- This requires that both FortiGate devices in the FGSP pair have:
  - Internal and outgoing interfaces in the same subnet
  - Layer 2 access with each other

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 0
    set layer2-connection available
    unset session-sync-dev
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

When traffic passes asymmetrically through FGSP peers, UTM inspection can be supported by always forwarding traffic back to the session owner for processing. The session owner is the FortiGate that receives the first packet of the session.

The layer 2 connection setting is for forwarded traffic between FGSP peers. Set it to `available` if the peer interface user for traffic forwarding is directly connected and supports layer 2 forwarding.

In this example, traffic from the internal network first hits FGT_1, but the return traffic is routed to FGT_2. Consequently, traffic bounces from FGT_2 port1 to FGT_1 port1 using the FGT_1's MAC address. Traffic is then inspected by FGT_1.

This example requires that the internal and outgoing interfaces of both FortiGate devices in the FGSP pair are in the same subnet, and that both peers have layer 2 access with each other.

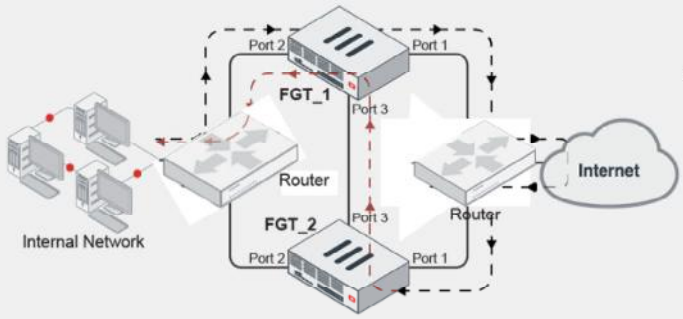
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Inspection with Asymmetric Traffic—Layer 3

- Some environments do not have layer 2 connectivity
  - Cloud environments
- Traffic is forwarded through the peer interface
- Traffic is forwarded using a UDP connection

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 0
    set layer2-connection unavailable
    unset session-sync-dev
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

For networks where layer 2 connectivity is not available, such as cloud environments, traffic bound for the session owner is forwarded through the peer interface using a UDP connection.

In this example, traffic from the internal network first hits FGT_1, but the return traffic is routed to FGT_2. Consequently, return traffic is packed and sent from FGT_2 to FGT_1 using UDP encapsulation between two peer interfaces (port 3). Traffic is then inspected by FGT_1.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Configuration Synchronization

- FGSP configuration synchronization is also known as standalone config sync
- Configuration and external files are synced over heartbeat connections from one device to another in the same way as in FGCP
  - Layer 2 connectivity required
  - Configure multiple heartbeat ports for redundancy
- Standalone configuration synchronization is basically the same configuration synchronization feature that is available in FGCP
  - A primary device is elected by following the same election process
  - The primary and secondary device roles are only for config sync purposes and *not* for traffic
  - The same two-layer approach that is used for config sync in FGSP, is used in FGCP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

In addition to enabling session synchronization for FGSP deployments, you may want to enable configuration synchronization as well. Configuration synchronization, also known as standalone configuration synchronization, is basically the same configuration synchronization feature that is available in FGCP deployments, but it can be enabled separately, in case you want to synchronize the configuration between two devices operating in standalone mode. Remember, FGSP is just a cluster formed by two devices or FGCP clusters operating in standalone mode, but they can synchronize sessions and configuration between them.

Standalone configuration synchronization allows for configuration and external files to synchronize from one device to another, in the same way it happens for FGCP. A primary device is elected by the same election process that is used in FGCP. Just keep in mind that in standalone configuration synchronization, the primary and secondary device roles are useful only for configuration synchronization purposes and *not* for traffic processing purposes.

Finally, the approach used by standalone configuration synchronization is the same two-layer approach that is in FGCP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Config Sync

- The following are not synchronized when standalone configuration synchronization is used:
  - Interface settings—`config system interface`
  - Cluster-sync settings—`config system cluster-sync`
  - Sniffer settings—`config firewall sniffer`
  - Static route settings—`config router static`
  - Policy route settings—`config router policy`
  - BFD router settings—`config router bfd`
  - RIP router settings—`config router rip`
  - Partial BGP settings—`config router bgp`
  - Partial OSPF settings—`config router ospf`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

When standalone configuration synchronization is used, most of the configuration, including policies, objects, users, and security profiles, are synchronized between the peers. In addition to the settings that are not synchronized with FGCP configuration synchronization, such as hostname and select HA settings, settings relating to networking are also not synchronized. These include interface settings, cluster synchronization settings, sniffer settings, static route settings, policy route settings, BFD router settings, RIP router settings, and partial BGP and OSPF settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGSP—Sample Config—Config Sync—HA Settings

- Device 1

```
config global
config system ha
    set group-id 1
    set group-name "Cluster1"
    set mode standalone
    set password fortinet1
    set hbdev "port2" 50 "port3" 50
    set standalone-config-sync enable
    set override disable
    set priority 200
end
```

- Device 2

```
config global
config system ha
    set group-id 1
    set group-name "Cluster1"
    set mode standalone
    set password fortinet1
    set hbdev "port2" 50 "port3" 50
    set standalone-config-sync enable
    set override disable
    set priority 100
end
```

The settings enable (standalone) config sync

FORTINET Training Institute

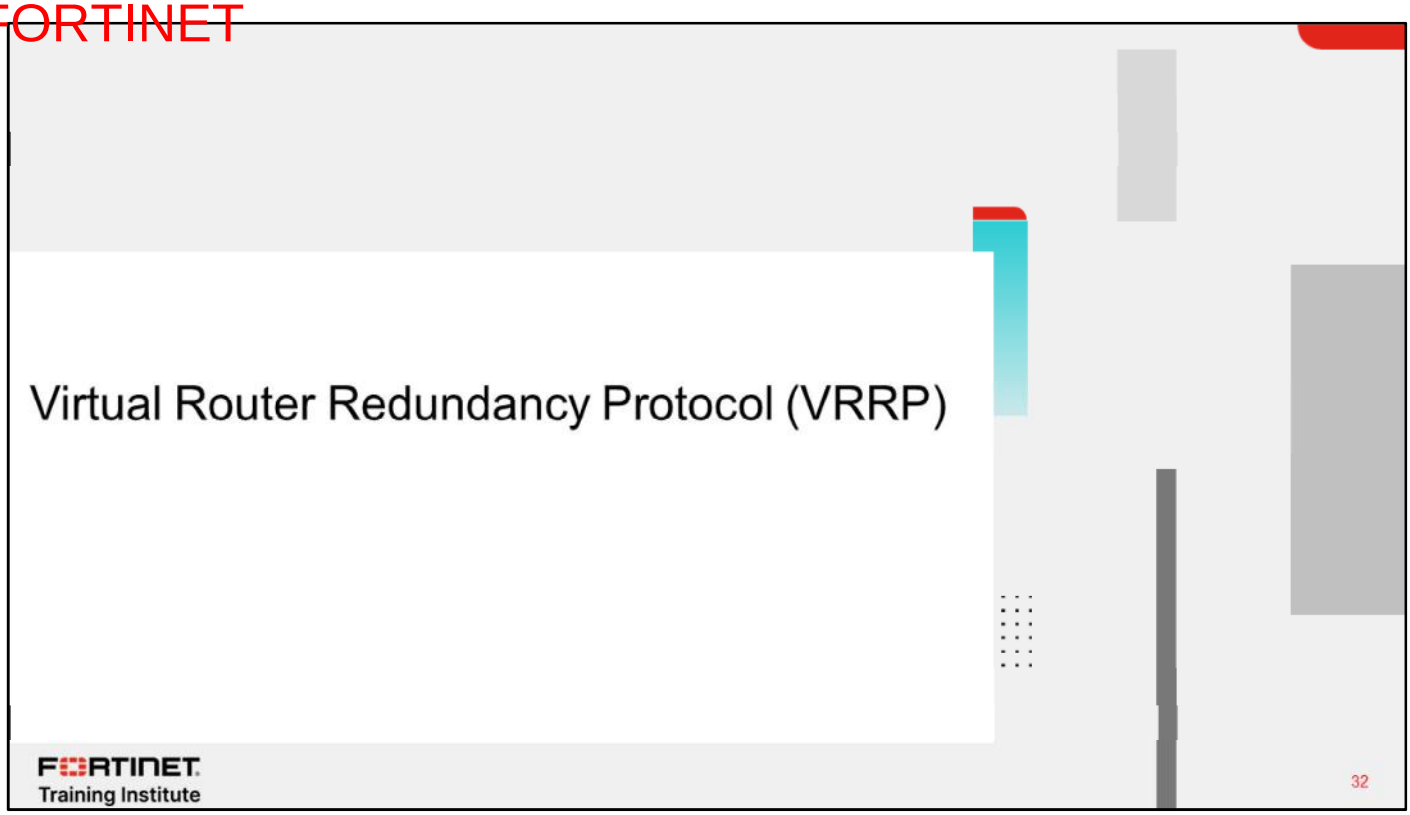
© Fortinet Inc. All Rights Reserved.

31

If you want to enable standalone configuration synchronization, you can apply a configuration like the one shown on this slide. The key is to set `mode` to `standalone` and after that, enable the `standalone-config-sync` option. The rest of the settings have the same purpose as they do in active-passive mode; therefore, they are used for primary device election, heartbeat communication, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

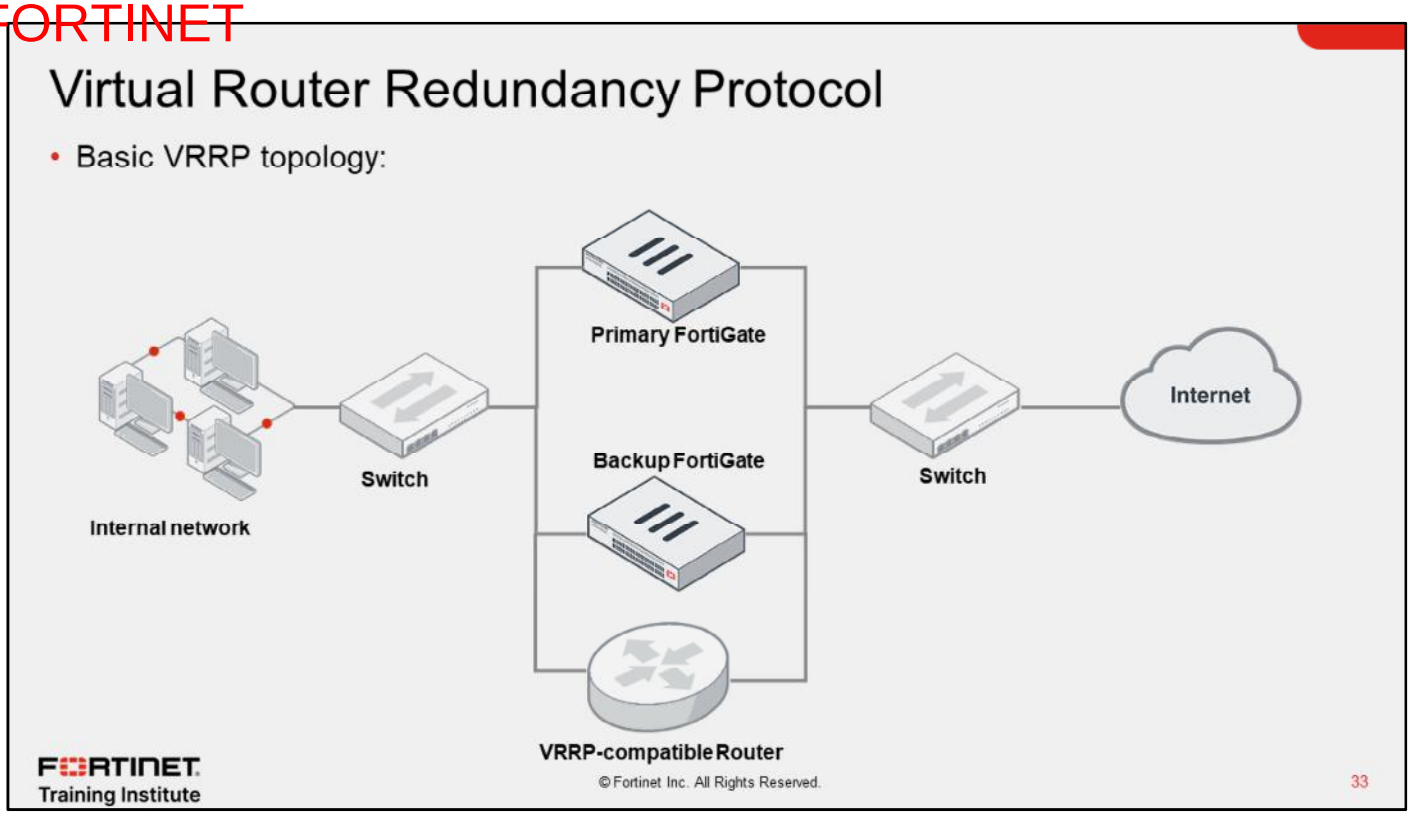
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about Virtual Router Redundancy Protocol (VRRP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows the basic single domain Virtual Router Redundancy Protocol (VRRP) topology. A VRRP configuration can be used as a high availability solution to ensure that a network maintains connectivity with the internet (or with other networks), even if the default router for the network fails. If a router or a FortiGate device fails, all traffic to this device transparently fails over to another router or FortiGate that takes over the role of the failed device. If the failed device is restored, it will take over processing the network traffic.

FortiOS supports VRRP versions 2 and 3. VRRP domains can be created, which can include multiple FortiGate devices and other VRRP-compatible routers. Different FortiGate models can be added to the same VRRP domain. FortiOS supports IPv4 and IPv6 VRRP, so IPv4 and IPv6 VRRP virtual routers can be added to the same interface. FortiGate devices can quickly and easily integrate into a network that has already deployed VRRP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VRRP—Virtual Router

- You add the virtual router to an interface
- Only physical and VLAN interface support virtual router
- Support both IPv4 and IPv6 virtual router using `config vrrp` and `config vrrp6` CLI command

```
config system interface
  edit port<number>
       config vrrp
         edit <virtual router ID>
         set vrip <IP address>
         set priority <1-255>
       next
     end
   next
  end
```

```
config system interface
  edit port<number>
       config ipv6
           set vrip6_link_local <IPv6_address>
           config vrrp6
             edit <virtual router ID>
             set vrip <IP address>
             set priority <1-255>
         next
       end
     next
  end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

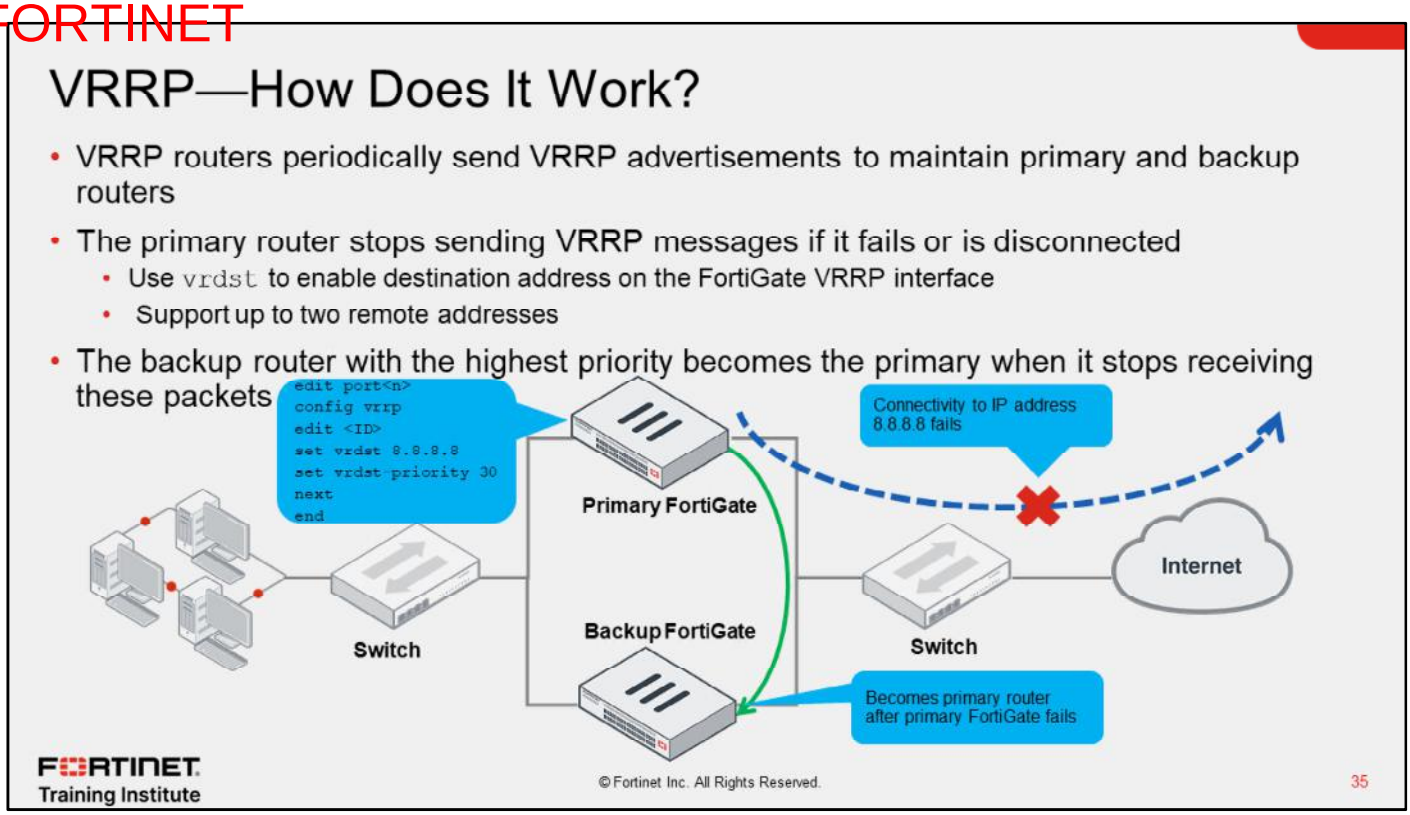
34

You can configure the VRRP virtual routers on an interface. VRRP can only be configured on physical or VLAN interfaces. VRRP cannot be configured on hardware switch interfaces where multiple physical interfaces are combined into a hardware switch interface.

The CLI commands on this slide add VRRP virtual router to the FortiGate device. The `vrip` setting determines the default gateway IP address of the internal network. The `priority` setting determines the primary FortiGate device in the VRRP domain. By default, it is set to `100`: `1` is the lowest and `255` is the highest value. The device with highest priority becomes the primary virtual router.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



VRRP FortiGate devices in a VRRP domain periodically send VRRP advertisement messages to all FortiGate devices in the domain to maintain one device as the primary router and the others as backup routers. The primary FortiGate device has the highest priority. If the backup FortiGate stops receiving these packets from the primary FortiGate device, the backup FortiGate device with the highest priority becomes the new primary.

The primary FortiGate device stops sending VRRP advertisement messages if it fails or becomes disconnected. Up to two VRRP destination addresses can be configured to be monitored by the primary device. As a best practice, the destination addresses should be remote addresses, as shown on this slide. If the primary router is unable to connect to the IP address `8.8.8.8`, it stops sending VRRP advertisement messages and changes its priority to `50`, set by the `set vrdst-priority` setting . The backup FortiGate device with the priority `50` becomes the primary router.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VRRP—How Does It Work? (Contd)

- VRRP virtual MACs
  - The `set vrrp-vitual-mac` command determines which MAC address is used during failover
  - When disabled (default setting):
    - Uses the MAC address of primary FortiGate interface that the VRRP was added to
    - On failover, the new primary sends gratuitous ARPs with the MAC address of the new primary
  - When enabled:
    - Virtual MAC address is shared MAC address adopted by the primary FortiGate
    - Combination of VRRP router ID and VRRP router own virtual MAC address <00-00-5E-00-01-<VRID_hex> where last octet is based on the ID
    - For example, if the VRRP router ID is 10, then the virtual MAC is `00-00-5E-00-01-0a`
    - The new primary uses the same MAC address as the old primary
- Preempt mode
  - When enabled:
    - A higher priority backup FortiGate can preempt a lower priority primary FortiGate
    - Occurs when a backup FortiGate takes over the primary role and then the former primary FortiGate becomes available
  - When disabled:
    - A former primary FortiGate that has a higher priority would not take over as the primary FortiGate

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

The `set vrrp-vitual-mac` command enables or disables the virtual MAC address feature on the FortiGate. If the VRRP virtual MAC address feature is disabled (default setting), the VRRP domain uses the MAC address of the primary FortiGate. On a FortiGate VRRP virtual router, this is the MAC address of the FortiGate interface that the VRRP router is added to. If the primary fails, when the new primary takes over, it sends gratuitous ARPs to associate the VRRP router IP address with the MAC address of the new primary (or the FortiGate interface that became the new primary).

When a VRRP virtual MAC address is enabled, the new primary uses the same MAC address as the old primary. The VRRP virtual MAC address (or virtual router MAC address) is a shared MAC address adopted by the primary router. If the primary router fails, the same virtual MAC address is picked up by the new primary FortiGate, allowing all devices on the network to transparently connect to the default route using the same virtual MAC address. This feature must be enabled on all members in a VRRP domain.

Each VRRP router has its own virtual MAC address. The last part of the octet is based on the VRRP router ID using the following format: `00-00-5E-00-01-<VRID_hex>` where `<VRID_hex>` is the VRRP router ID in hexadecimal format in the internet standard bit order. For example, If the VRRP router ID is `10`, then the virtual MAC address is `00-00-5E-00-01-0a`.

When preempt mode is enabled (default setting), a higher-priority backup FortiGate can preempt a lower-priority primary FortiGate. This can happen if the primary FortiGate fails, the backup FortiGate becomes the primary, and the failed primary FortiGate becomes available. Since the FortiGate has a higher priority, if preempt mode is enabled, the available FortiGate replaces the current primary FortiGate, becoming the new primary.

If preempt mode is disabled, a former primary FortiGate that has a higher priority would not take over as the primary FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Understand HA virtual MAC addresses
- ✓ Understand traffic flow in HA active-active mode
- ✓ Monitor an HA cluster
- ✓ Check configuration and session synchronization
- ✓ Examine FGCP
- ✓ Understand FGSP and VRRP

FORTINET Training Institute

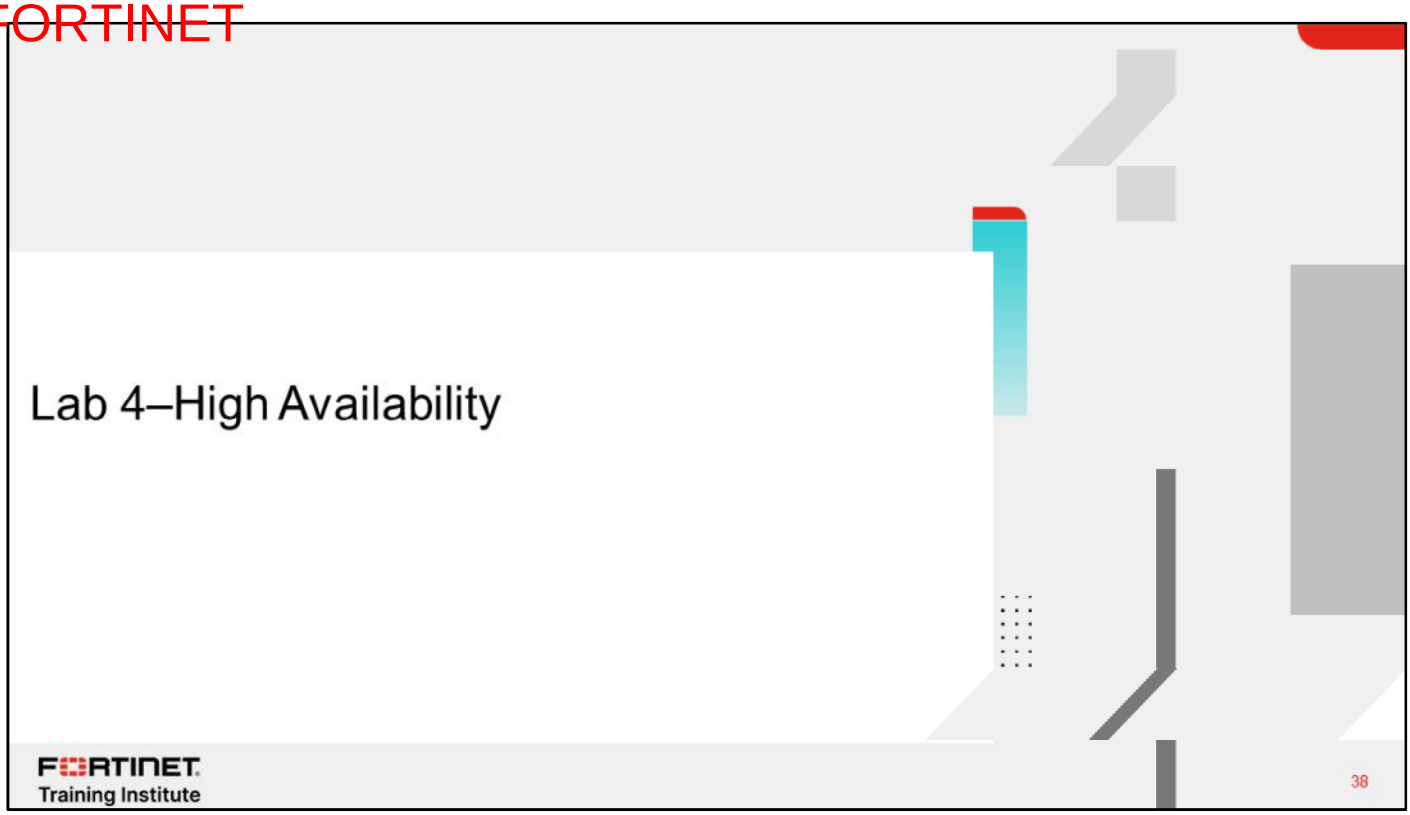
© Fortinet Inc. All Rights Reserved.

37

This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to troubleshoot HA issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

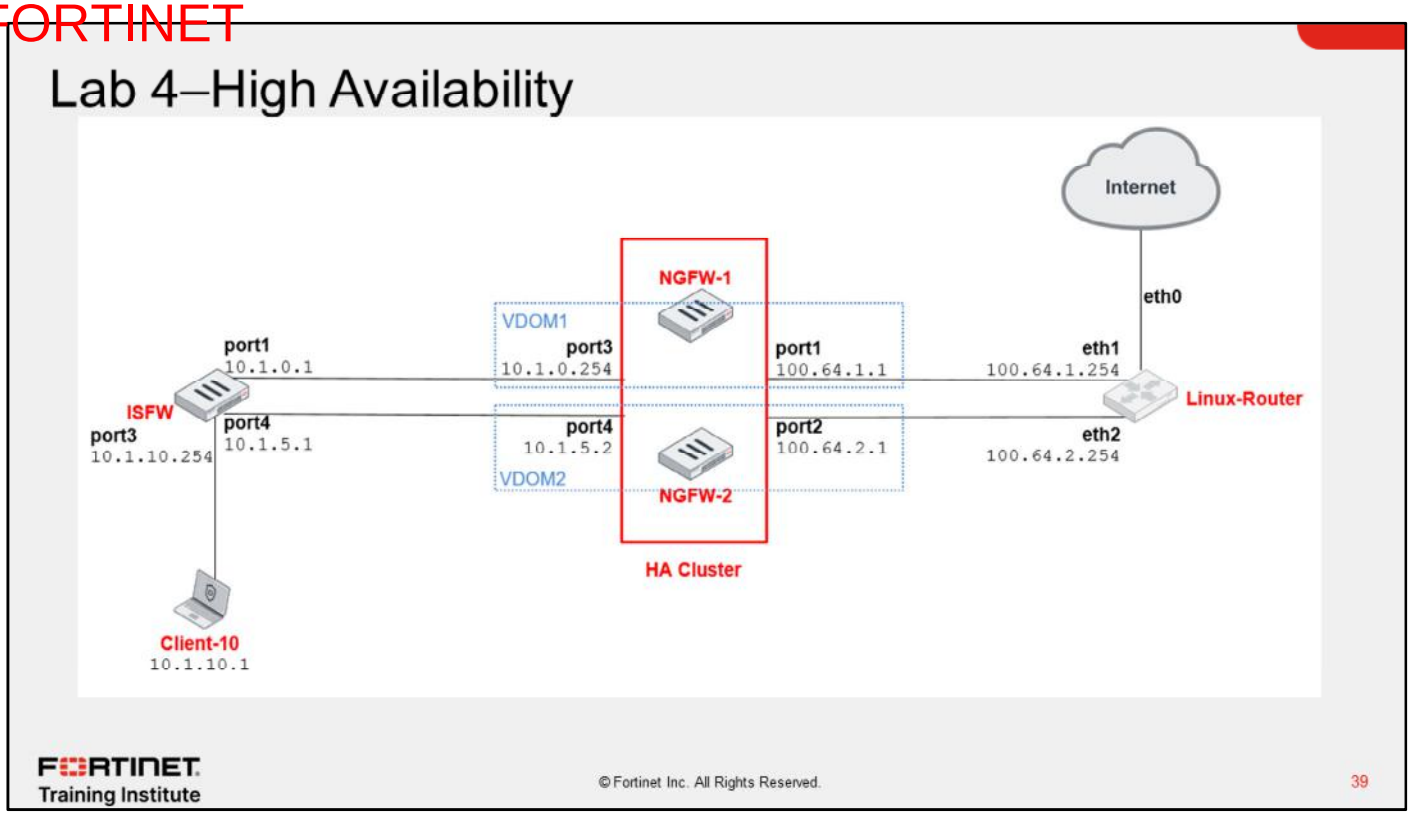
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will work on *Lab 4–High Availability*.

Vouchers & Dumps are Available | WhatsApp +201224560923

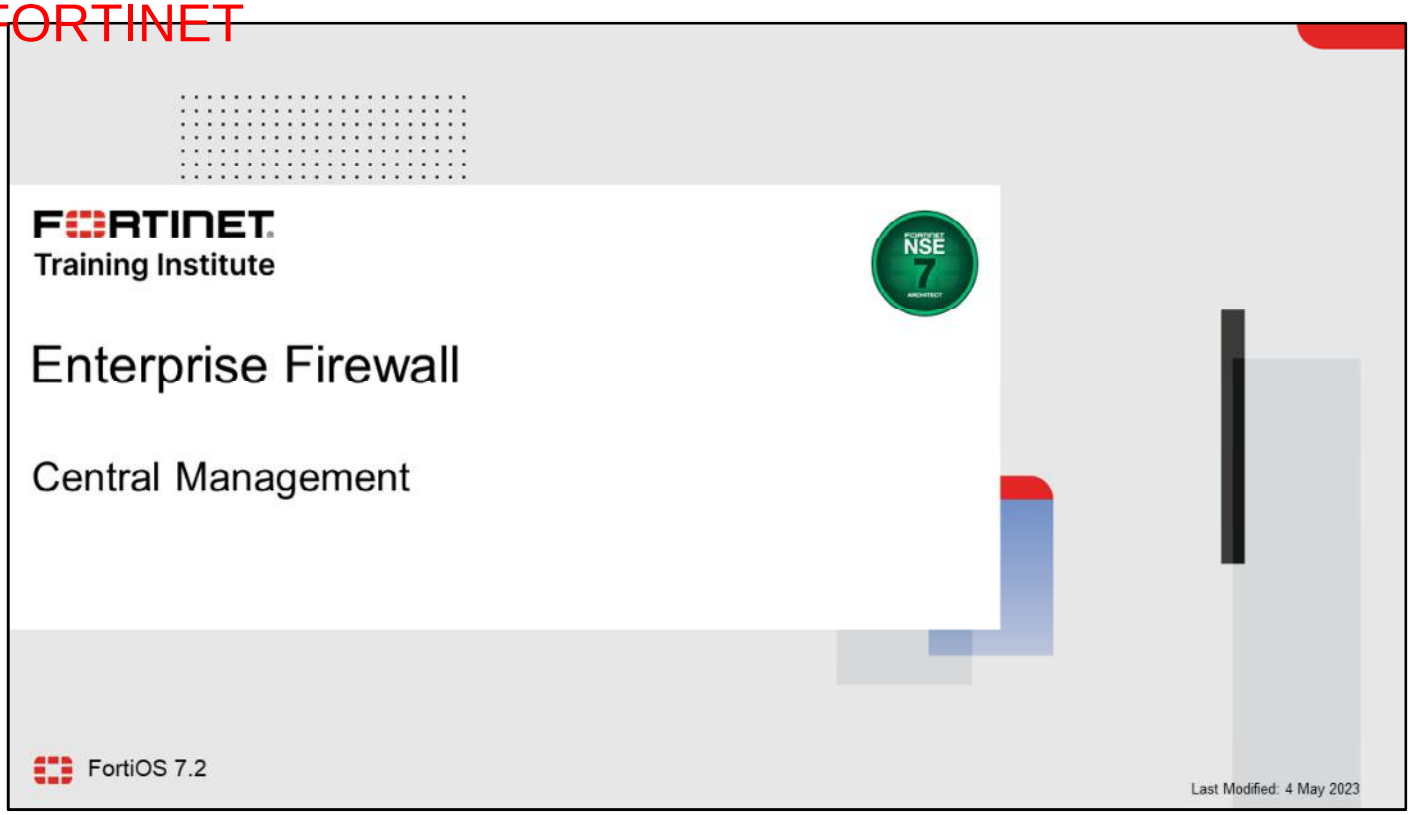
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lab, you will configure FGSP and VRRP between two FortiGate devices. You will also configure virtual clustering and distribute traffic between two FortiGate devices in the virtual cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn about using FortiManager for the central administration of all FortiGate devices in an enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Objectives

- Examine FortiManager key features
- Explore FortiManager architecture
- Explore Device Manager wizards
- Learn about scripts
- Identify the APIs supported by FortiManager
- Understand the meta fields available on FortiManager

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

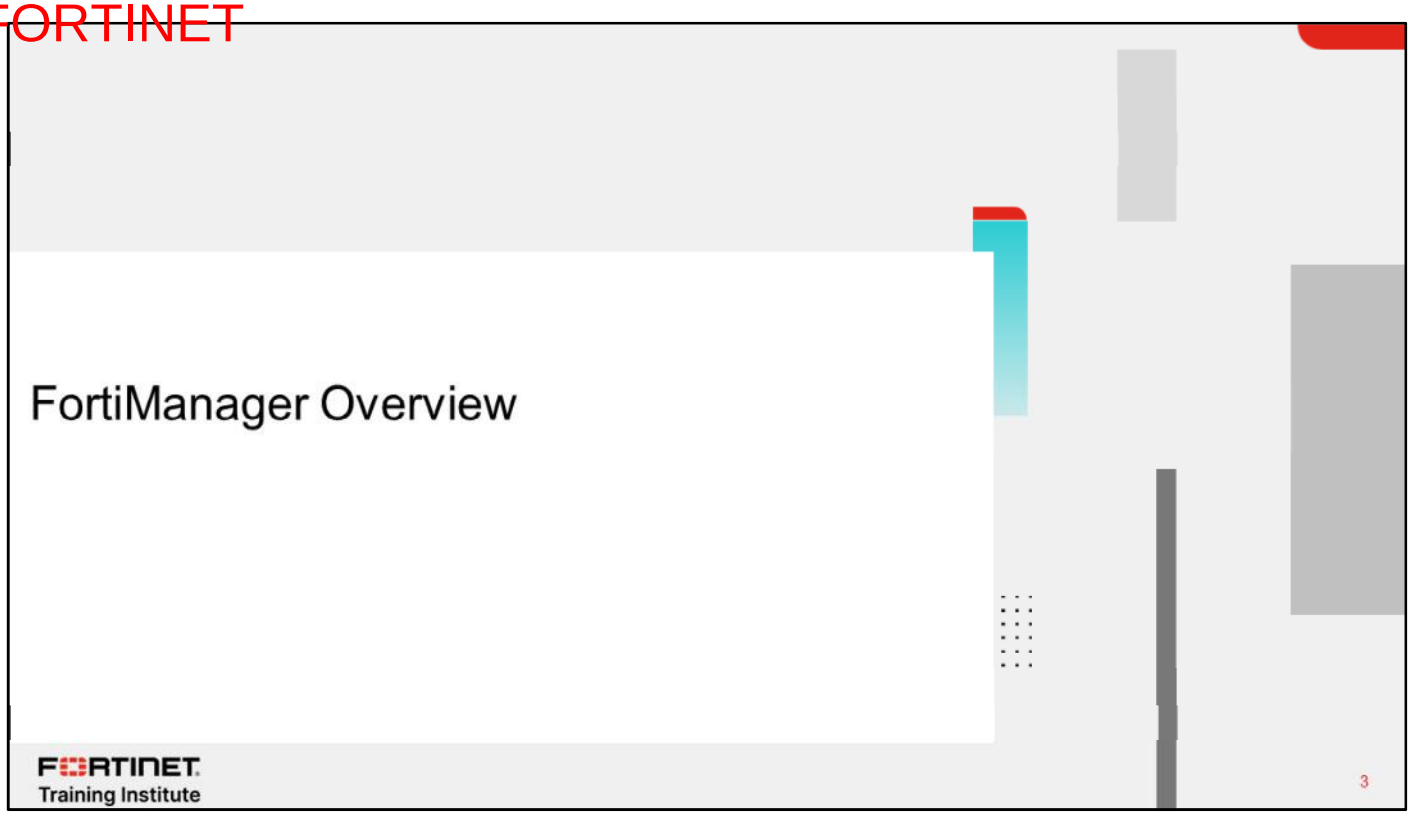
2

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

By demonstrating competence in using FortiManager, you will be able to centralize the administration of all FortiGate devices in an enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will review the key features of FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

What Is FortiManager?

- Single-pane-of-glass management
- Minimizes both initial costs and ongoing operating expenses for large deployments
- Helps maintain regulatory compliance
- Reduces WAN usage with local FortiGuard cache server
- Provides centralized device management for many Fortinet devices
- Automates mass device provisioning and maintains policies
  - Local distribution and control point for firmware and policy updates
  - Complex mesh and star IPsec VPN
- Provides logging and reporting

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

When should you use FortiManager in your network?

In large enterprises and managed security service providers (MSSPs), the size of the network introduces challenges that smaller networks don't have: mass provisioning; scheduling rollout of configuration changes; and maintaining, tracking, and auditing many changes.

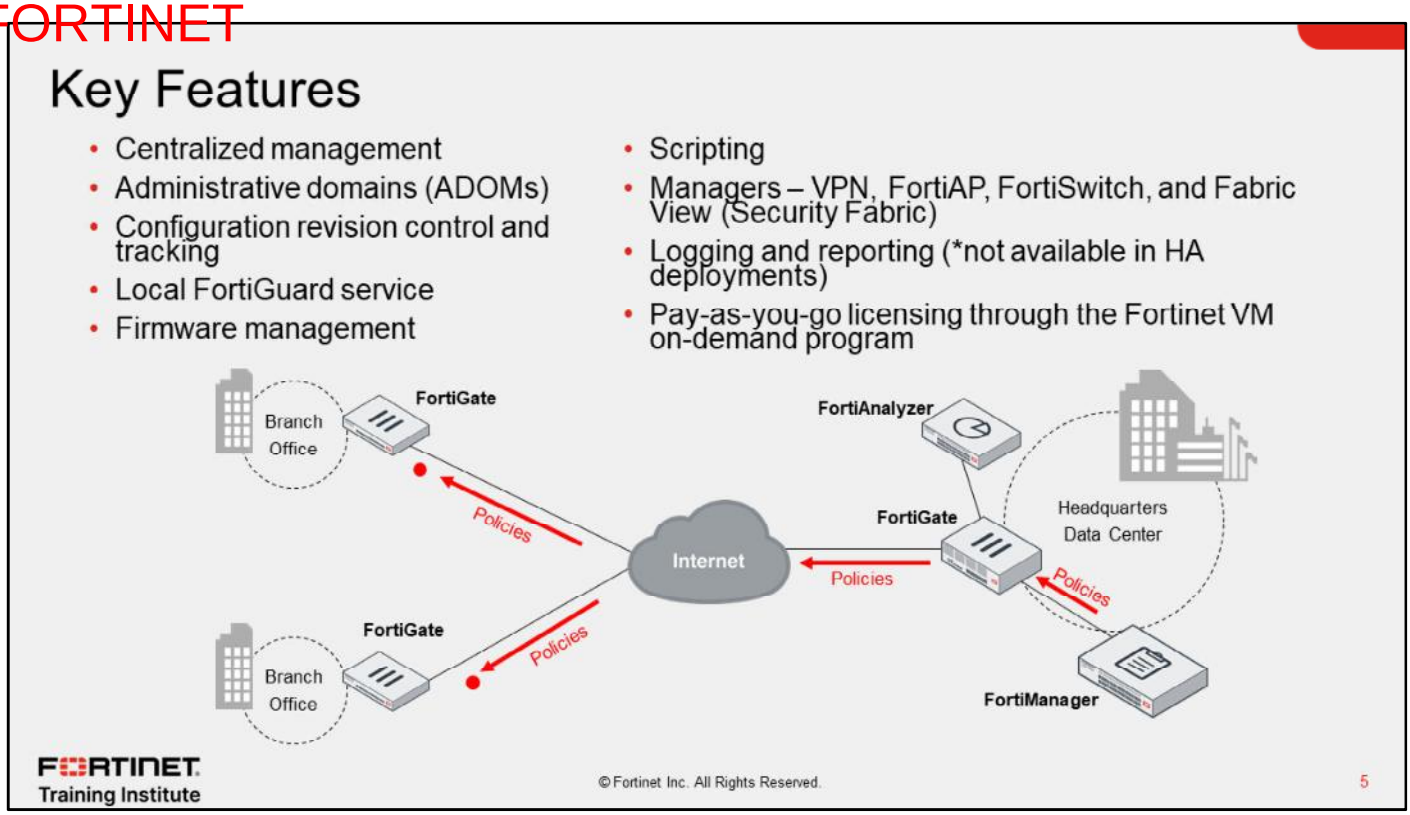
Centralized management through FortiManager can help you to more easily manage many deployment types with many devices, and to reduce the cost of operation.

What can FortiManager do?

- Provision firewall policies across your network
- Act as a central repository for configuration revision control and security audits
- Deploy and manage complex mesh and star IPsec VPNs
- Act as a private FortiGuard distribution server (FDS) for your managed devices
- Script and automate device provisioning, policy changes, and more, with JSON APIs

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

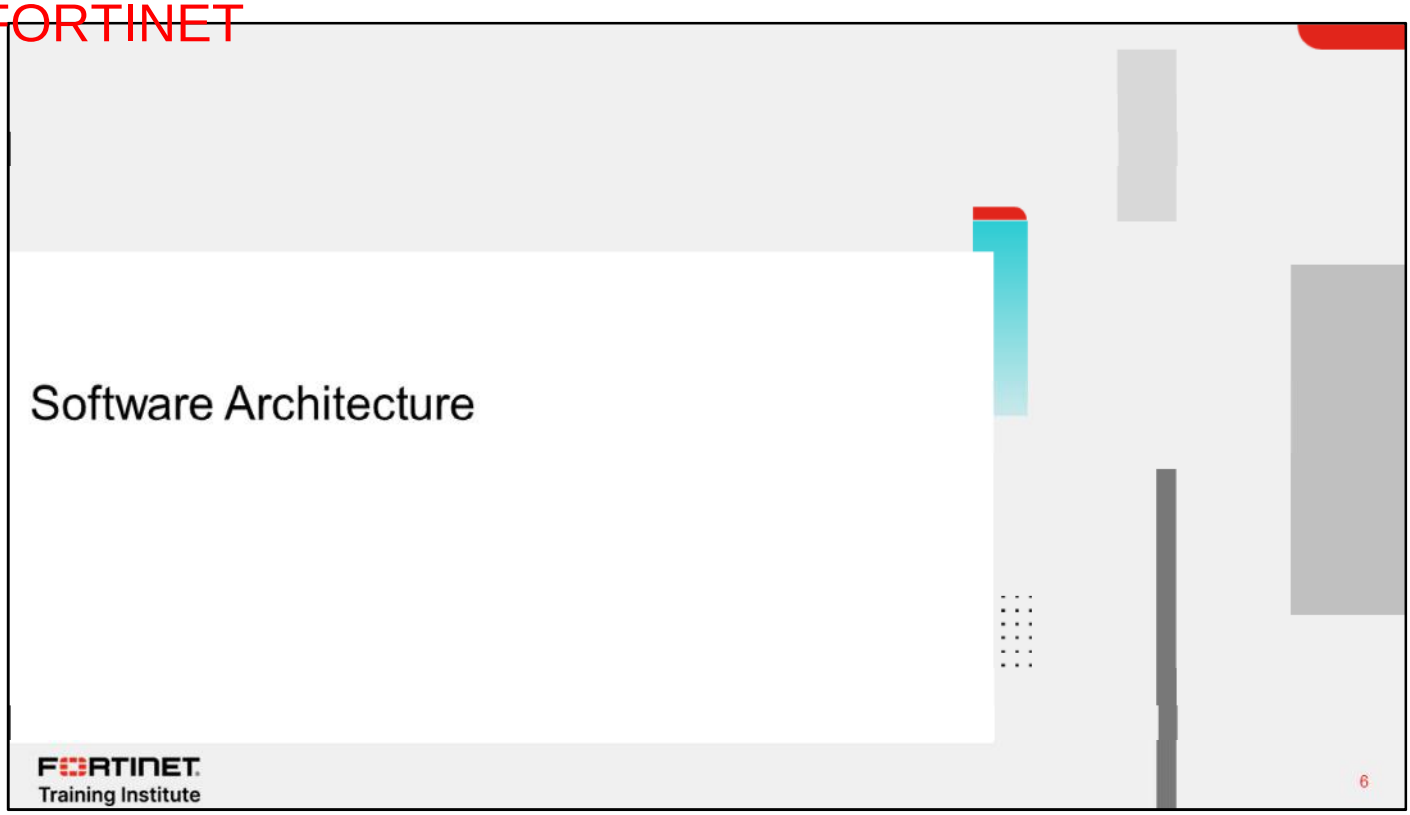


FortiManager can help you to better organize and manage your network. Key features of FortiManager include:

- **Centralized management**: Instead of logging in to hundreds of FortiGate devices individually, you can use FortiManager to manage them all from a single console.
- **Administrative domains (ADOMs)**: FortiManager can group devices into geographic or functional ADOMs, which is ideal if you have a large team of network security administrators.
- **Configuration revision control**: Your FortiManager keeps a history of all configuration changes. You can schedule FortiManager to deploy a new configuration or revert managed devices to a previous configuration.
- **Local FortiGuard service provisioning**: To reduce network delays and minimize internet bandwidth usage, your managed devices can use FortiManager as a private FDN server.
- **Firmware management**: FortiManager can schedule firmware upgrades for managed devices.
- **Scripting**: FortiManager supports CLI-based and TCL-based scripts for configuration deployments.
- **Pane Managers (VPN**, **FortiAP**, **FortiSwitch**, **and Fabric View)**: FortiManager management panes simplify the deployment and administration of VPN, FortiAP, FortiSwitch, and Fabric View (Security Fabric).
- **Logging and reporting**: Managed devices can store logs on FortiManager. From that log data, you can generate SQL-based reports, because FortiManager has many of the same logging and reporting features as FortiAnalyzer.
- **FortiMeter**: Allows you turn FortiOS-VMs and FortiWebOS-VMs on and off as needed, paying only for the volume and consumption of traffic that you use. These VMs are also sometimes called pay-as-you-go VMs. You must have a FortiMeter license and the FortiMeter license must be linked with FortiManager by using FortiCare.

Vouchers & Dumps are Available | WhatsApp +201224560923

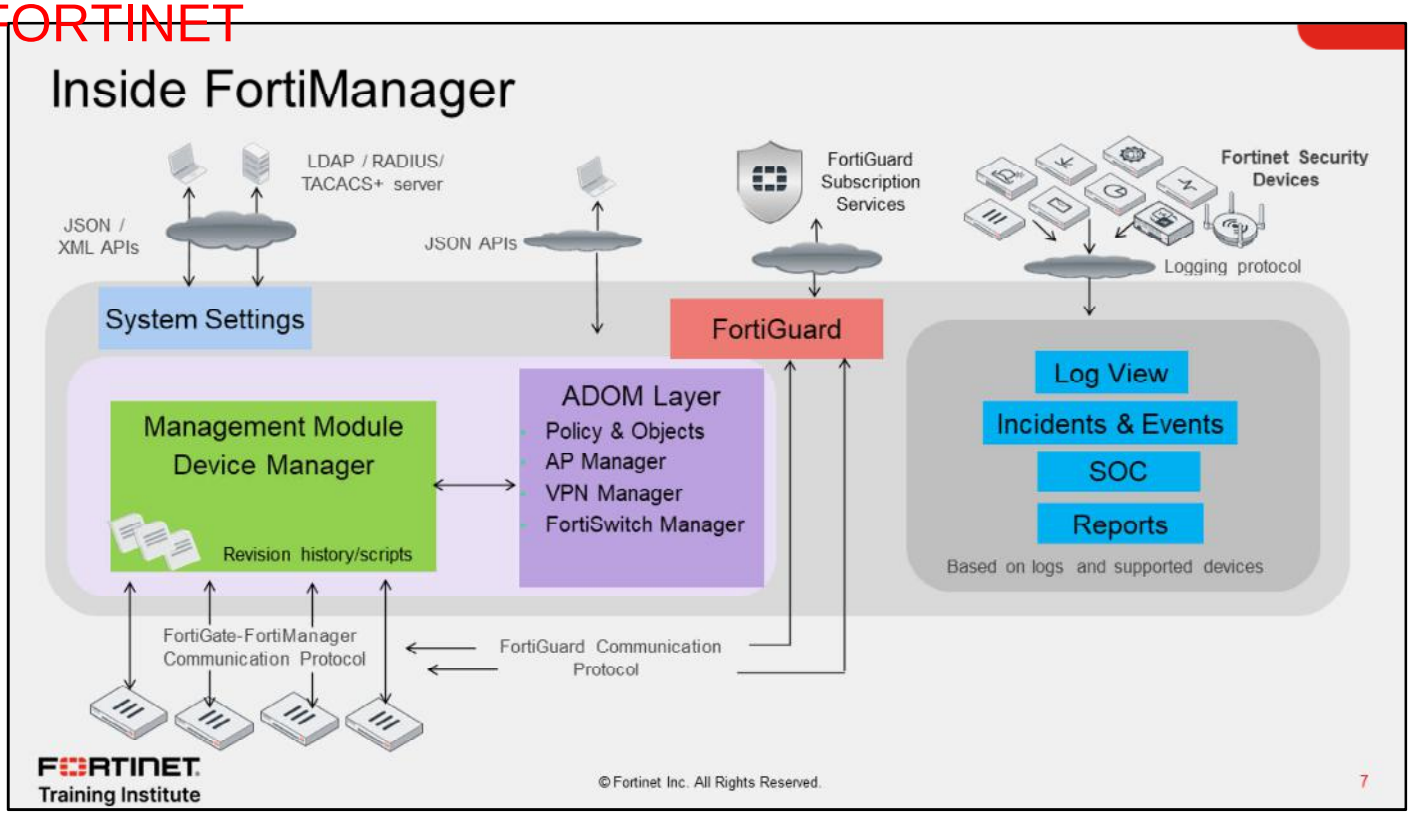
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will examine FortiManager software architecture.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Inside FortiManager, there are management layers that are represented as panes on the GUI. The device management layer, for example, is represented by the **Device Manager** pane, which performs revision history and scripting.

Now, you will look at the management layers in further detail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Management Layers

- Global ADOM layer
  - Global objects
  - All header and footer policies
- ADOM layer
  - Common object database, devices, device groups, policy packages
- 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.

8

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

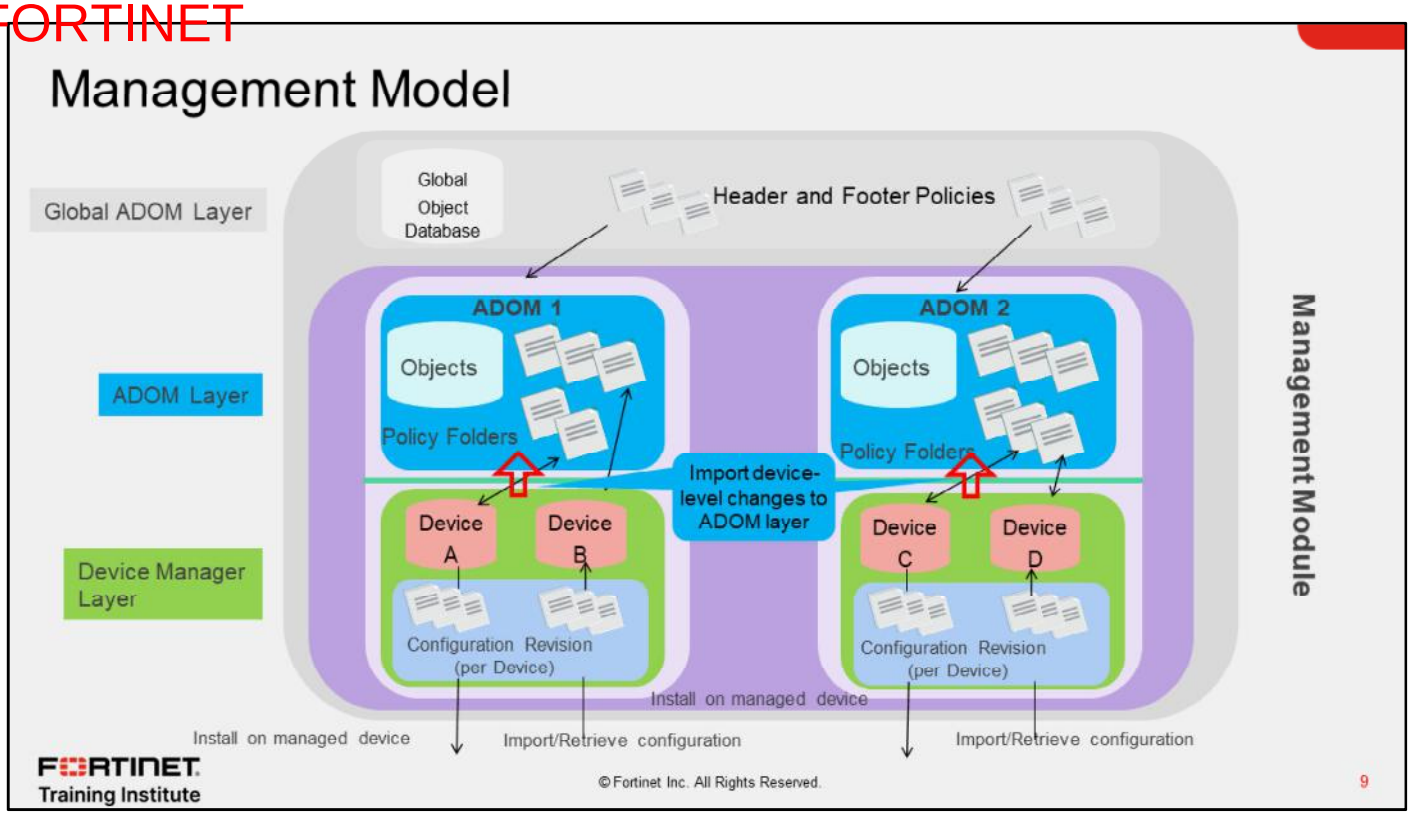
The Global ADOM layer has two key pieces: the global object database, and header and footer policy packages. Header and footer policy packages envelop the policies of each ADOM. An example of where policy packages are used is in a carrier environment, where the carrier allows customer traffic to pass through their network, but does not allow the customer to have access to the carrier 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.

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.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Understanding the layers of the FortiManager management model is important.

In the Global ADOM layer, you create header and footer policy rules. You can assign these policy rules to multiple ADOMs. If multiple ADOM policy packages require the same policies and objects, you can create them in this layer so that you don't have to maintain copies in each ADOM.

In the ADOM layer, objects and policy packages in each ADOM share a common object database. You can create, import from, and install policy packages on many managed devices at once.

In the Device Manager layer, you can configure and install device settings for each device. If a configuration change is detected—made locally or on FortiManager—FortiManager compares the current configuration to the changed configuration, and creates a new configuration revision on FortiManager. Whether the configuration change is big or small, FortiManager records it and saves the new configuration. This can help administrators to audit configuration changes, and to revert to a previous revision, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Administrative Domains

- Administrative subdivision
- Not enabled by default
  - Can only be enabled by administrator accounts
- Accounts are assigned to ADOM
  - Administrators with the Super_User profile have full access
  - Other administrators can have access to all ADOMs, or be restricted to a specific ADOM subset
- You can assign FortiGate devices with multiple VDOMs to multiple ADOMs
- Maximum number of ADOMs varies by model

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

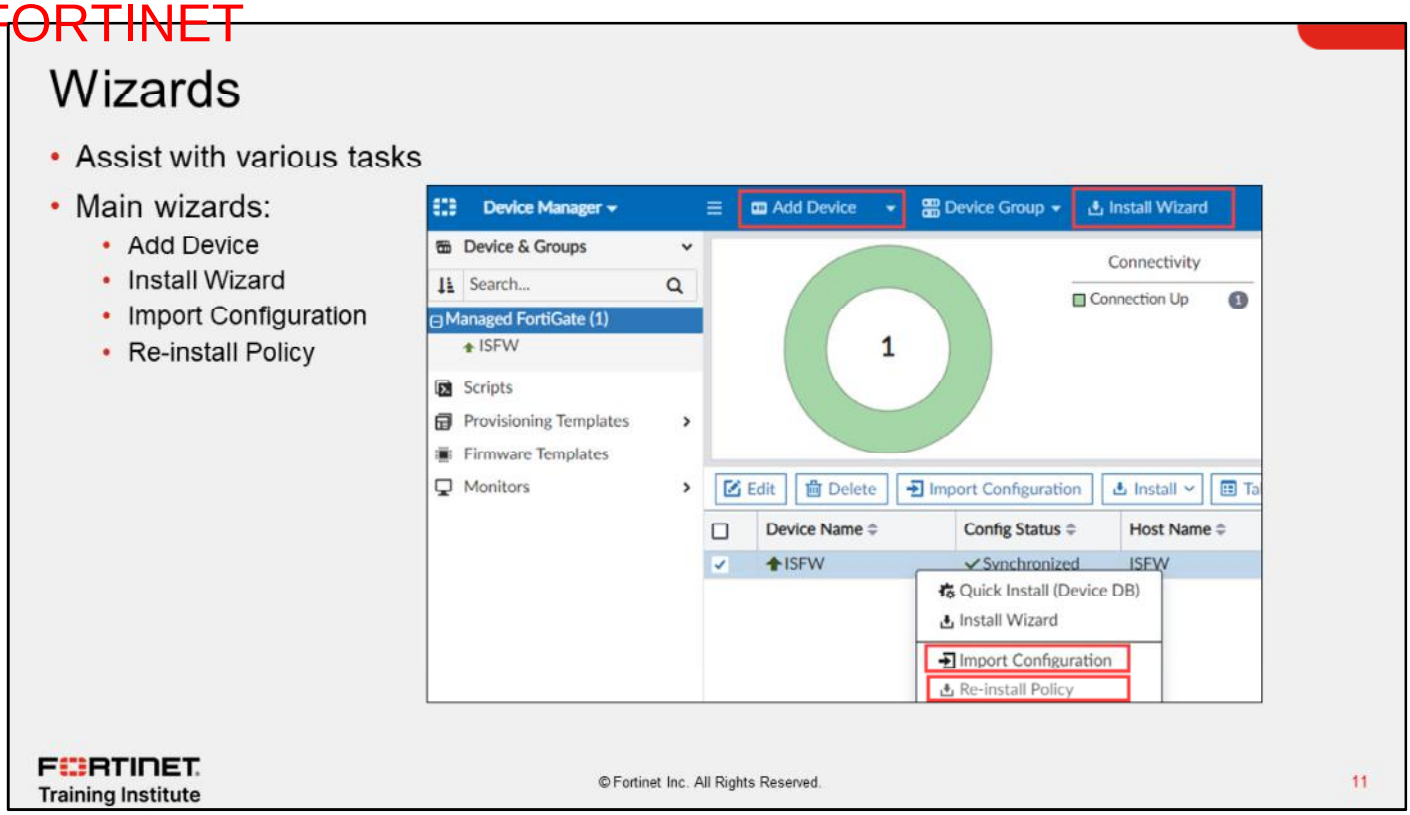
What is an ADOM?

ADOMs enable the administrator account to create groupings of devices for administrators to monitor and manage. For example, administrators can manage devices specific to their geographic location or business division. ADOMs are not enabled by default and must be enabled by the administrator.

The purpose of ADOMs is to divide the administration of devices, by grouping them based on management criteria, and to control (restrict) administrative access. Administrative access is assigned based on an administrator profile that allows access to one or multiple ADOMs on the device. If the administrator uses virtual domains (VDOMs), ADOMs can further restrict access to data from only the VDOM of a specific device. The number of available ADOMs varies based on model.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



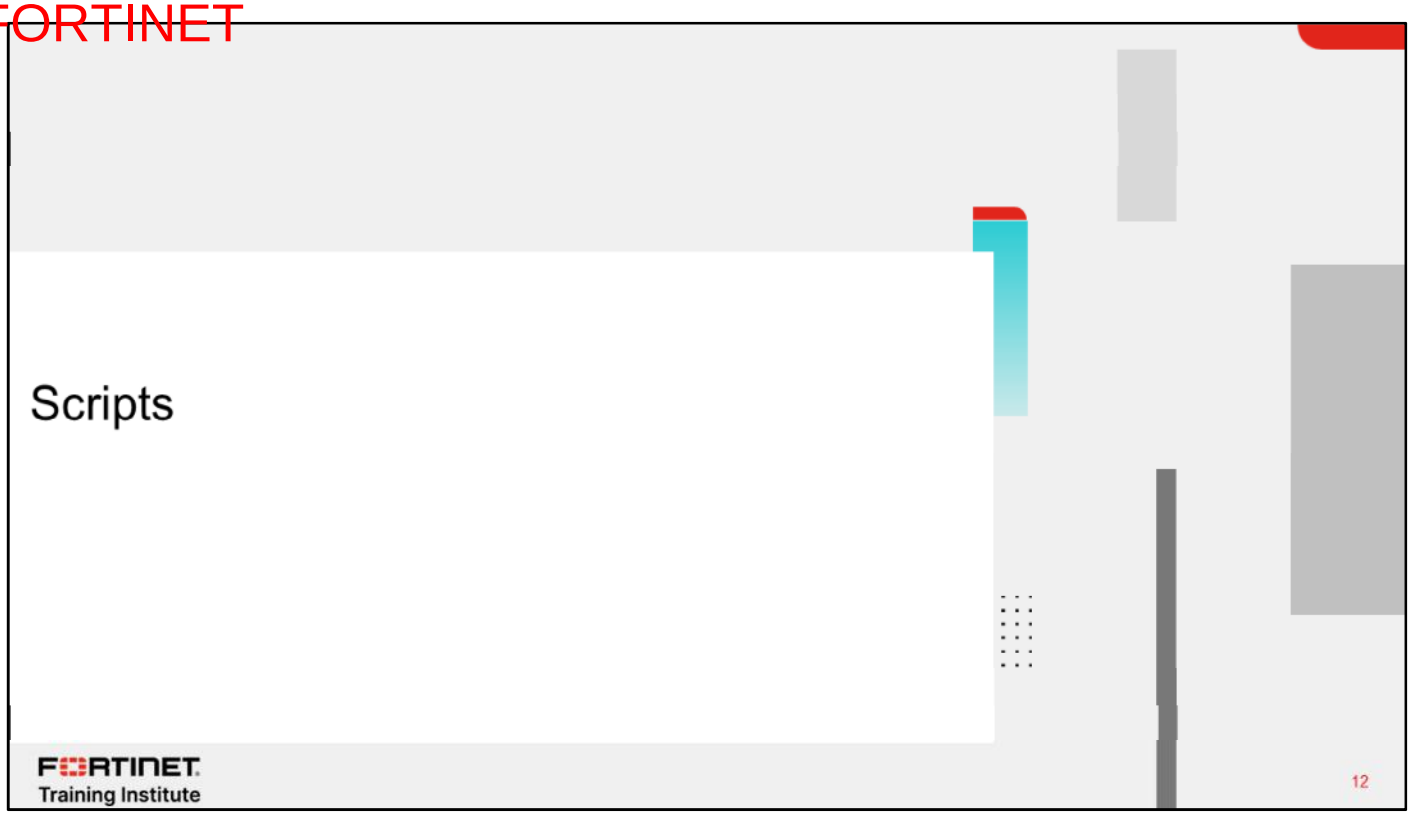
The **Device Manager** pane provides device and installation wizards to aid you in various administrative and maintenance tasks. Using these wizards can decrease the amount of time it takes to do many common tasks. There are four main wizards in the **Device Manager** pane:

- **Add Device** is used to add devices to central management and import their configurations.
- **Install Wizard** is used to install configuration changes from the **Device Manager** pane or **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.
- **Import Configuration** is used to import interface mappings, policy databases, and objects associated with the managed devices into a policy package under the **Policy & Object** pane. It runs with the **Add Device** wizard, by default, and may be run at any time from the managed device list.
- **Re-install Policy** is used to perform a quick install 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

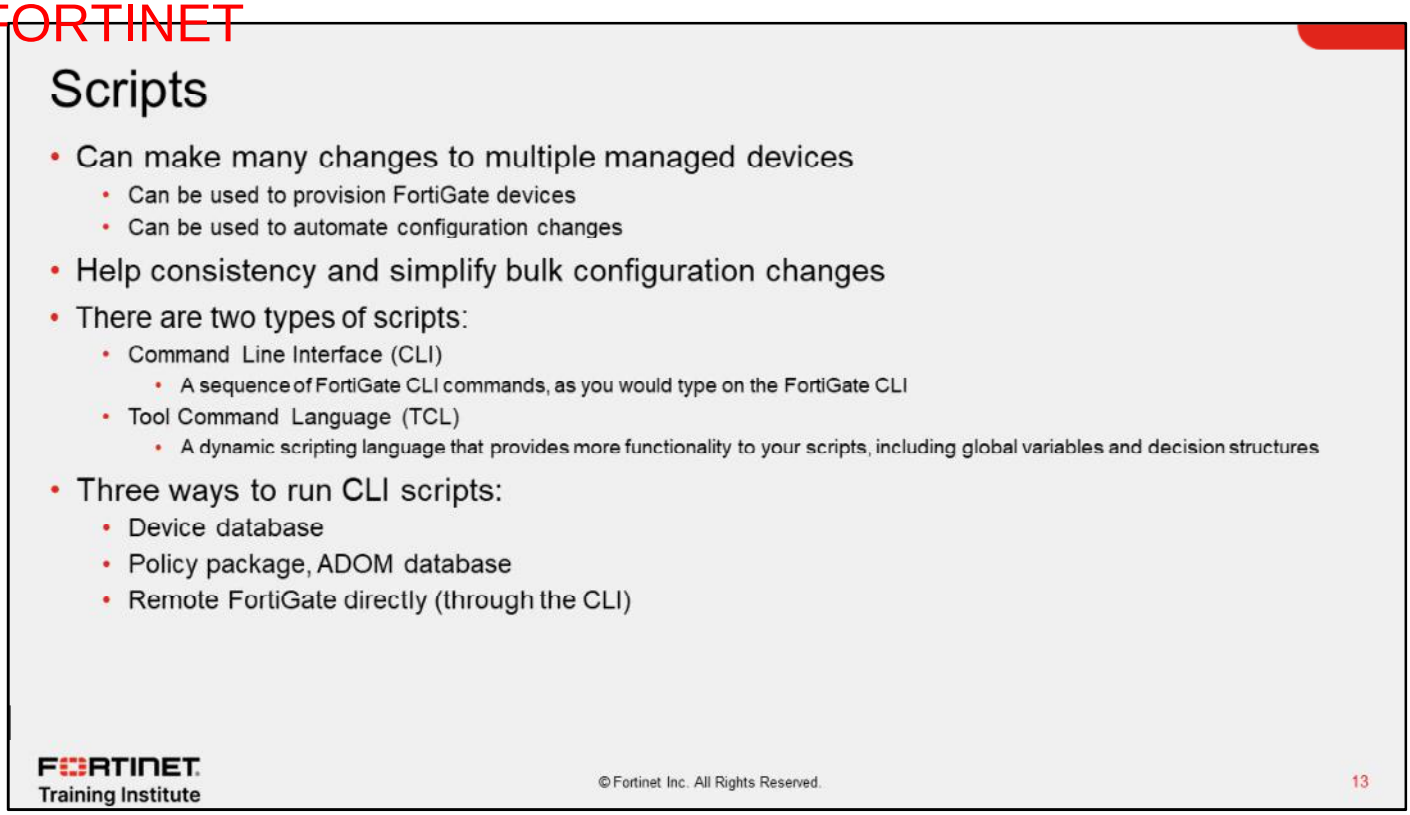
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn about the scripting options that are available on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A script can make many changes to a managed device and is useful for bulk configuration changes and consistency across multiple managed devices. FortiManager supports two types of scripts: CLI scripts and TCL scripts.

CLI scripts include only FortiOS CLI commands as they are entered on the command line prompt on a FortiGate device. TCL is a dynamic scripting language that extends the functionality of CLI scripting. In FortiManager TCL scripts, the first line of the script is `#!`. This is standard for TCL scripts. Do not include the exit command that normally ends TCL scripts because it prevents the script from running. You need to be familiar with the TCL language and regular expressions. For more information on TCL scripts, refer to the official TCL website: http://www.tcl.tk.

CLI scripts are enabled by default.

CLI scripts can be run in three different ways:

- **Device database**: By default, a script is run on the device database. It is recommend that you run the changes on the device database (default setting), because this allows you to check what configuration changes you will send to the managed device. After scripts run on the device database, you can install these changes to a managed device using the installation wizard.
- **Policy package, ADOM database**: If a script contains changes related to ADOM-level objects and policies, you can change the default selection to run on **Policy package, ADOM database**, and then install it using the installation wizard.
- **Remote FortiGate directly (through CLI)**: You can run a script directly on the device without installing these changes using the installation wizard. Because you installed the changes directly on the managed device, the system does not provide an option to verify and check the configuration changes through FortiManager before executing it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

TCL Scripts

- You can enable TCL scripts on the FortiManager CLI

```
config system admin setting
  set show_tcl_script enable
end
```

- TCL scripts do not run through the FGFM tunnel like CLI scripts
- TCL scripts use SSH and require SSH authentication to work

- Can run only on:
  - Remote FortiGate directly (through the CLI)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

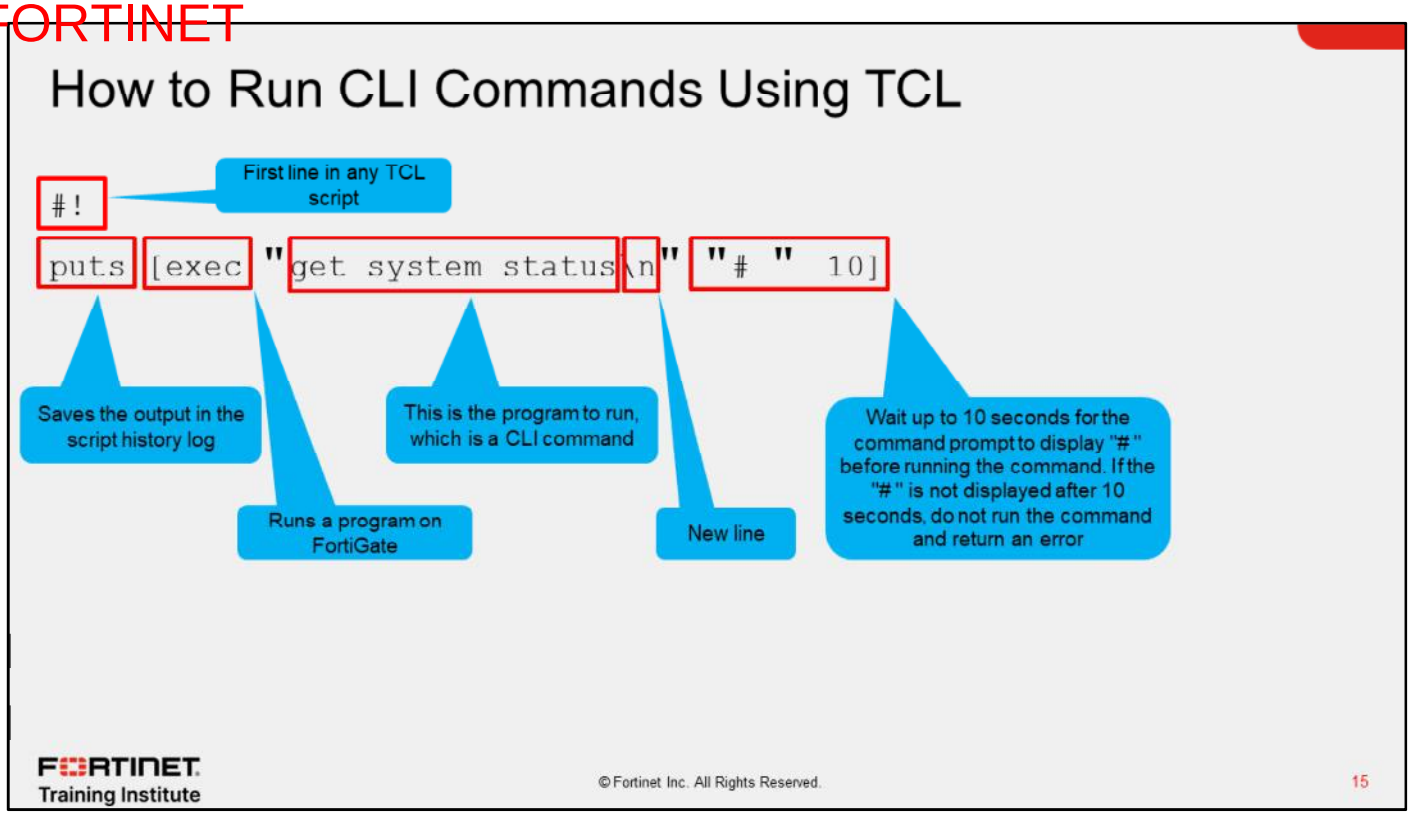
For TCL scripts, you must enable the `show` command for TCL scripts on the FortiManager CLI.

Note that TCL scripts do not run through the FGFM tunnel like CLI scripts do. TCL scripts use SSH to tunnel through FGFM, and they require SSH authentication to do so. If FortiManager does not use the correct administrative credentials in Device Manager, the TCL script fails. CLI scripts use the FGFM tunnel, and the FGFM tunnel is authenticated using the FortiManager and FortiGate serial numbers.

You can run TCL scripts only on the remote FortiGate directly (through the CLI). The main advantage of a TCL script over a Jinja script is that it runs on the managed devices, whereas a Jinja script runs only on FortiManager, and then you push the configuration changes to the managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The example on this slide shows how you can run a CLI command from a TCL script. Any TCL script must start with `#!`.

The next line, `exec TCL`, runs the CLI command `get system status`.

The CLI command runs only if the TCL interpreter gets the `#` from the FortiGate command prompt within 10 seconds. If that is not the case, the CLI command does not run, and the script generates an error.

You can use the TCL command `puts` to save the output of the CLI command to the FortiManager script history log.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

TCL Variables

Variable name

Value

```
#!
set newhostname "NGFW"

puts [exec "config system global\n" "# " 10]
puts [exec "set hostname $newhostname\n" "# " 10]
puts [exec "end\n" "# " 10]
```

Prepend the $ sign to a variable name to use its value

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

This slide shows an example of using TCL variables.

The TCL `set` command creates a new variable (`newhostname`) and sets its value to `NGFW`.

You then use the value of the variable (prepending the `$` sign) to configure the FortiGate hostname.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Creating and Calling TCL Procedures

```
#!
proc do_cmd {cmd}
puts [exec "$cmd\n" "# " 10]
}

do_cmd "config system interface"
do_cmd "edit port1"
do_cmd "set ip 10.0.1.10 255.255.255.0"
do_cmd "next"
do_cmd "end"
```

Procedure name

Procedure parameter

Calling the procedure

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

If you are running a command, or a group of commands, multiple times in a script, you can add those commands to a TCL procedure for simplification. You can pass one or more parameters to a TCL procedure.

The example on this slide shows the creation of a TCL procedure called `do_cmd`. This procedure instructs the interpreter to run a CLI command (received through the parameter `cmd`) if the `#` is received within 10 seconds.

After that, the script calls that procedure five times (each time passing a different parameter) to configure the IP address on `port1`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

TCL Example Using Loops

- Creates 150 firewall addresses:

numhost contains the number of addresses to create

Loop: Set the initial value of i to 1 and run the following three lines 150 times

```
set numhosts = 150
do_cmd "config firewall address"
for {set i=1} {$i <= $numhosts} {i=i+1} {
do_cmd "edit host-$i"
do_cmd "set subnet 10.0.1.$i/32"
do_cmd "next"
}
do_cmd "end"
```

Increment the value of i after each loop

Script Results:

```
config firewall address
edit host-1
set subnet 10.0.1.1/32
next
edit host-2
set subnet 10.0.1.2/32
next
...
edit host-150
set subnet 10.0.1.150/32
next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

This slide contains a more complex TCL example that shows the power of TCL scripts. Say that you have 150 hosts in your network and you need to create 150 different firewall addresses: one for each of your hosts. This TCL script uses a loop to do that.

The script uses two variables. The variable `numhosts` contains the number of addresses to create. The variable `i` starts with the value 1 and is incremented after each loop. The loop is run a number of times equal to the variable `numhosts`.

Inside each loop, the variable `i` is used to set the name of the firewall address and its IP address. What is actually run on FortiGate are the 150 firewall addresses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Best Practices for Scripts

- Use complete CLI commands
  - Incomplete CLI commands may cause the script to fail

```
config router static   ✓
conf rout stat         ✗
```

- Commands that start with a number sign (#) do not run

```
#config system dns     ✗
```

- Disable the output more function on the FortiGate CLI
  - Scripts and other outputs longer than a screen length will not run or display correctly

```
config system console
set output {standard | more}
end
```

Default is `more`
Change it to `standard`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

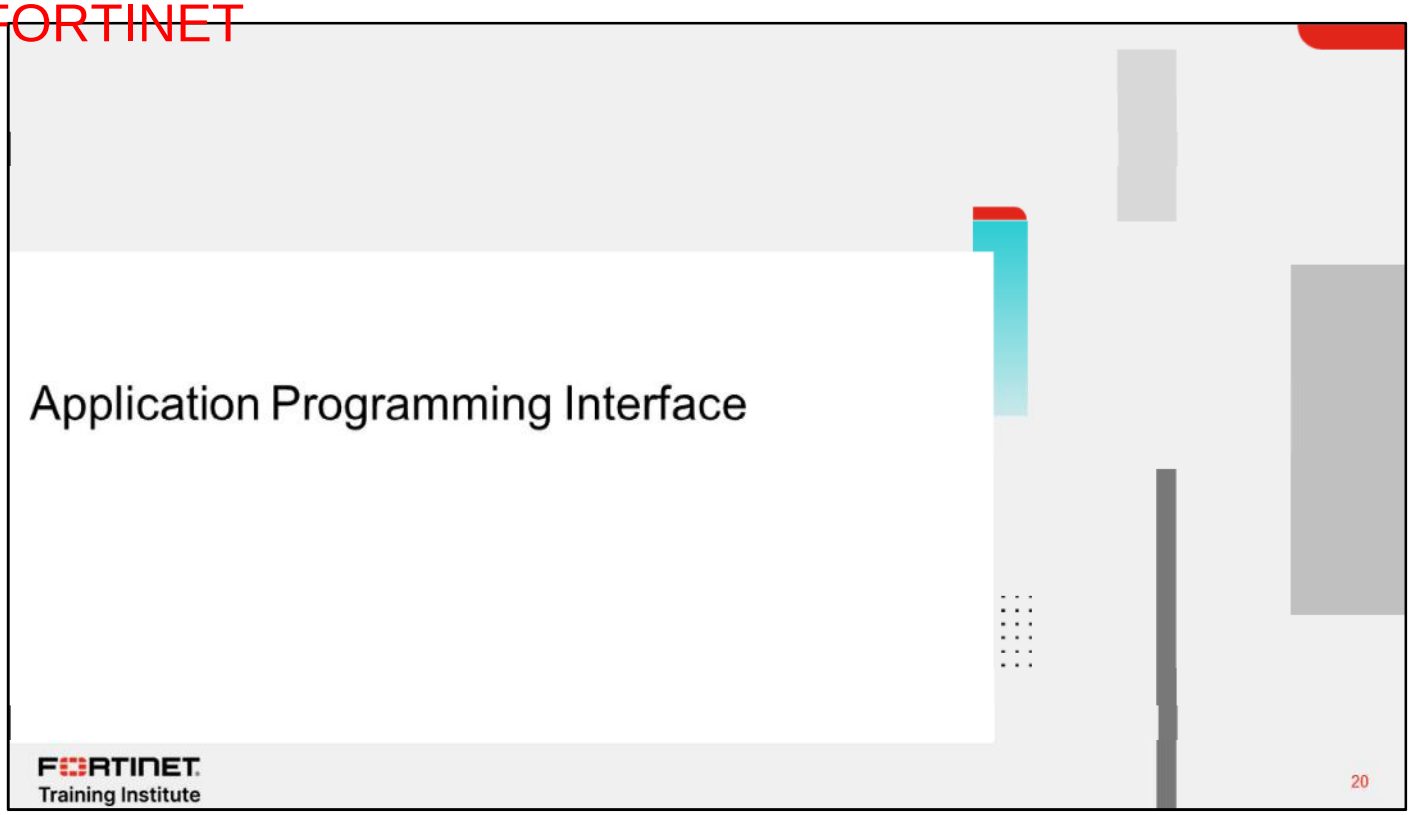
19

When creating CLI scripts, follow these best practices:

- Use complete FortiOS CLI commands. You can use partial syntax; however, it may cause the script to fail.
- Comment lines that start with the number sign (#) do not run.
- On the FortiGate CLI, ensure you set the console output to `standard`. Otherwise, scripts and other outputs longer than a screen in length do not run or display correctly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



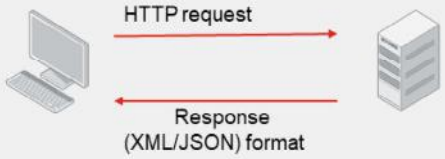
In this section, you will learn about the application programming interface (API) available on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager—API

- An API is a set of rules that allow programs to talk to each other
- The FortiManager API is based on the JSON RPC standard
- Allows MSSPs and large enterprises to create FortiManager self-service web portals
  - Using FortiPortal or any other third-party applications
- A RESTful API uses standard HTTP methods (GET, POST, DELETE) to provide interactions between a client and a server
- The following operations are supported by a RESTful API:
  - Fetch data by sending a GET request
  - Add data by sending a POST request
  - Update data by sending a POST request
  - Delete data by sending a DELETE request
- More details: FNDN and Fortinet document library



JSON example

```
{"employees":[
  { "firstName":"John", "lastName":"Doe" },
  { "firstName":"Anna", "lastName":"Smith" },
  { "firstName":"Peter", "lastName":"Jones" }
]}
```

XML example

```
<employees>
  <employee>
    <firstName>John</firstName> <lastName>Doe</lastName>
  </employee>
  <employee>
    <firstName>Anna</firstName> <lastName>Smith</lastName>
  </employee>
  <employee>
    <firstName>Peter</firstName> <lastName>Jones</lastName>
  </employee>
</employees>
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

The FortiManager JSON API allows you to perform configuration and monitoring operations on a FortiManager device or VM. The JSON API is based on JSON RPC, which is a remote procedure call protocol encoded in JSON. This API allows you to perform many of the same tasks as you can on the FortiManager GUI using FortiPortal or other third-party applications. It allows MSSPs and large enterprises to create customized, branded web portals for FortiManager administration, without directly logging in to FortiManager. This method is very useful in an MSSP environment, where many MSSP customers require their own portal to access FortiManager.

FortiPortal uses the REST API to communicate with FortiManager and gather device details. A RESTful API uses standard HTTP methods (GET, POST, DELETE) for client-server interactions. When FortiPortal (client) makes an HTTP request, FortiManager or FortiAnalyzer (server) responds by returning the requested data in XML or JSON formats. This process is similar to what happens when a browser requests a web page from a server, and then the server responds with the web page in HTML format. When the REST API is being used, the application (FortiPortal) cannot parse the data in HTML format. The application works only with the XML or JSON formats.

The Fortinet Developer Network (FNDN) provides access to tools, sample code, documentation, and access the Fortinet developer community when you subscribe. You can also get more information from the Fortinet documents library.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API HTTP Response Codes

- The API returns an HTTP status code to indicate the status of the request

Code	Message	Details
200	Status ok	Request successful
400	Bad request	Bad request
403	Forbidden	Request is missing the CSRF token or administrator is missing access profile permissions
404	Not Found	Unable to find the specified resource
405	Method Not Allowed	Specified HTTP method is not allowed for this resource
413	Request Entity Too Large	
424	Failed Dependency	
500	Internal Server Error	

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

As shown in this table, the API returns an HTTP status code to indicate the status of the request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API—Example

- View the policy package in the ADOM

Request

```
https://<ip address>:<port>/jsonrpc
{
  "method": "get",
  "params": [
    {
      "fields": [
        [
          "{attribute}"
        ]
      ],
      "url": "/pm/pkg/adom/Core"
    }
  ],
  "session": "string",
  "id": 1
}
```

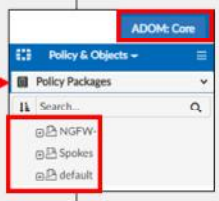
FortiManager IP address and port

Method: GET

Requesting the policy package from the ADOM

Response

```
{    "id": 1,
     "result": [
         {
           "data": [
               {
                   "name": "default",
                   "oid": 1418
               },
               {
                   "name": "Spokes",
                   "oid": 1589
               },
               {
                   "name": "NGFW-1",
                   "oid": 5465
               }
           ],
           "status": {
               "code": 0,
               "message": "OK"
           },
           "url": "\/pm\/pkg\/adom\/Core"
         }
       ]
     }
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

The API example on this slide shows how to get the policy package information from the ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API—Example (Contd)

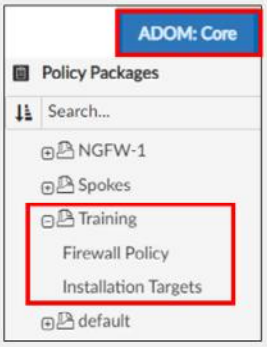
- Add the policy package in the ADOM

Request

```
https://<ip address>:<port>/jsonrpc
{
  "method": "add",
  "params": [
    {
      "data": [
        {
          "name": "Training",
          "type": "pkg"
        }
      ],
      "url": "/pm/pkg/adom/Core"
    }
  ],
  "session": "string",
  "id": 1
}
```

Response

```
{
    "id": 1,
    "result": [
        {
            "status": {
                "code": 0,
                "message": "OK"
            },
            "url": "\/pm\/pkg\/adom\/Core"
        }
    ]
}
```



name and type parameters are mandatory to create the policy package

FORTINET Training Institute

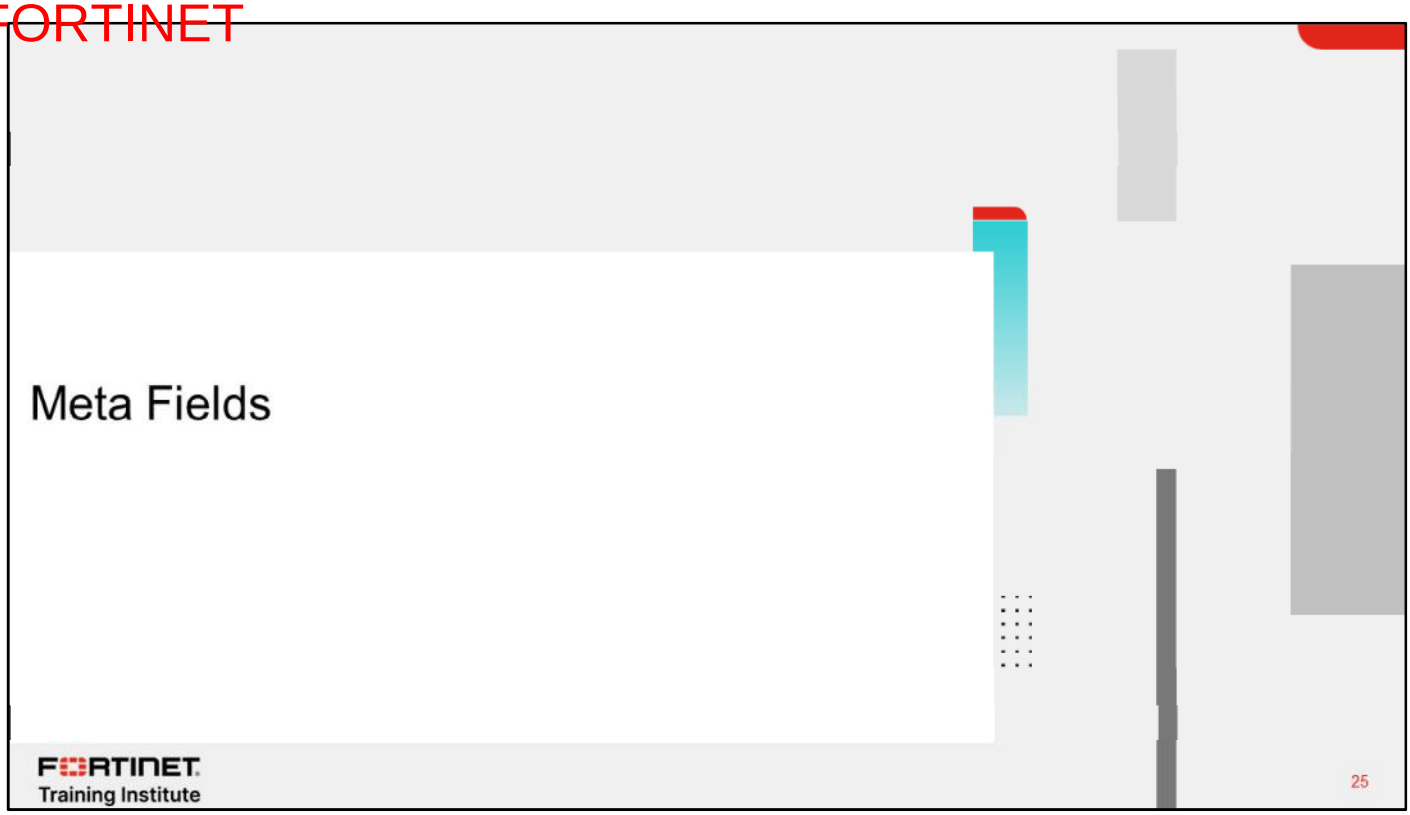
© Fortinet Inc. All Rights Reserved.

24

The API example shows how to add a policy package in the ADOM. As shown on this slide, the policy package named **Training** has been added to the ADOM **Core**.

Vouchers & Dumps are Available | WhatsApp +201224560923

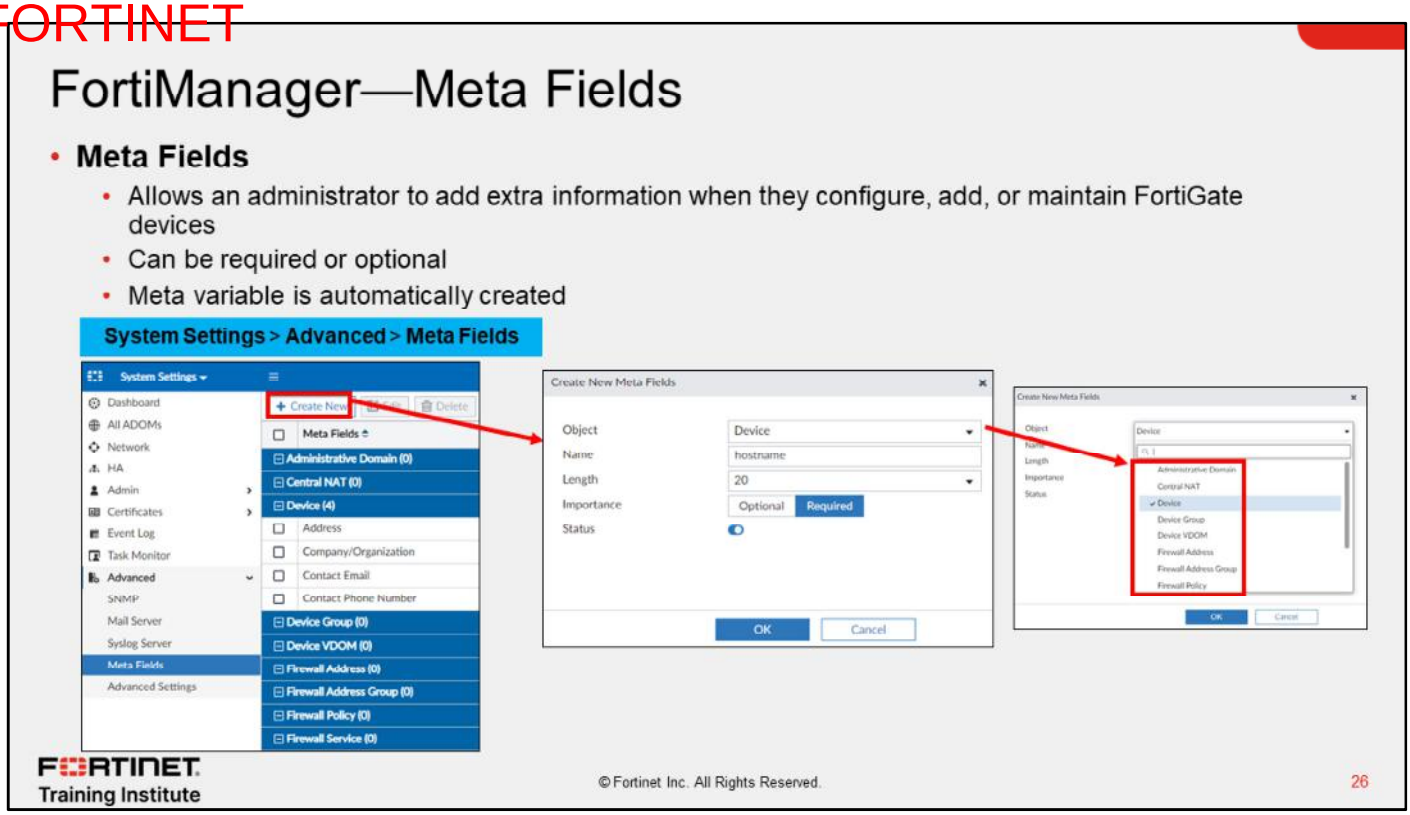
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn about the meta fields that are available on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



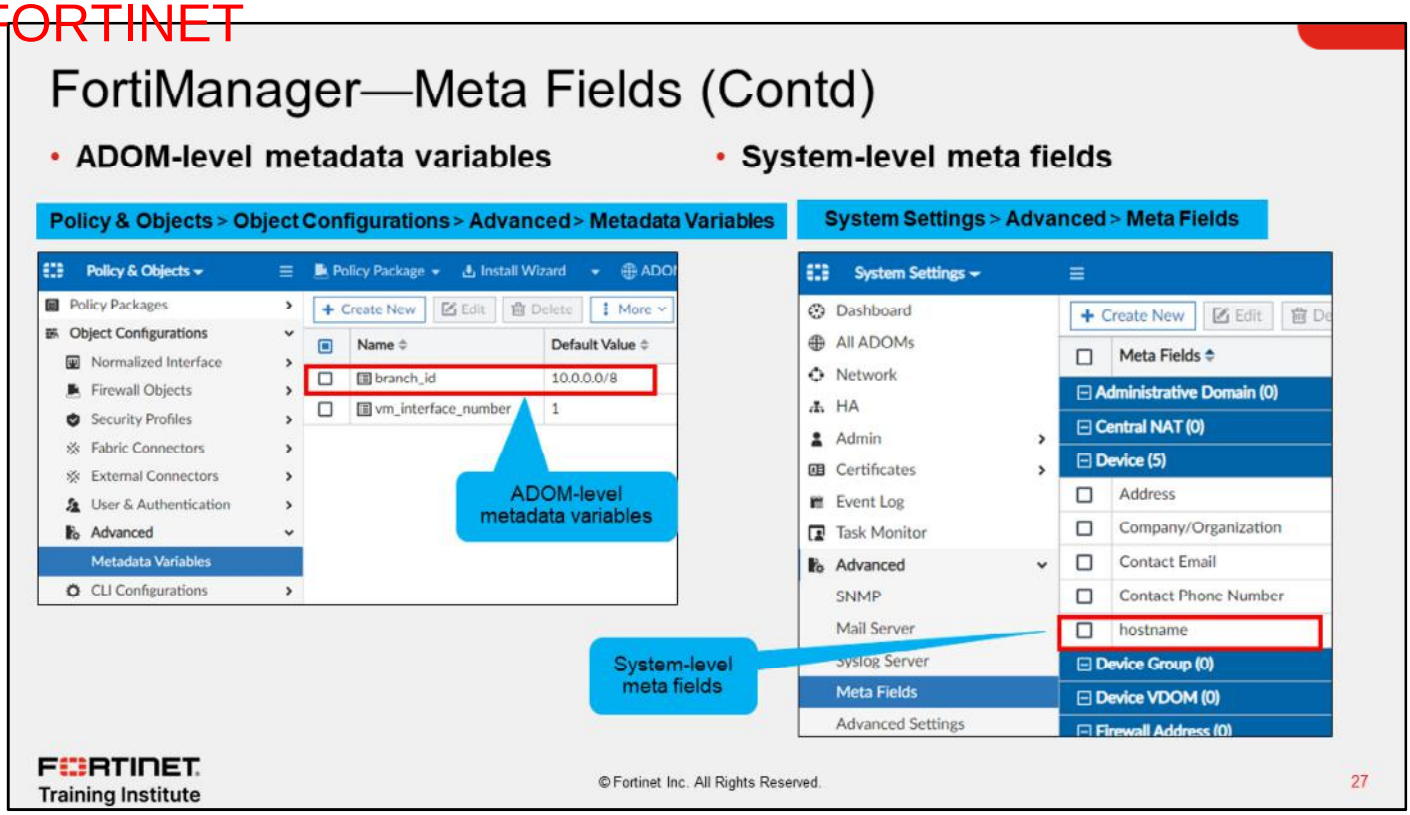
Meta fields allow administrators to add extra information when they configure, add, or maintain FortiGate devices or add new administrators. You can make meta fields required or optional. When meta fields are required, administrators must supply additional information when they create an associated object. For example, if you create a required meta field for a device object, administrators must define a value for the meta field for all devices.

When you create a meta field, a variable for the meta field is automatically created. You can configure the following fields to create new meta fields:

- **Object**: allows you to select the object type, such as administrative domain, firewall address group, firewall policy, central NAT, administrator, and so on. This determines where the meta field is used in the configuration.
- **Importance**: allows you to make the meta field setting compulsory on the object that has the meta field option available. For example, if you set the **Contact Email** variable to **Required**, when a FortiManager administrator creates a new administrator, they must provide a contact email address. If you set this field to **Optional**, providing a contact email address is optional.
- **Status**: Determines whether the meta field is available in the object for administrators to configure. If you disable this field, administrators cannot see or select the meta field. This option is available only for non-firewall objects

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

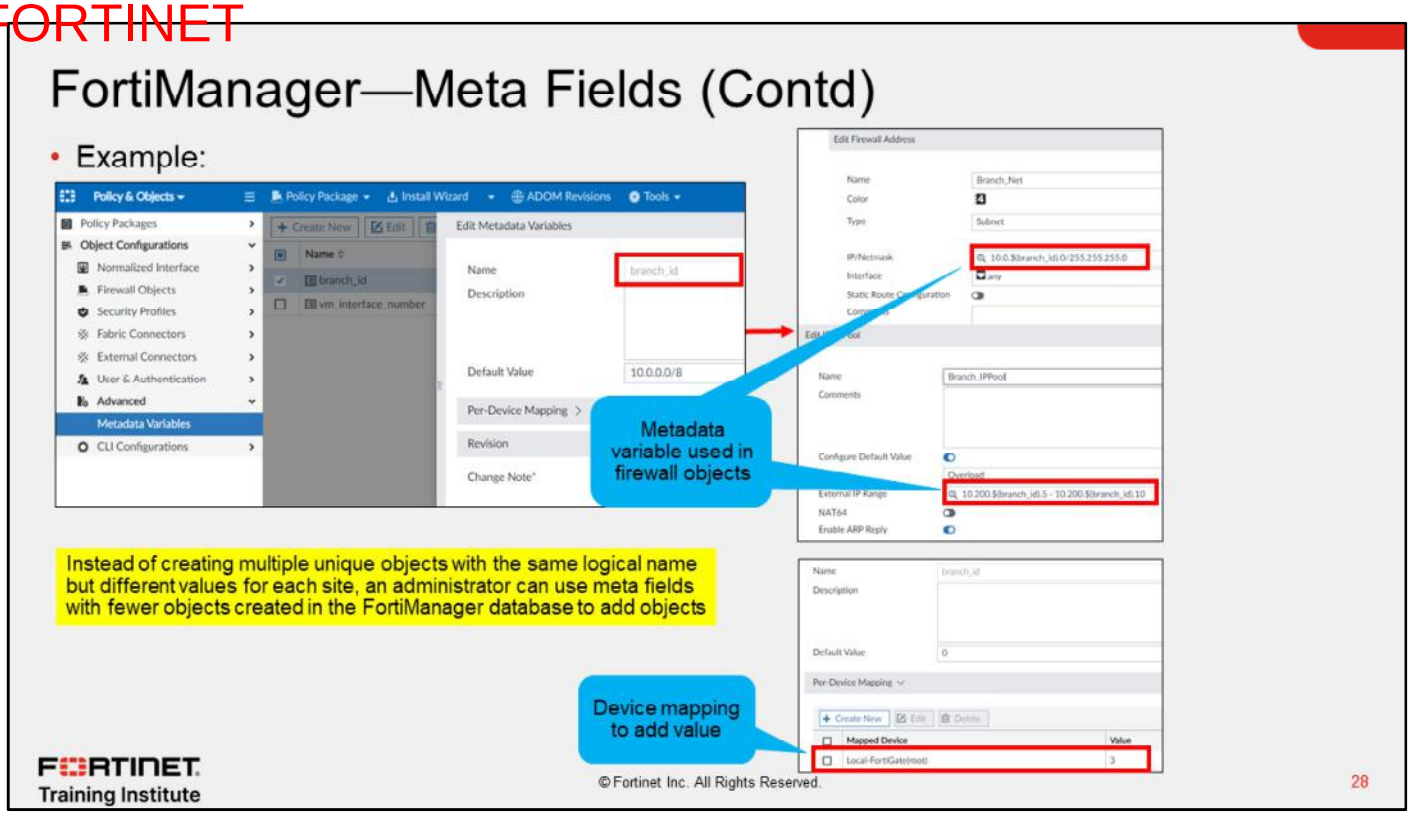


In FortiManager, ADOM-level metadata variables are also available for general use in scripts, templates, and model devices. This slide shows both ADOM-level metadata variables and system-level meta fields. In system-level meta fields, you must also select the object type, such as **Device**, **System Administrator**, and so on.

The terms meta field and metadata variable are interchangeable. Generally, meta field is a legacy term that refers to global changes and metadata variable refers to ADOM-level variables

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

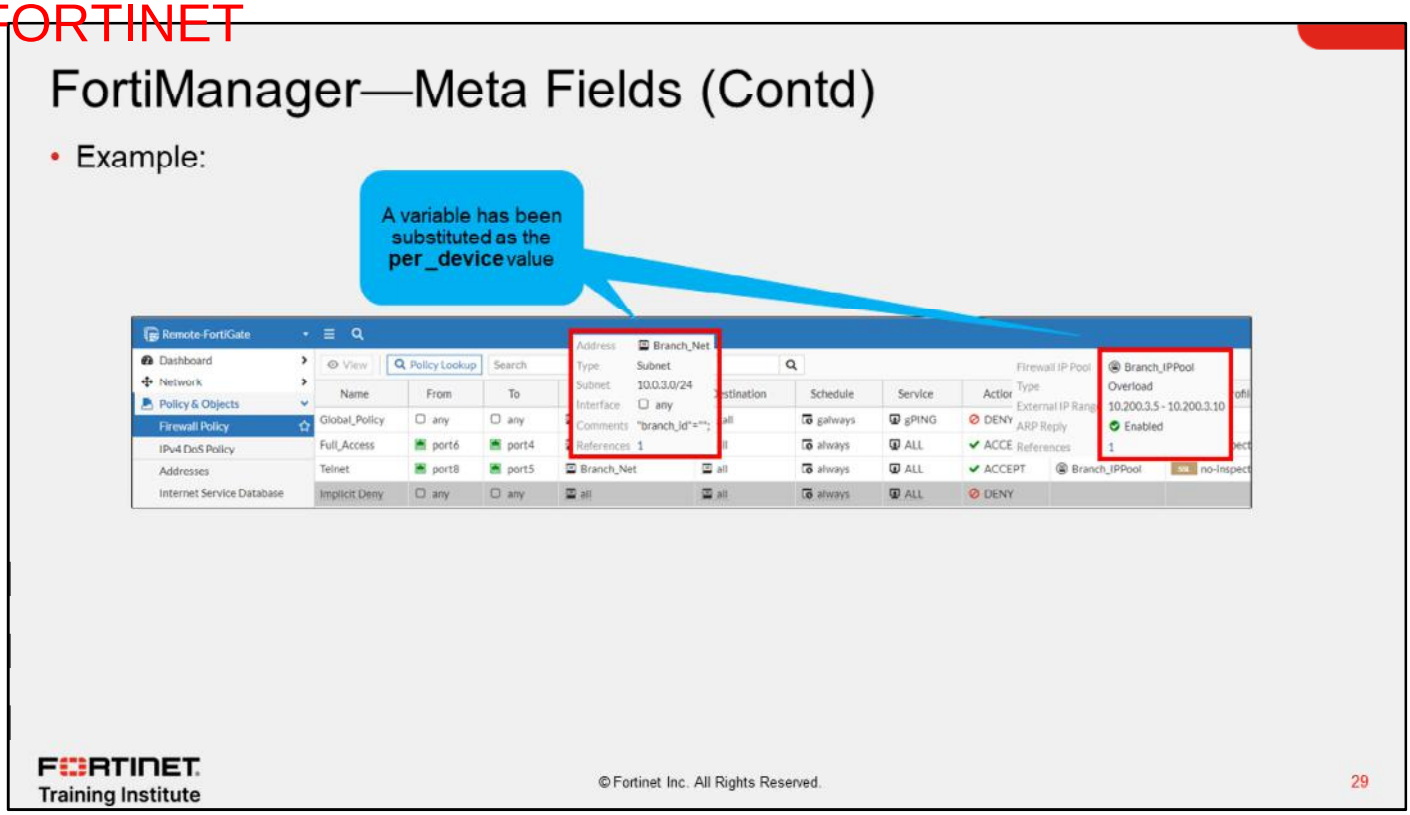


Meta fields are useful when an enterprise has global offices or branches and the FortiManager administrator must create multiple objects with the same logical name, but different values. Instead of creating hundreds of separate address objects or IP pools in the FortiManager ADOM database, an administrator can create a few logical objects and then map each object to create specific address objects for each FortiGate.

In the example shown on this slide, the metadata variable **branch_id** is used in the firewall address object and IP pool. A **branch_id** value is unique for each branch FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

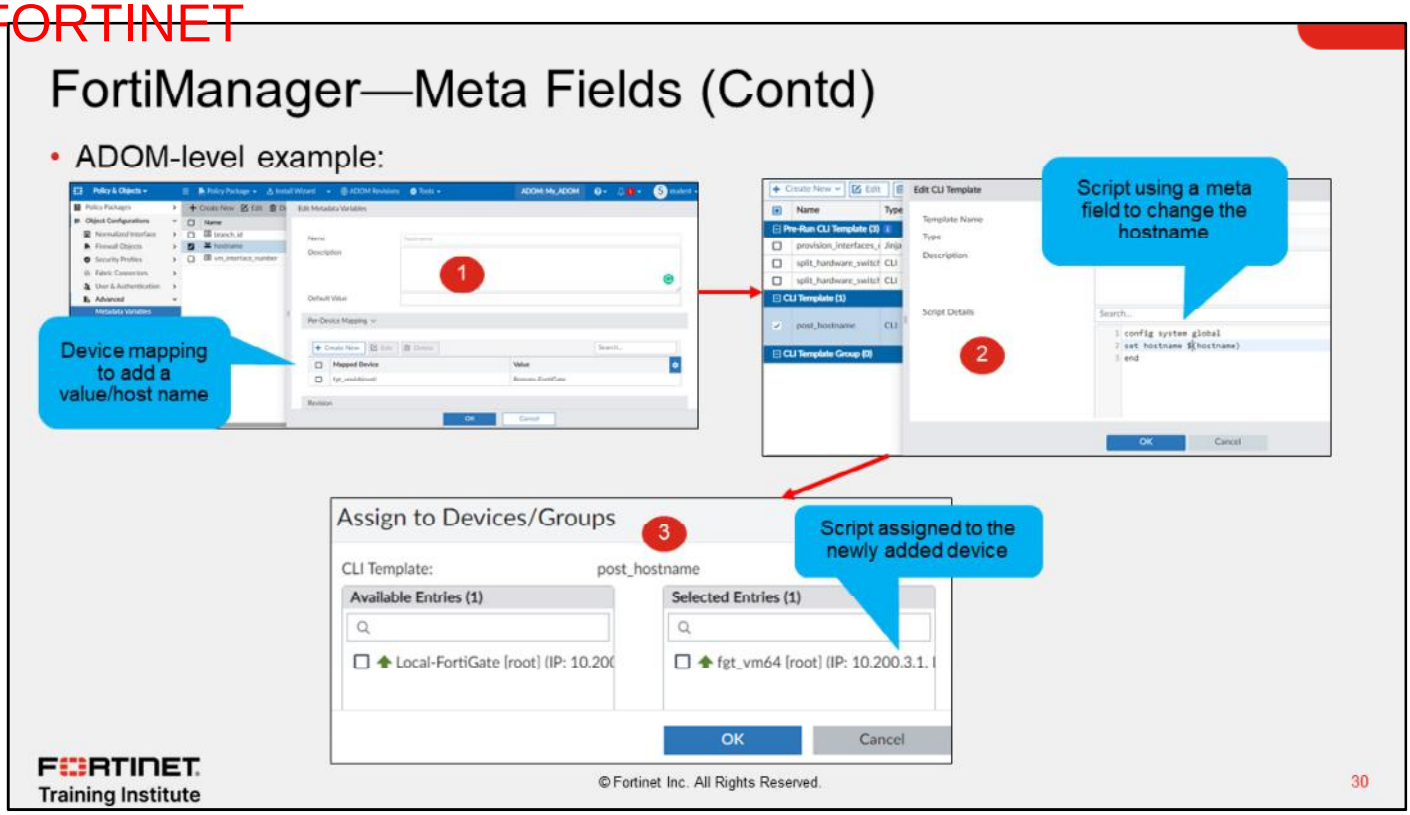
DO NOT REPRINT Brave-dumps.com
© FORTINET



After firewall objects are assigned and the policy package is installed, the **Firewall Policy** on FortiGate shows that the variable **(branch_id)** has been substituted with its **per-device** value **3**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

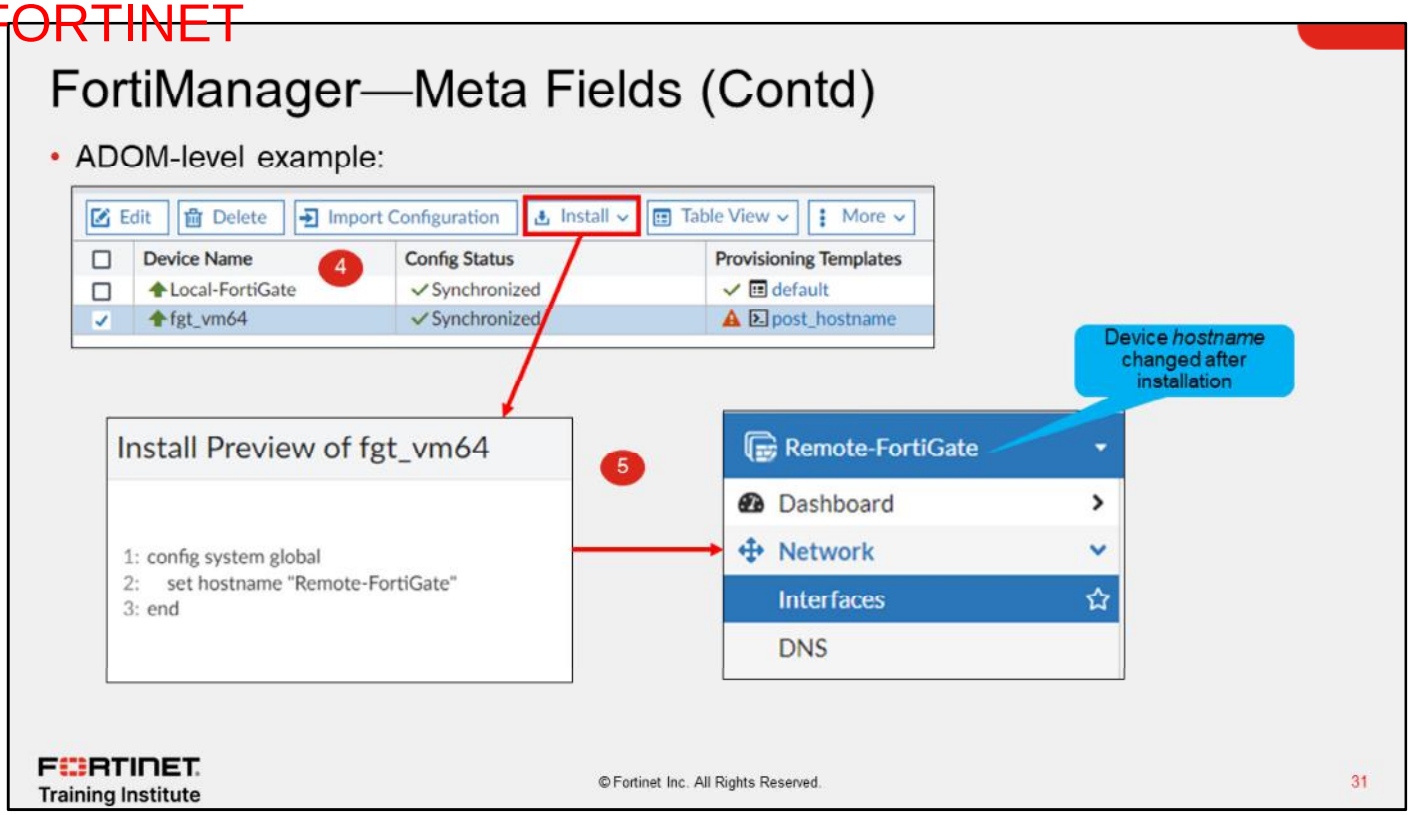


In this example, the CLI template is assigned to and installed on FortiGate **fgt_vm64**. When an installation is performed, the install preview shows that the variable (host name) has been substituted with its per device value **Remote-FortiGate**.

1. Create or edit the metadata variable to map the device and type the value. In this example, **Remote-FortiGate** is set as the value.
2. Use the metadata variable in the script.
3. Assign the script to the targeted FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



4. Install to apply the device-level configuration.
5. The device host name changes to the defined metadata variable value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Examine FortiManager key features
- ✓ Explore FortiManager architecture
- ✓ Explore Device Manager wizards
- ✓ Learn about scripts
- ✓ Identify the APIs supported by FortiManager
- ✓ Understand the meta fields available on FortiManager

FORTINET Training Institute

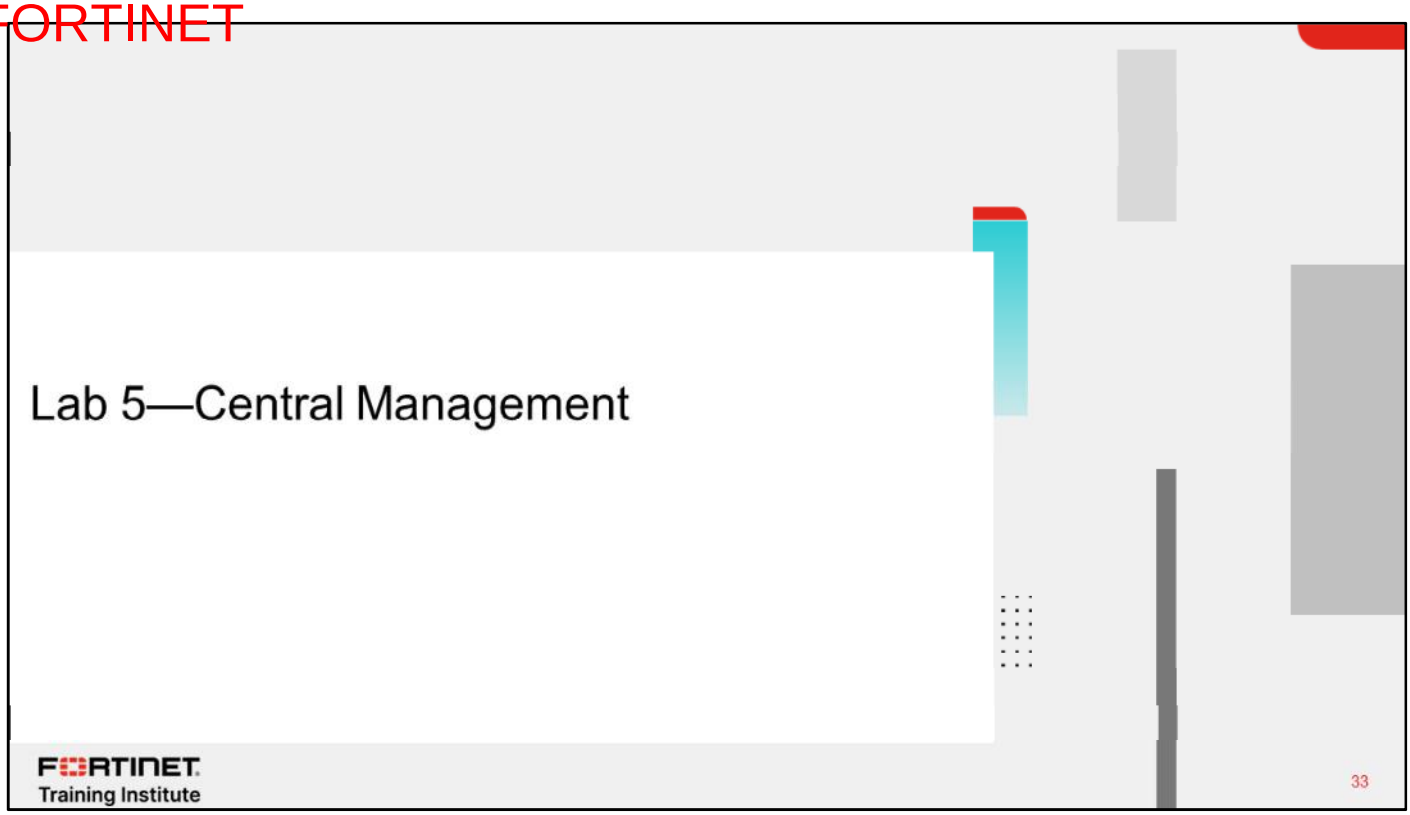
© Fortinet Inc. All Rights Reserved.

32

This slide shows the objectives that you covered in this lesson.
By mastering the objectives covered in this lesson, you learned how to use FortiManager for the central administration of all FortiGate devices in an enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



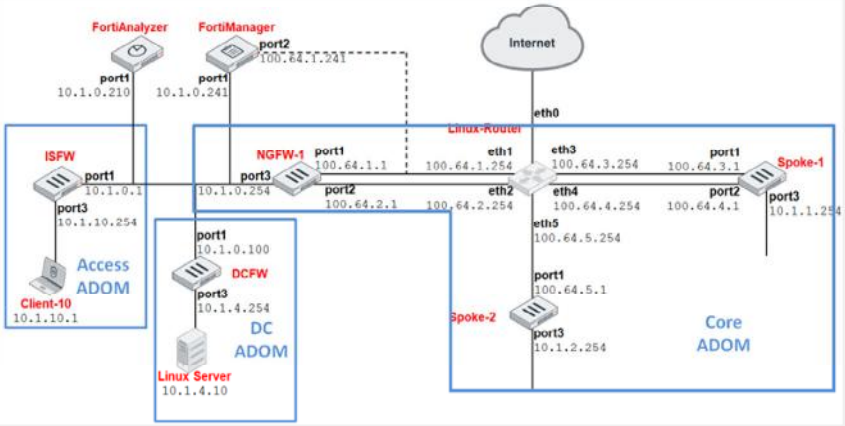
You will now work on *Lab 5–Central Management*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 5—Central Management

- For each FortiGate:
  - Configure the FortiManager IP address
  - Register FortiGate on FortiManager
  - Import the policy package



FORTINET Training Institute

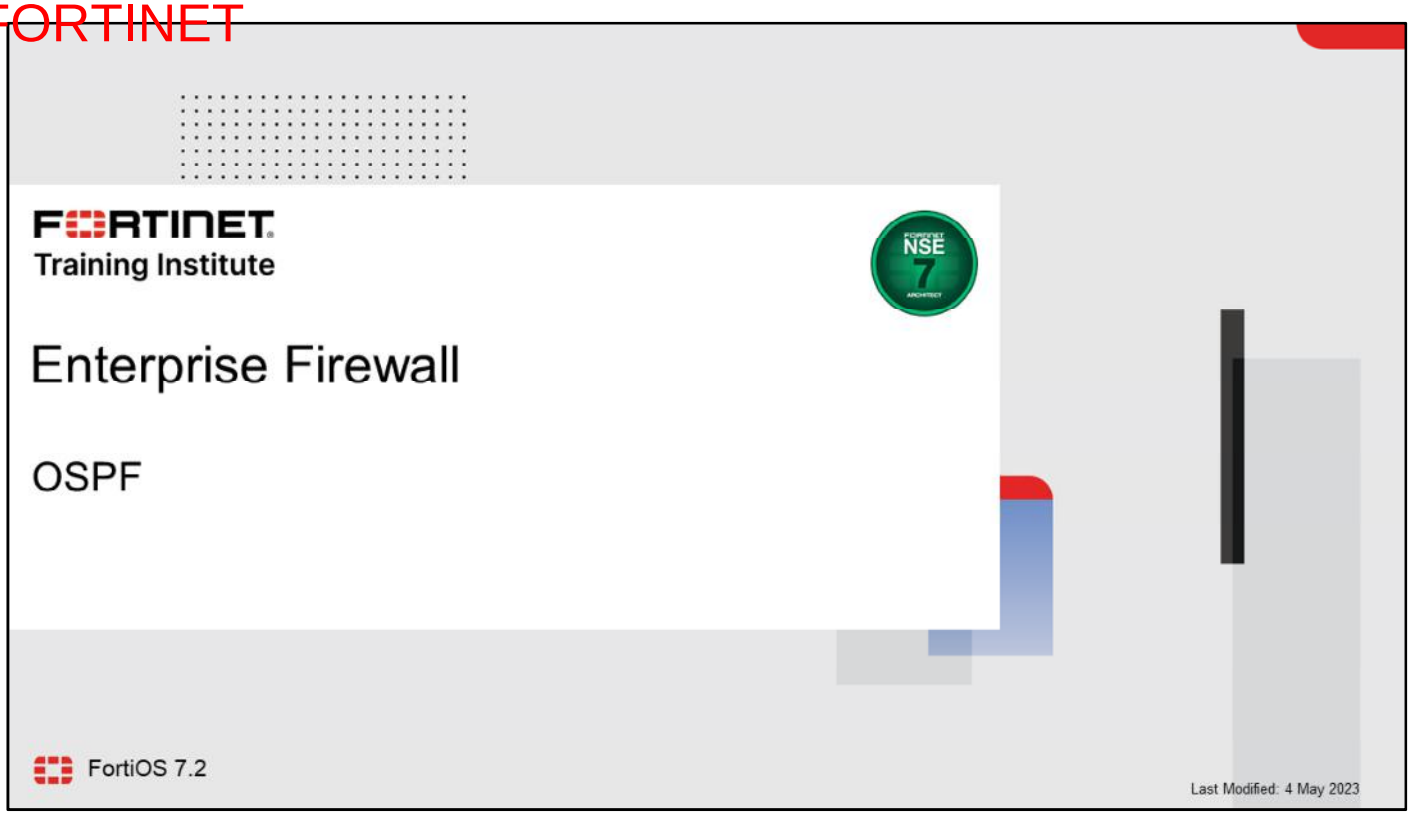
© Fortinet Inc. All Rights Reserved.

34

In this lab, you will configure FortiGate devices and FortiManager to centralize the management of the enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn about how to configure open shortest path first (OSPF) on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Objectives

- Deploy OSPF from FortiManager using CLI templates
- Configure OSPF filter networks
- Redistribute other routes into OSPF
- Configure OSPF over IPsec
- Configure ECMP with OSPF routes
- Fine-tune OSPF for faster failover
- Use BFD for OSPF
- Monitor the status of an OSPF network

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating a competent understanding of OSPF, you will be able to configure OSPF from FortiManager and understand the advanced features that are available.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

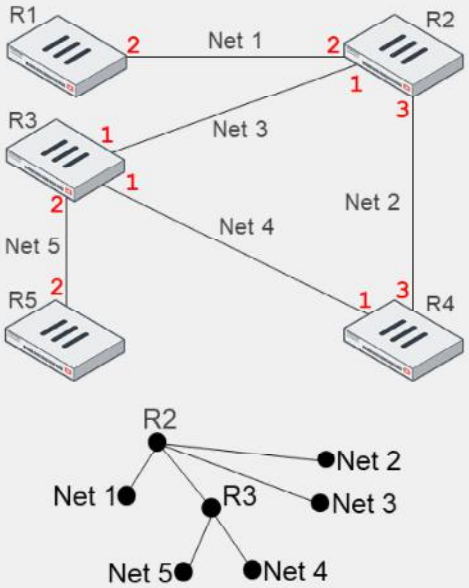
In this section, you will learn about OSPF routing protocol.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Overview

- Link state protocol, each router maintains identical databases describing the network topology
- It uses Dijkstra's algorithm, each router builds a tree with the shortest paths
- The tree gives an OSPF route to each destination
- Advantages:
  - Scalable to large networks
  - Faster convergence than distance-vector routing protocols
  - Relatively quiet during steady-state conditions
    - Periodic refresh every 30 minutes
    - Otherwise, updates only sent when there are changes
- Disadvantages:
  - May require planning and tuning to optimize performance
  - May be difficult to troubleshoot in large networks



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

Each router in the same area has identical and synchronized databases. An OSPF router uses the information in the link state database (LSDB) and Dijkstra's algorithm to determine the best route to each destination. The best routes can be represented as a tree with the local router at the root. Dijkstra's algorithm is a recursive process that the router repeats multiple times, until it finds the best routes. For example, this slide shows the OSPF tree for router R2. It indicates that the best route to Net 5 and Net 4 is through R3, and that Net 1, Net 2, and Net 3 are locally connected.

In a link state protocol like OSPF, every router has a complete view of the network topology. Advantages of OSPF include scalability and fast convergence. Every 30 minutes, routers readvertise their OSPF information. Between those 30-minute intervals, updates are sent when a topology change is detected. So, it is a relatively quiet protocol, as long as the network topology is stable. In large networks, using OSPF requires good planning and may be difficult to troubleshoot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Network Types

- Point-to-point
  - A pair of routers connected through a point-to-point link
- Broadcast (multi-access)
  - Supports more than two attached routers
  - Supports the sending of a single message to all routers (multicast)
  - Example: Ethernet networks
- Point-to-multipoint
  - Supports more than two attached routers
  - Does not support multicast

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

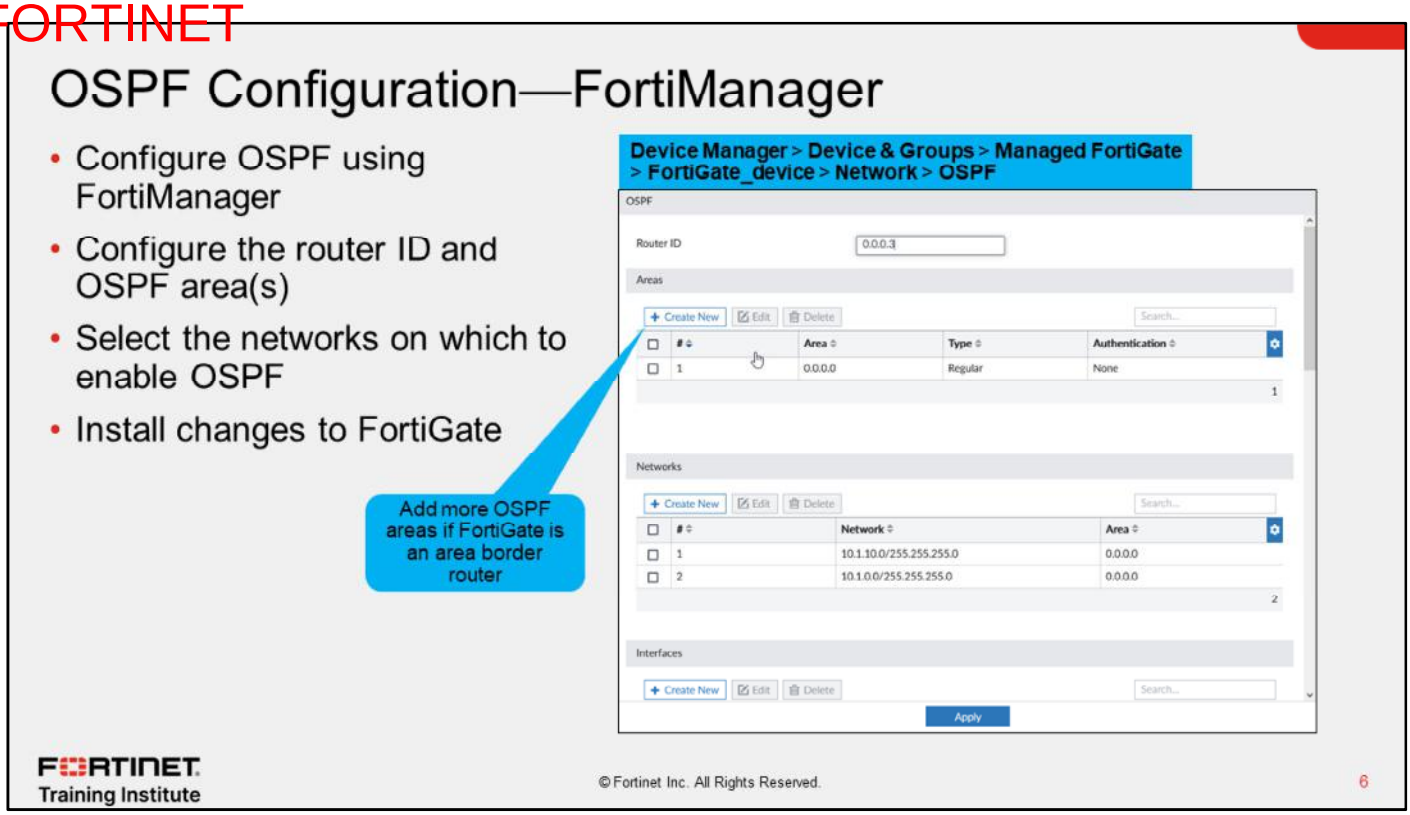
5

There are three types of OSPF networks:

- Point-to-point networks contain only two peers, one at each end of a point-to-point link.
- Broadcast networks support more than two attached routers. They also support sending messages to multiple recipients (broadcasting).
- Point-to-multipoint networks support more than two attached routers, but they do not support broadcasting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can configure OSPF directly on FortiGate if it is standalone or using FortiManager if it is managing FortiGate. The basic settings to enable OSPF on FortiGate are to set the router ID and OSPF areas FortiGate connected to.

You also configure networks and interfaces as part of the basic OSPF settings. When completing the configuration, you must push the changes to the managed FortiGate by installing the device settings level. If you want to make other changes to the policy package of the managed device, you can change both the policy package and device settings at the same time.

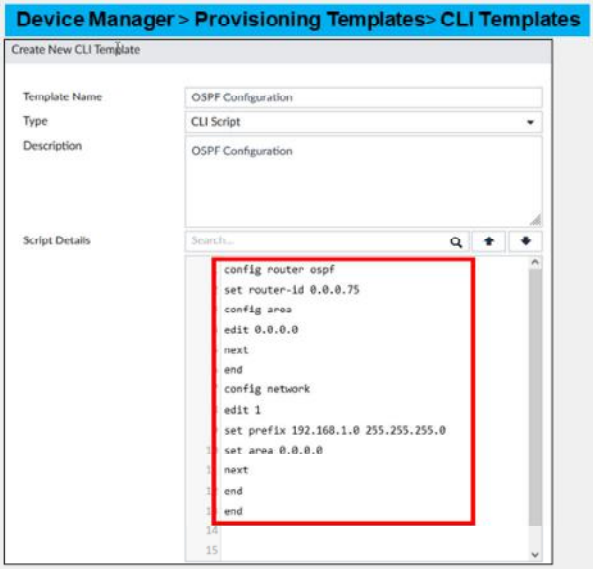
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Configuration—FortiManager CLI Templates

- Basic CLI commands to enable OSPF
- Can use the CLI commands to create CLI template on FortiManager

```
config router ospf
    set router-id 0.0.0.75
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
            set area 0.0.0.0
        next
    end
    ...
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

This slide shows a basic FortiGate OSPF configuration. It has the list of areas, the list of OSPF networks, and the OSPF router ID.

You can create a CLI template and assign it to FortiGate. This type of CLI template is referred to as post-run, which means it is suitable for FortiGate devices that have been already provisioned and managed by FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Routes Filtering and Protocol Redistribution

- Routes filtering work on OSPF routers of two or more areas
- There are three route filtering rules on OSPF:
  1. Access lists
  2. Prefix lists
  3. Route maps
- OSPF routers with one OSPF area can use redistribution control
  - Provides control on other routing protocols
  - By default, is not enabled in OSPF settings

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

You can filter routes on OSPF when FortiGate is configured to be part of two or more different OSPF areas. There are three route filtering rules available on OSPF:

1. Access lists
2. Prefix lists
3. Route maps

The route filtering methods help to control or prevent advertising routes from one OSPF area to another OSPF area. This is possible on area border routers (ABR) and is configured using the CLI within each OSPF area segment.

For routers that are only part of one OSPF area, you can filter routes using redistribution settings of the other routing protocols. By default, the setting is disabled on all of the routing protocols within OSPF router settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access lists

- Use route maps to filter routes based on a prefix
- Apply access lists in OSPF to prevent routes from being injected in the routing table

```
config router access-list
    edit "ROUTES"
        config rule
            edit 1
                set action {permit | deny}
                set prefix <IPv4_address>
                set wildcard <wildcard_filter>
                set exact-match {enable | disable}
            next
        end
    next
end
```

```
config router ospf
    set distribute-list-in "ROUTES"
    config distribute-list
        edit <id>
            set access-list "ROUTES"
            set protocol {connected | static | rip}
        next
    end
end
```

The access list act to prevent injecting routes in the routing table

The access list act to prevent injecting routes in the routing table

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Access lists are used to filter routes based on the prefix of an IP address and a netmask. It is used to act as a filter to prevent a certain route injected into the routing table. Another use case for access lists in OSPF is to filter routes that are being distributed from other routing protocols such as directly connected routes, static routes, or RIP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Prefix Lists

- Similar to access lists with additional logical operator settings
- Apply prefix lists to prevent injecting routes that use condition parameters on the prefix

```
config router prefix-list
    edit "ROUTES"
        config rule
            edit 1
                set action deny
                set prefix 10.1.0.0 255.255.0.0
                set ge 16
                set le 24
            next
            edit 1
                set action permit
                set prefix any
                set ge <integer>
                set le <integer>
            next
        end
    next
end
```

```
config router ospf
    set distribute-list-in "ROUTES"
end
```

ge and le are integer values set to match routers consisting of the prefix

Setting the prefix list prevents certain routes from injecting in the routing table

The action associated with the prefix list rule reflects in OSPF distribute-list-in setting

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

A prefix list is a filtering method, similar to an access list, with additional parameters to configure, such as setting conditions with the rule action. The conditions can be whether the prefix length of the matched object is greater or equal (`ge`) to the given route, or less than or equal (`le`) the given route. The example above shows that OSPF will drop networks between `10.1.0.0/16` and `10.1.0.0/24`, and allow the rest.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Route Maps

- Use route maps to filter external routes
- Configure route map to redistribute other routing protocols

```
config router route-map
    edit "ROUTES"
        config rule
            edit 1
                set action {permit | deny}
                set match-ip-address <prefix-list>
                set match-ip-nexthop <string>
            next
        end
    next
end
```

Assign a prefix list to the rule to process and match routes

```
config router ospf
    set default-information-route-map "ROUTES"
    set distribute-route-map-in "ROUTES"
    config redistribute <ROUTING_PROTOCOL>
        set routemap "ROUTES"
    end
end
```

Set the route map rules to redistribute other routing protocols routes

Enter the route map to filter incoming external routes

Specify the route map rules to apply to control OSPF advertising default routes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

Route maps in OSPF are used to apply conditional rules on default OSPF routes, filtering external routes, or matching specific routes for redistributing from other routing protocols. Route map rules reference prefix list objects to process and match routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Over IPsec

- Protect OSPF using IPsec VPN tunnels
- Two implementations:
  1. Site-to-site IPsec
  2. Dial-up IPsec (hub and spoke)
- OSPF over site-to-site:
  - Route-based IPsec VPN phase1 and phase2 are required
  - IPsec VPN interfaces must have tunnel-end IP address
  - Require static routes to each FortiGate device
  - VPN subnets must be part of OSPF networks configuration
  - IPsec interfaces must define as OSPF interfaces
- OSPF over dial-up:
  - Hub must have IPv4 range configured on IPsec phase1
  - OSPF on hub must redistribute static and connected routes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

OSPF can be protected using IPsec VPN tunnels. The two most commonly used implementations of OSPF over IPsec VPN are:

- Site-to-site
- Dial-up

Site-to-site OSPF requires route-based IPsec VPN tunnels with complete phase1 and phase2 configuration. On both FortiGate devices, the phase1 configuration must have tunnel-end IP addresses assigned on tunnel interfaces. OSPF must be defined on the VPN tunnel interfaces as part of OSPF interface configuration. You will need static routes on each FortiGate pointing to the other FortiGate connected on the VPN tunnel.

In a hub and spoke implementation, OSPF over dial-up uses the generic VPN setup for FortiGate as a dial-up client. The hub must have an IPv4 range specified in the VPN phase1 configuration to ensure that spokes are assigned an IP address. The hub also must have OSPF redistributing other routing protocols, especially static and directly connected routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF ECMP

- OSPF ECMP allows FortiGate to install external routes of the same cost, into the routing database
- By default, ECMP is disabled and must be enabled using `rfc1583-compatible` in OSPF settings

```
config router ospf
    set rfc1583-compatible enable
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

Equal cost multiple path (ECMP) allows multiple routes to the same destination with different next-hops and load balanced routed traffic over the next hop. OSPF ECMP, when enabled, installs the external routes of the same cost in the routing table, even if the cost is equal.

The default setting on OSPF ECMP is disabled. You can enable ECMP in OSPF settings on the CLI by setting `rfc1583-compatible` to `enable`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Graceful Restart Mode

- Ideal for FortiGate HA clusters
- Router sends grace LSAs before restart
- Neighbors receive the grace LSA
  - Enter into helper mode
  - Act as no changes on the restarting router
- Communication resumes after 120 seconds, by default
- Routers configured with graceful mode will not exit graceful mode in the case of a network topology change

```
config router ospf
    set restart-mode graceful-restart
    set restart-period 120
    set restart-on-topology-change [enable|disable]
    end
end
```

If set to enable, the router will not exit graceful restart mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

OSPF can run smoothly when FortiGate is part of a high availability (HA) cluster using graceful restart mode. Graceful restart mode helps you avoid traffic interruption if the router goes offline. In an HA cluster with OSPF graceful restart mode enabled, the primary FortiGate fails over operation to the backup FortiGate. The action sets the router to send a grace LSA. When the neighbors receive it, they then enter into helper mode to prevent the OSPF status of the router from being updated. By default, the neighbors wait 120 seconds before restarting communication again with the restarting router.

The `restart-on-topology-change` setting gives the restarting router the option to remain in a graceful restart mode, if there is a change in the network topology. If you want the router to exit graceful restart mode, you will need to disable this setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BFD in OSPF

- Co-exists with other dynamic routing protocols, such as OSPF
- Is used to quickly detect hardware failures in OSPF neighbors
- Must be configured on all OSPF routers to fully function
- Must be enabled on the OSPF global setting as well as OSPF interfaces

```
config router ospf
    set bfd enable
end
end
```

```
config system interface
    edit "port3"
        set bfd enable
    next
end
```

```
NGFW # get router info bfd neighbor

OurAddress      NeighAddress    State    Interface    LDesc/RDesc
10.1.0.254      10.1.0.1        UP       port3        2/2
10.1.0.254      10.1.0.100      UP       port3        1/2
```

OSPF global and the physical interface BFD setting must be enabled to ensure correct operation

Neighbors that have BFD enabled and are reachable show with state UP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

For faster convergence, the Bidirectional Forwarding Detection (BFD) protocol helps OSPF to quickly detect hardware failure in OSPF neighbors. Routers running BFD send packets to each other using the protocol standards timers to keep communication ongoing. If one of the routers fails to receive BFD packets, meaning it does not continue the communication, the router is then declared to be down. At this point, the BFD protocol informs the other routing protocol, in this case OSPF, to update its neighbor's states and declare it unreachable.

BFD must be configured globally and per physical interface. The global setting should not impact other routing protocols. These protocols can disable BFD on the routing protocol level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Status

```
# get router info ospf status
 Routing Process "ospf 0" with ID 0.0.0.2
 Process uptime is 2 hours 32 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Do not support Restarting
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 1. Checksum 0x00533A
 Number of opaque AS LSA 0. Checksum 0x000000
...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

The command shown on this slide provides detailed information about the OSPF process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Status (Contd)

```
....
Number of non-default external LSA 1
 External LSA database is unlimited.
 Number of LSA originated 36
 Number of LSA received 13
 Number of areas attached to this router: 1
   Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 3(3)
        Number of fully adjacent neighbors in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:02:38.780 ago
        SPF algorithm executed 32 times
        Number of LSA 5. Checksum 0x028b9c
```

Shows number of fully adjacent neighbors

Backbone router

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

The command on this slide also shows information about each area the router belongs to.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Interfaces

```
Spoke1 # get router info ospf interface
wan1 is up, line protocol is up
  Internet Address 10.10.2.2/24, Area 0.0.0.0, MTU 1500
  Process ID 0, VRF 0, Router ID 0.0.0.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1

  Designated Router (ID) 0.0.0.2, Interface Address 10.10.2.2

  Backup Designated Router (ID) 0.0.0.1, Interface Address 10.10.2.1
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5

    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 8612
  Hello received 93 sent 94, DD received 6 sent 3
  LS-Req received 1 sent 1, LS-Upd received 3 sent 17
  LS-Ack received 13 sent 2, Discarded 0

wan2 is up, line protocol is up
...
```

DR: Designated router
BDR: Backup designated router
DROther: Neither DR, nor BDR

Local router is a DR

Number of adjacencies

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

For OSPF information about each interface, use the command shown on this slide. It shows:

- Network type, in this case broadcast multi-access
- If it is a DR or a BDR
- DR and BDR IDs and IP addresses
- Number of adjacencies and traffic statistics

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Neighbors

```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address       Interface
0.0.0.1           1   Full/DR         00:00:39    10.10.2.1     wan1
0.0.0.3           1   Full/DROther    00:00:37    10.10.3.2     wan2
0.0.0.10          1   Full/ -         00:00:36    172.16.1.2    ToHub
```

This represents a point-to-point network

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

The command on this slide shows a summary of the statuses of all the OSPF neighbors. For each neighbor, it displays the adjacency state and if it is a DR, a BDR, or neither (DROther). The response displays a dash after the state, if the neighbor is in a point-to-point network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF LSDB

```
Spoke1 # get router info ospf database brief

            OSPF Router with ID(0.0.0.1) (Process ID 0, VRF 0)

                        Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#     CkSum Flag Link count
0.0.0.1         0.0.0.1         283  80000006 d0ce  0012 2
0.0.0.2         0.0.0.2         1601 8000000a 7725  0021 3
0.0.0.3         0.0.0.3         1520 80000007 4133  0012 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#     CkSum Flag
10.10.2.2       0.0.0.2         143  80000002 70cb  0031
10.10.3.1       0.0.0.2         1601 80000001 8dad  0021

                AS External Link States

Link ID         ADV Router      Age  Seq#     CkSum Flag Route              Tag
172.20.121.0    0.0.0.1         693  80000002 513b  0012 E2 172.20.121.0/24 0
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

The command shown on this slide provides a summary of all the LSDB entries on FortiGate, ordered by LSA types. It shows the type 1 LSAs (router link states) first, then the type 2 (net link states).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Self-Originated LSAs

```
Spoke1 # get router info ospf database self-originate

               OSPF Router with ID(0.0.0.1) (Process ID 0, VRF 0)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#     CkSum Flag Link count
0.0.0.2         0.0.0.2         1700 8000000a 7725  0021 3

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#     CkSum Flag
10.10.2.2       0.0.0.2         243  80000002 70cb  0031
10.10.3.1       0.0.0.2         1700 80000001 8dad  0021
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

The command shown on this slide lists the LSAs that originated on the local FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LSA Details

```
Spoke1 # get router info ospf database router lsa

            OSPF Router with ID(0.0.0.1) (Process ID 0, VRF 0)

                                    Router Link States (Area 0.0.0.0)

  LS age: 572
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 : ASBR
  LS Type: router-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 0.0.0.1
  LS Seq Number: 80000006
  Checksum: 0xd0ce
  Length: 48
   Number of Links: 2

    Link connected to: Stub Network
     (Link ID) Network/subnet number: 192.168.1.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metric: 1

...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Use the command shown on this slide to see details about type 1 LSAs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LSA Details (Contd)

```
 ...
Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.10.2.2
     (Link Data) Router Interface address: 10.10.2.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

  LS age: 72
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x0
  LS Type: router-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 0.0.0.2
  LS Seq Number: 8000000b
  Checksum: 0x7526
  Length: 60
   Number of Links: 3
...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

This slide shows a sample of more output from the command `get router info ospf database router lsa`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Deploy OSPF from FortiManager using CLI templates
- ✓ Configure OSPF filter networks
- ✓ Redistribute other routes into OSPF
- ✓ Configure OSPF over IPsec
- ✓ Configure ECMP with OSPF routes
- ✓ Fine-tune OSPF for faster failover
- ✓ Use BFD for OSPF
- ✓ Monitor the status of an OSPF network

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

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

By mastering the objectives covered in this lesson, you learned about configuring OSPF from FortiManager and understand advanced features available.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

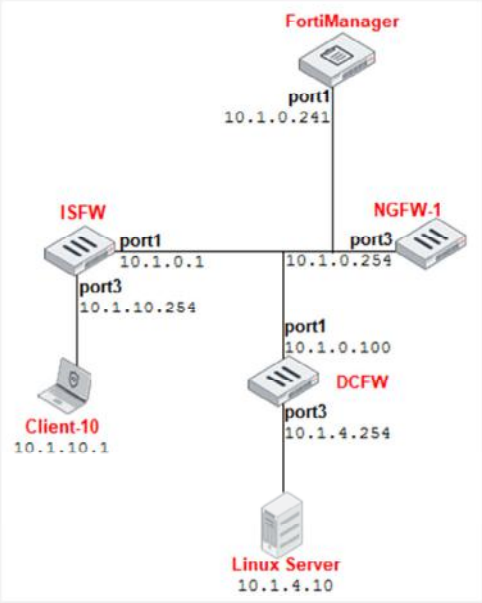
Now, you will work on *Lab 6–OSPF*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 6—OSPF

- For each FortiGate:
  - Add OSPF router ID
  - Add OSPF area
  - Add OSPF network(s)
  - Remove static routes
- For each FortiGate:
  - Configure BFD
  - Test hardware failure



FORTINET Training Institute

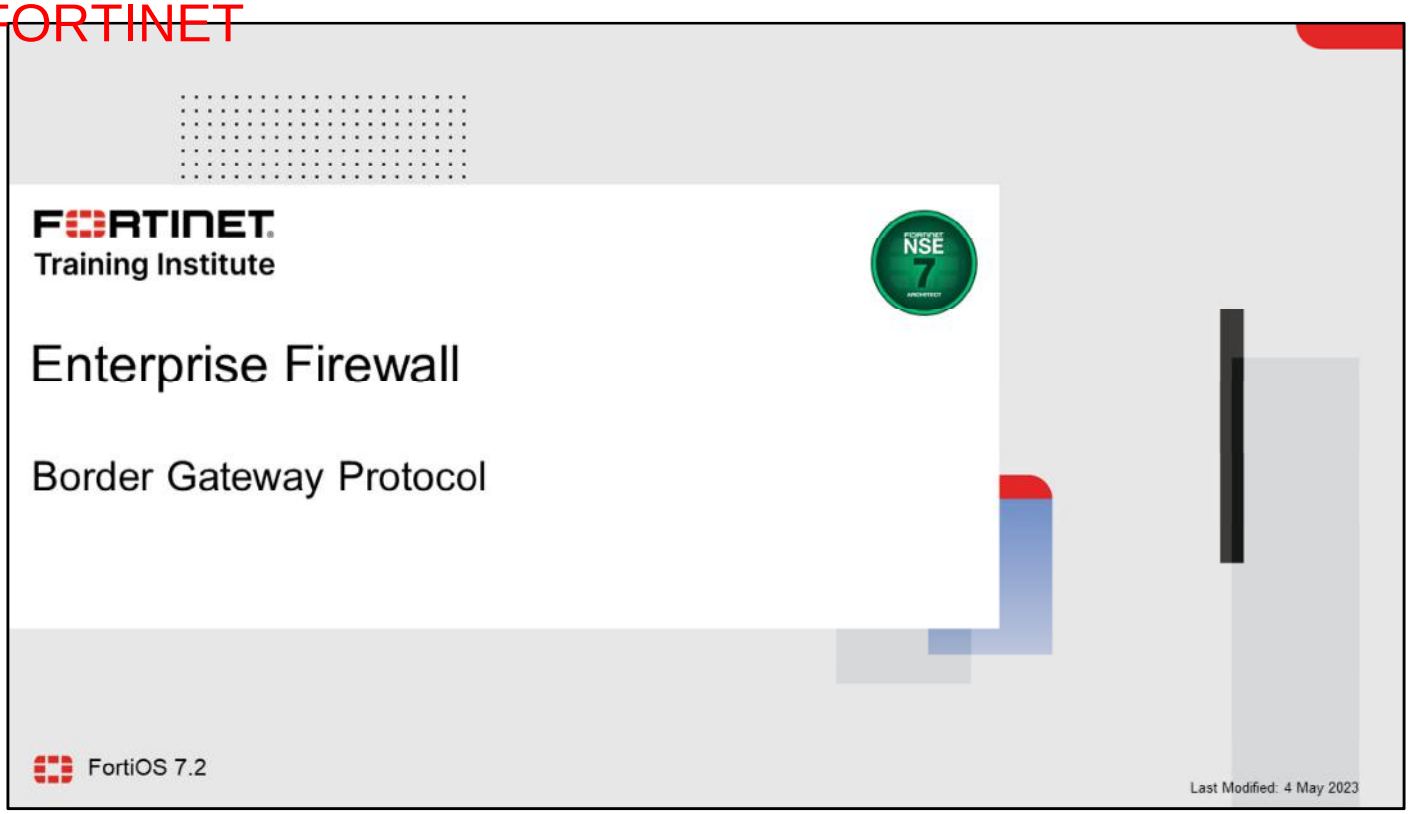
© Fortinet Inc. All Rights Reserved.

26

In this lab, you will configure FortiGate devices using FortiManager to use OSPF as the dynamic routing protocol for the enterprise network. You will configure BFD routing to support OSPF to detect failures.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about Border Gateway Protocol (BGP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Objectives

- Configure BGP on FortiGate using FortiManager
- Redistribute other routes into BGP
- Filter networks with BGP
- Improve BGP convergence with BFD
- Configure ECMP with BGP routes
- Terminate BGP on a loopback interface
- Use the neighbor-group and neighbor-range commands to deploy more scalable networks

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

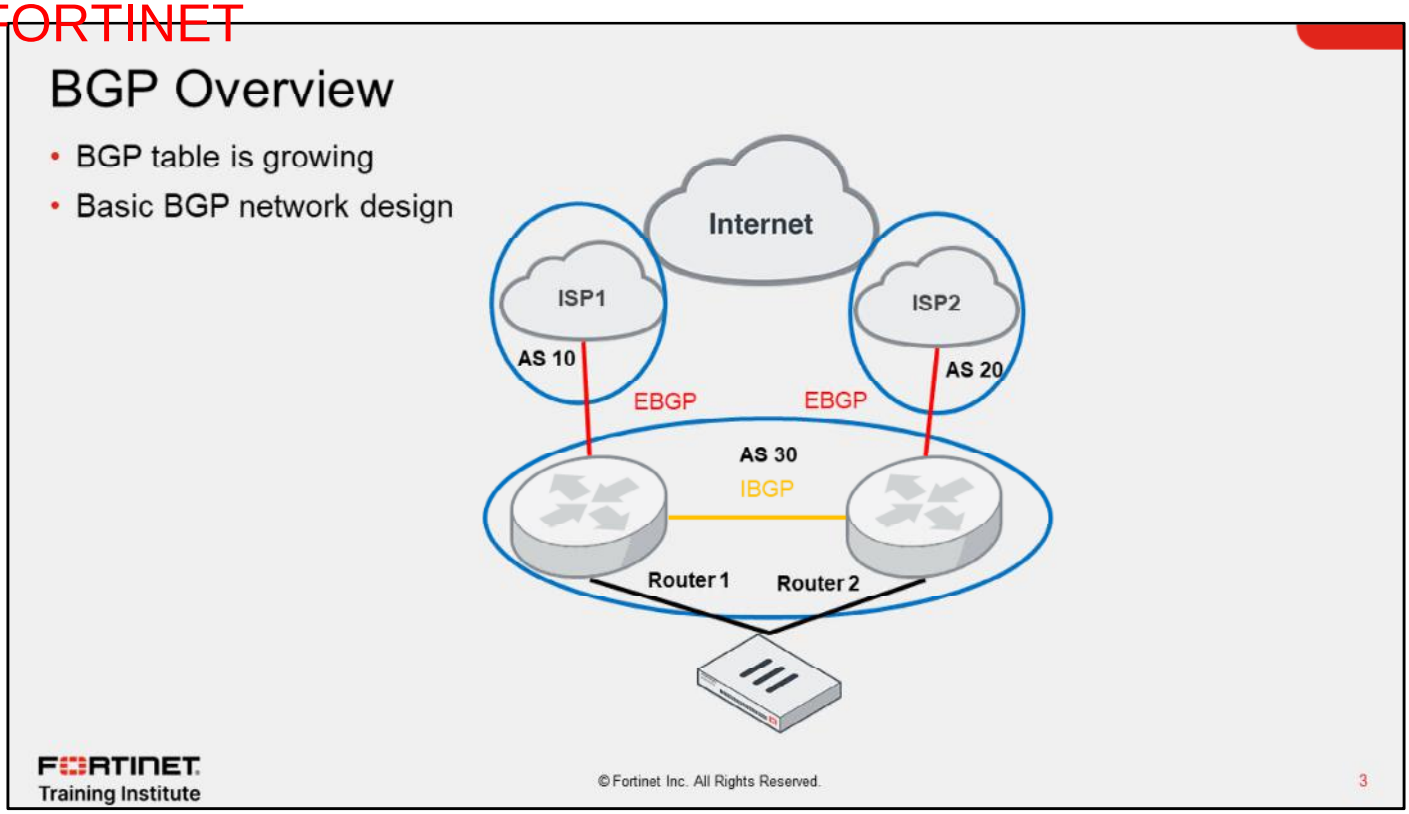
2

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

By demonstrating competence in BGP, you will be able to configure FortiGate for BGP using FortiManager, handle advanced BGP features, and apply them to use cases.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

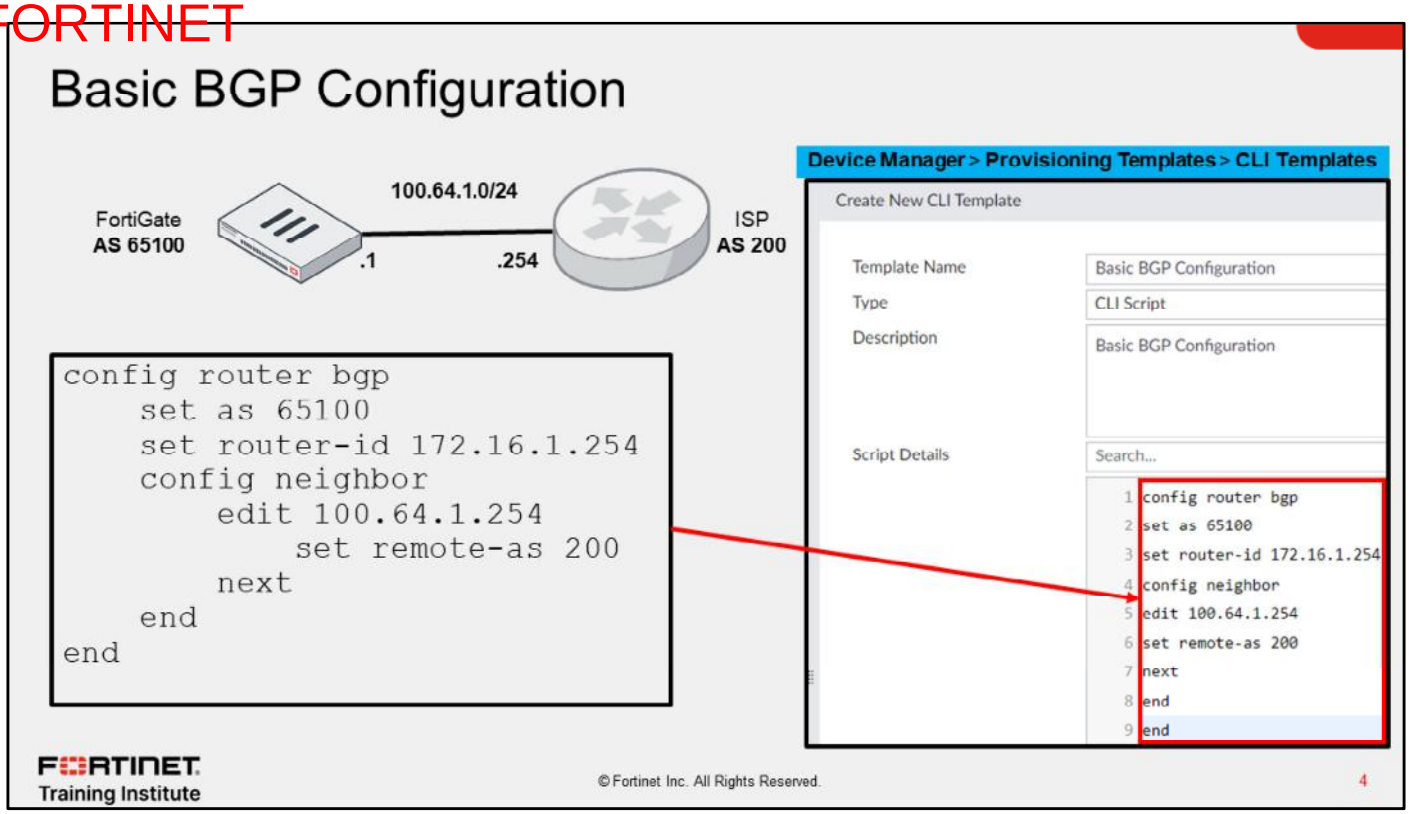


BGP is the protocol underlying the global routing system of the internet. BGP is therefore widely and increasingly used to exchange routing and reachability information.

BGP uses autonomous systems (AS) as shown in the basic design on this slide. Routers 1 and 2 are in the same AS and advertise routes that follow IBGP. They are connected to ISP1 and ISP2, which are on different ASs. They therefore establish a connection and advertise routes through EBGP.

Vouchers & Dumps are Available | WhatsApp +201224560923

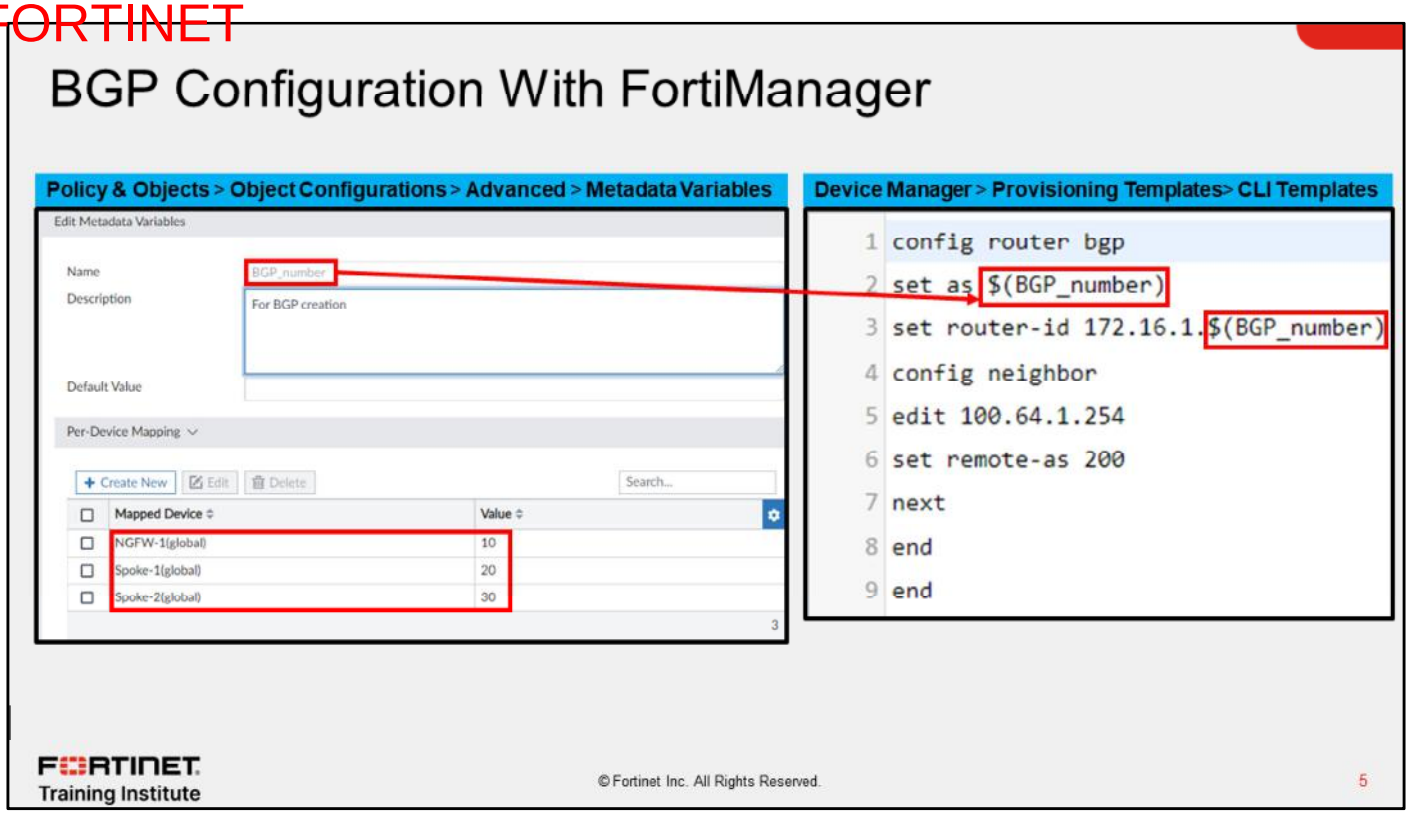
DO NOT REPRINT Brave-dumps.com
© FORTINET



In the basic network diagram shown on this slide, FortiGate is connected to an ISP, and they are in different ASs. Therefore, you must create an EBGP configuration. You can use the CLI configuration shown on this slide, or you can use the **CLI Templates** options on the FortiManager GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



On the FortiManager GUI, you can use the **Metadata Variables** option to help configure a large BGP environment. For example, in the configuration shown on this slide, a metadata variable allows you to implement the same CLI template on different FortiGate devices in the same AS. FortiManager automatically configures the AS number and the last byte of the `router-id` individually according to the metadata variable mapped to each device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Protocol Redistribution

- A non-BGP route can be redistributed into BGP

```
config router bgp
    config redistribute static
    set status enable
    end
end
```

- By default, FortiGate BGP doesn't advertise prefixes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

By default, FortiGate BGP doesn't advertise prefixes. You can use the redistribution command to configure FortiGate to advertise prefixes. You can redistribute connected and static routes, and routes learned from other routing protocols, into BGP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Config Network Command

- An alternative to redistribution of protocols into BGP:

```
config router bgp
 config network
   edit <id>
     set prefix <prefix>
...
```

- By default, the prefix is advertised only when it matches the destination subnet of an active route in the routing table
- To globally advertise the prefix (regardless of the active routes):

```
config router bgp
     set network-import-check disable
end
```

- To advise only specific prefixes (regardless of the active routes):

```
config router bgp
 config network
   edit <id>
    set network-import-check disable
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

You can also use the `config network` command to configure FortiGate BGP to advertise prefixes. However, an exact match of the prefix in the `config network` command must be active in the routing table. If the routing table doesn't contain an active route whose destination subnet matches the prefix, FortiGate doesn't advertise the prefix. You can change this behavior by disabling the `network-import-check` setting. After you disable the setting, FortiGate advertises all prefixes in the BGP network table, regardless of the active routes present in the routing table. If you disable the setting in `config network`, only the corresponding prefixes are advertised in the BGP network table, regardless of the active routes present in the routing table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Routing Information Bases

- Routes are stored in the routing information bases (RIBs)
  - RIB-in:
    - Routing information learned from inbound update messages
    - Contains unprocessed routing information advertised to the local BGP speaker by its peers
  - Local RIB:
    - Routing information that the BGP speaker has selected after applying its local policies to the RIB-in
  - RIB-out:
    - Routing information that the local BGP speaker has selected to advertise to its peers

FORTINET Training Institute

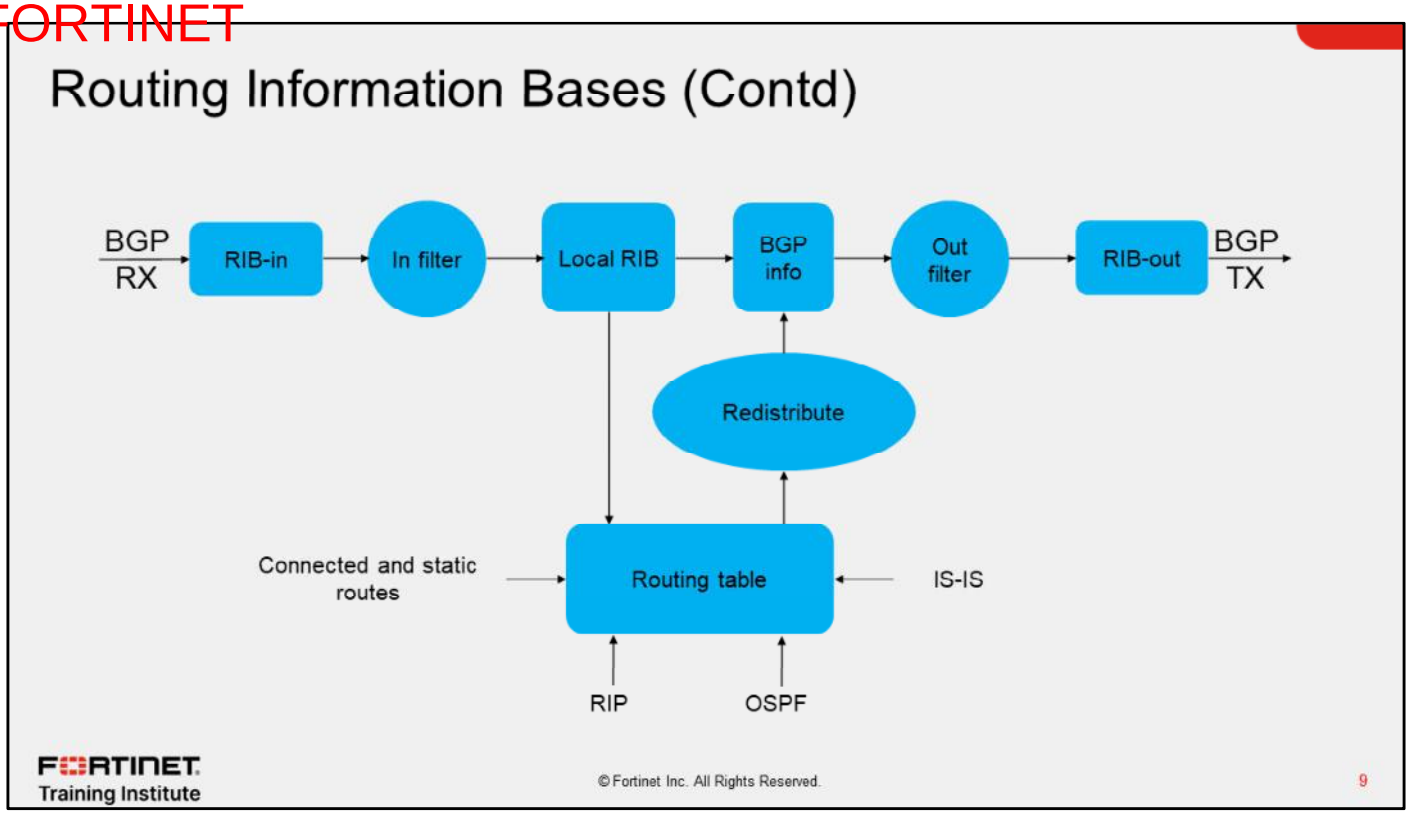
© Fortinet Inc. All Rights Reserved.

8

Once the BGP peering is established, a BGP router stores the routing information in three logical tables specific to BGP. The RIB-in table contains all the routing information received from other BGP routers before any filtering. The local RIB table contains that same information after the filtering. The RIB-out table contains the BGP routing information selected to advertise to other BGP routers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows a flowchart that summarizes the BGP process. The BGP router stores the BGP routes it receives from other routers in the RIB-in table. The BGP router applies a filter, and the resulting routes are stored in the local RIB table. Then, the BGP router adds routes that were redistributed from the routing table and applies another filter (outbound). The BGP router advertises the resulting routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Filtering With the access-list Command

- Access lists filter based on prefix consisting of an IP address and netmask

```
config router access-list
   edit filter-subnets
      config rule
         edit 1
           set prefix 10.1.0.0/16
           set action deny
         next
         edit 2
           set prefix 10.0.0.0/8
           set action permit
         next
      end
   end
end
```

```
config router bgp
  config neighbor
    edit 100.64.1.254
      set distribute-list-in filter-subnets
    next
  end
end
```

By default, traffic not matching the prefix list will not be learned (or advertised)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

By default, the subnets under the `config network` command, and the subnets redistributed from other routing protocols, are advertised to all the neighbors.

With an access list, you can be more selective about which prefixes to advertise to each neighbor. Additionally, access lists allow you to select which prefixes you want to use from each neighbor. This example shows an access list that allows the prefix `10.0.0.0/8`, but blocks the prefix `10.1.0.0/16`. By default, all the traffic that does not match a prefix list is denied. The access list is applied in the incoming direction from the neighbor `100.64.1.254`. The local FortiGate applies this filter for all the prefix advertisements coming from `100.64.1.254`.

When applying an access list, any prefixes that don't match an entry in the list are not learned or advertised by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Filtering With the prefix-list Command

- Prefix lists can be used to filter out the subnets being advertised to and being received from each neighbor

```
config router prefix-list
   edit filter-subnets
      config rule
         edit 1
           set prefix 10.1.0.0/16
           set action deny
         next
         edit 2
           set prefix 10.0.0.0/8
           set action permit
           set ge 16
         next
      end
   end
end
```

```
config router bgp
  config neighbor
    edit 100.64.1.254
      set prefix-list-in filter-subnets
    next
  end
end
```

ge (and le) parameters provide additional granularity on prefix matching

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

Similar to access lists, prefix lists are simple lists used for filtering routes based on a prefix consisting of an IP address and netmask. Additionally, prefix lists have settings to specify the minimum (`ge`) and the maximum (`le`) prefix length to be matched. For example, in the configuration shown on this slide, the prefix of `10.0.0.0/8` with a `ge` of `16` will match anything in the 10.0.0.0/8 network with /16 or above, meaning 10.10.0.0/16 will match, and 10.10.0.0/12 will not match.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Filtering With the route-map Command

- A route map is composed of rules
- The rules are processed from top to bottom until a match, if any, is found
- The action is applied to a neighbor for advertised or received prefixes

```
config router route-map
  edit change-weight
    config rule
      edit 1
       set match-origin igp
       set set-weight 40000
      next
    end
  next
end
```

```
config router bgp
  config neighbor
    edit 100.64.1.254
      set route-map-in change-weight
    next
  end
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

Besides filtering, FortiGate can modify parameters when advertising or receiving prefixes from a neighbor with the `route-map` command.

For example, in the configuration shown in this slide, the `route-map` command changes the weight value for IBGP routes received from a BGP neighbor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Filtering With the route-map Command (Contd)

- You can use the `route-map` command to combine access lists and prefix lists

```
config router access-list
  edit lan
    config rule
      edit 1
       set prefix 10.1.0.0 255.255.255.0
       set exact-match enable
      next
    end
  next
end
```

```
config router route-map
  edit set-tag
    config rule
      edit 1
       set match-ip-address lan
       set set-route-tag 10
      next
    end
  next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

The `route-map` command is more powerful than access lists and prefix lists, as it can even combine them with the commands `match-ip-address` and `match-ip-nexthop`, available with the `config rule command`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BGP Convergence

- BGP convergence includes multiple steps:
  - Installing a new path in the routing and forwarding tables
  - Processing and finding an alternate path
  - Fast failure detection and information propagation
- Each step has available tuning including:
  - Adding in and out filters to reduce the RIB size
  - Implementing route reflectors in IBGP
  - Fine tuning BGP keepalive timers or enabling BFD

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

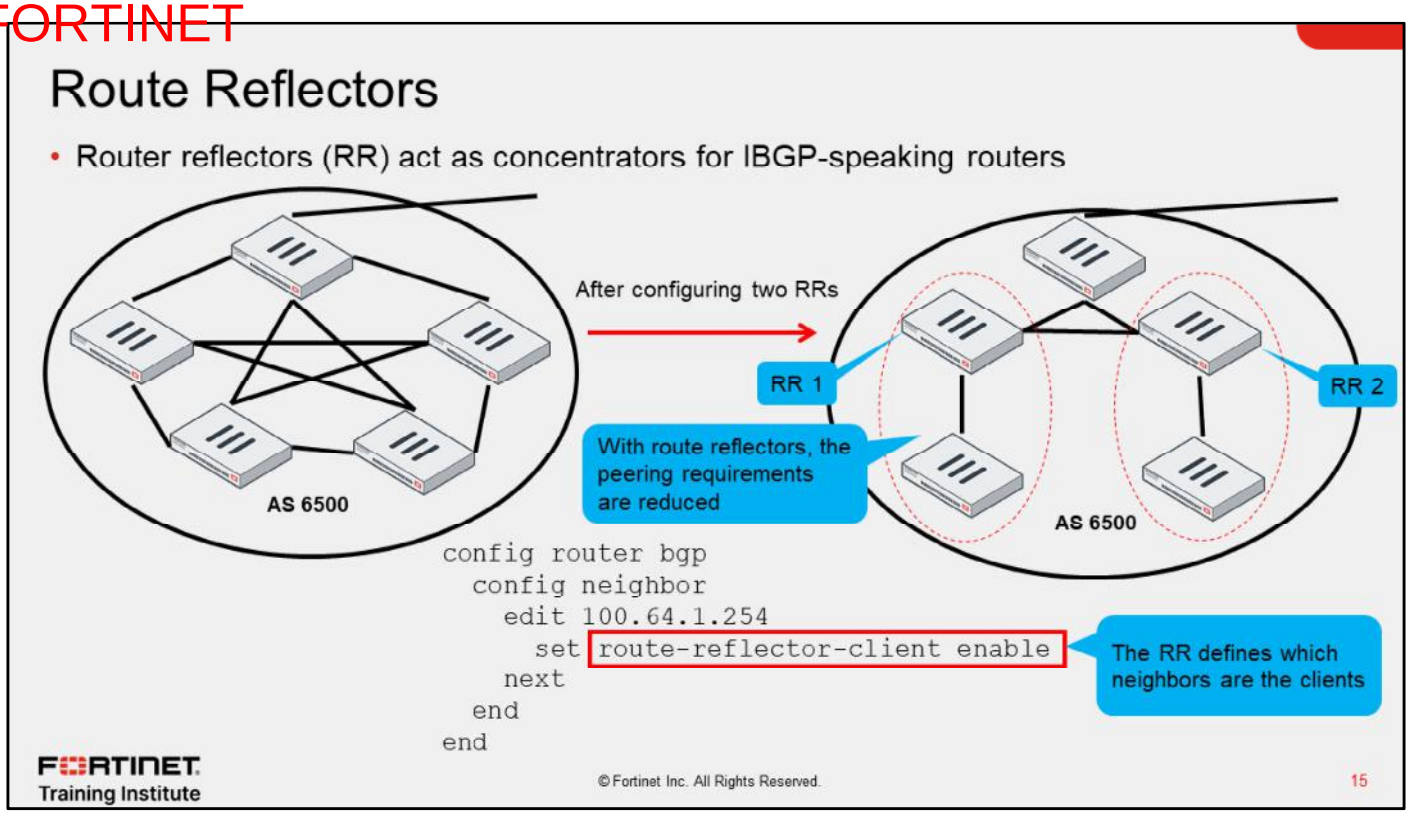
14

BGP is a distance vector protocol, which sends its entire routing table to directly connected neighbors. This routing table is regularly updated depending on new routing paths or failure detection. You can modify the timing of the update using parameters like the size of the RIB, the number of hops multiplied by the advertisement interval for each of them, and the delay involved in failure detection.

To improve BGP convergence, you must have a stable network, without port flapping, which creates BGP update messages that require RIB processing, adding to the CPU load. You can reduce RIB size using filters. In IBGP, you can implement route reflectors to concentrate the updates and avoid a full mesh between all BGP-speaking routers. For faster failure detection, you can reduce the BGP keepalive timers or enable bidirectional forwarding detection (BFD), as explained in the next slides.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When running IBGP, you usually need to configure full mesh peering between all the routers. In large networks, full mesh peering between routers can be difficult to administer and is not scalable.

RRs help to reduce the number of IBGP sessions inside an AS. An RR forwards the routes learned from one peer to the other peers. If you configure RRs, you don't need to create a full mesh IBGP network. RRs pass the routing updates to other RRs and border routers within the AS, improving the BGP convergence.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BFD Parameter

- BGP has a keepalive timer configured in seconds
- Enable BFD for faster failure detection (in less than 1 second)
- Configure BFD on both connected routers
- Configure BFD for each neighbor and for multihop paths

```
config router bgp
  config neighbor
    edit 100.64.1.254
      set bfd enable
      set ebgp-enforce-multihop enable
    next
  end
end
```

```
config router bfd
  config multihop-template
    edit 1
      set src 100.64.2.0 255.255.255.0
      set dst 100.64.1.0 255.255.255.0
      set auth-mode md5
      set md5-key password
    next
  end
end
```

For BFD multihop path, the check is performed using a template

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

BFD is like a probe that checks the status of the BGP peer. It is independent of the type of media and detects a one-way device failure in less than a second, allowing faster BGP convergence. BFD was initially supported for two routers directly connected on the same subnet. Now FortiGate can also support neighbors with BFD connected over multiple hops.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

The graceful-restart Command

- Use the BGP `graceful-restart` command to prevent traffic interruption during HA failover
- The HA cluster advertises that it is going offline
- Enable the parameter on both connected routers

```
config router bgp
    set as 65100
    set graceful-restart enable
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set capability-graceful-restart enable
            set remote-as 200
        next
    end
end
```

FORTINET Training Institute

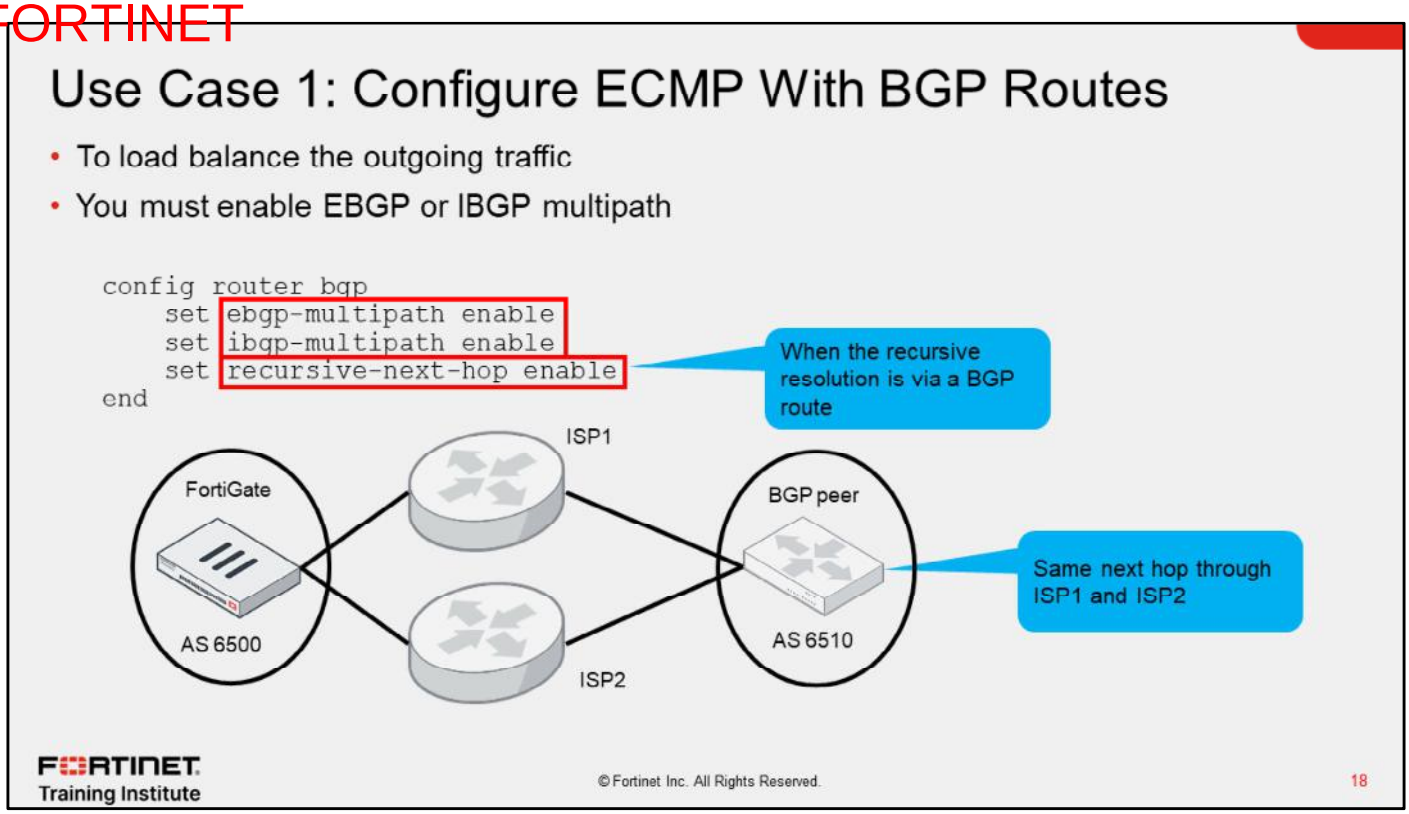
© Fortinet Inc. All Rights Reserved.

17

As the BGP router daemon process is only running on the primary unit, BGP peering needs to be reestablished upon HA failover. In a cluster, the FortiGate `graceful-restart` command allows BGP routes to remain in the routing tables. This is particularly important during a reboot or an upgrade maintenance window to avoid potential new BGP convergence and traffic interruption. In this situation, the HA cluster advertises that it is going offline, and does not appear as a route flap. It also enables the new HA main unit to come online with an updated and usable routing table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When multiple ECMP routes to a BGP next hop require recursive resolution, FortiGate can now consider all the ECMP routes for the next-hop resolution, allowing load balancing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case 2: Loopback Interfaces as BGP Source

- BGP uses loopback interfaces because they stay up, unlike physical interfaces
- For the neighbor, you must explicitly configure the loopback interface the same as the source interface
- Because the loopback interface adds one routing hop, you must enable multihop

```
config router bgp
    set as 65100
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set remote-as 65101
            set update-source Loopback_Interface
            set ebgp-enforce-multihop enable
        next
    end
end
```

Loopback interface configured in `system interface`

Multihop required as the loopback interface is not the next hop

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

In a production environment, a loopback interface as a source interface for BGP sessions is used mostly to ensure continuous BGP peering through redundant links to the same BGP peer. This allows the BGP session to work uninterrupted.

This slide shows the required FortiGate configuration in BGP:

- You must explicitly configure the loopback interface the same as the source interface in the config neighbor
- You must enable multihop because the loopback interface adds one hop

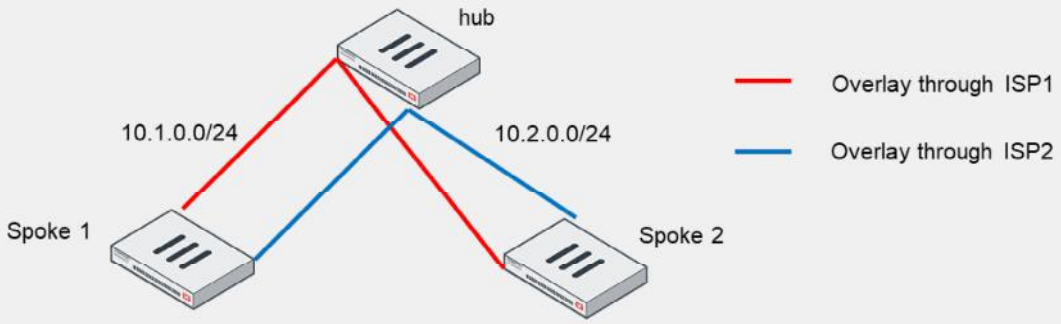
The BGP session on TCP port 179 may be traveling through a physical interface. Therefore, you must configure a corresponding firewall policy to allow the traffic between the loopback interface and the physical interface, so that the BGP connection can be established.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case 3: The neighbor-group Command

- Allows FortiGate to apply common settings in the neighbor group for each BGP peer relationship
- Is useful in SD-WAN overlay design



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

In a standard SD-WAN design, the spokes, which are the remote BGP speakers, are dial-up clients. By defining a neighbor group for overlays established over each underlay, FortiGate can apply the common settings in the neighbor group for each BGP peer relationship. You can use the `neighbor-range` command to define the IP address range that characterizes the neighbor group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Use Case 3: The neighbor-group Command (Contd)

- This use case is within the same AS, meaning IBGP

```
config router bgp
    set as 65100
    set router-id 172.16.1.254
    set ibgp-multipath enable
    config neighbor-group
        edit SpokeISP1
            set interface ISP1
            set remote-as 65100
        next
    end
end
```

```
config neighbor-range
    edit 1
    set prefix 10.1.0.0 255.255.255.0
    set neighbor-group SpokeISP1
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

This slide shows the BGP configuration on the hub.

The prefix in the neighbor range defines that peers with an IP address in the 10.1.0.0/24 subnet (the ISP1 subnet) are included in the SpokeISP1 neighbor group.

These peers will then receive the same settings configured in the SpokeISP1 neighbor group, meaning interface ISP1 and remote-as 65100.

Because this remote AS is the same as the local AS, `ibgp-multipath` is enabled to support ECMP for IBGP routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

The bgp summary Command

```
FGT # get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.64.1.254    4        100      18      20        3    0    0 00:02:55        1
100.64.2.254    4        100      18      18        3    0    0 00:02:56        1

Total number of neighbors 2
```

Remote AS

Packet count (received and sent)

How long the connection has been up

Neighbor state and prefixes received

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Use the command shown on the slide first, to get an overview of the BGP status, and the status of all its neighbors. This slide shows the local router ID and AS.

For each neighbor, the output also displays the following information:

- The AS
- Packet counters
- The length of time the neighbor has been up

The last column is the neighbor state and number of prefixes. If the state is not established, this column displays the BGP state. If the state is established, this column displays the number of prefixes received by the local FortiGate from that neighbor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

The bgp neighbors Command

```
# get router info bgp neighbors

BGP neighbor is 100.64.1.254, remote AS 100, local AS 65100, external link
  BGP version 4, remote router ID 100.64.1.254
  BGP state = Established, up for 00:49:26
  Last read 00:00:26, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  …
  Received 65 messages, 0 notifications, 0 in queue
  Sent 71 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  …
  Minimum time between advertisement runs is 30 seconds
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

As well as the `bgp summary` command, you can use the `bgp neighbor` command shown on this slide to get detailed information about each BGP neighbor. It displays information including the peer IP address, peer router ID, remote AS, BGP state, various timers, and message counters.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Configure BGP on FortiGate using FortiManager
- ✓ Redistribute other routes into BGP
- ✓ Filter networks with BGP
- ✓ Improve BGP convergence with BFD
- ✓ Configure ECMP with BGP routes
- ✓ Terminate BGP on a loopback interface
- ✓ Use the neighbor-group and neighbor-range commands to deploy more scalable networks

FORTINET Training Institute

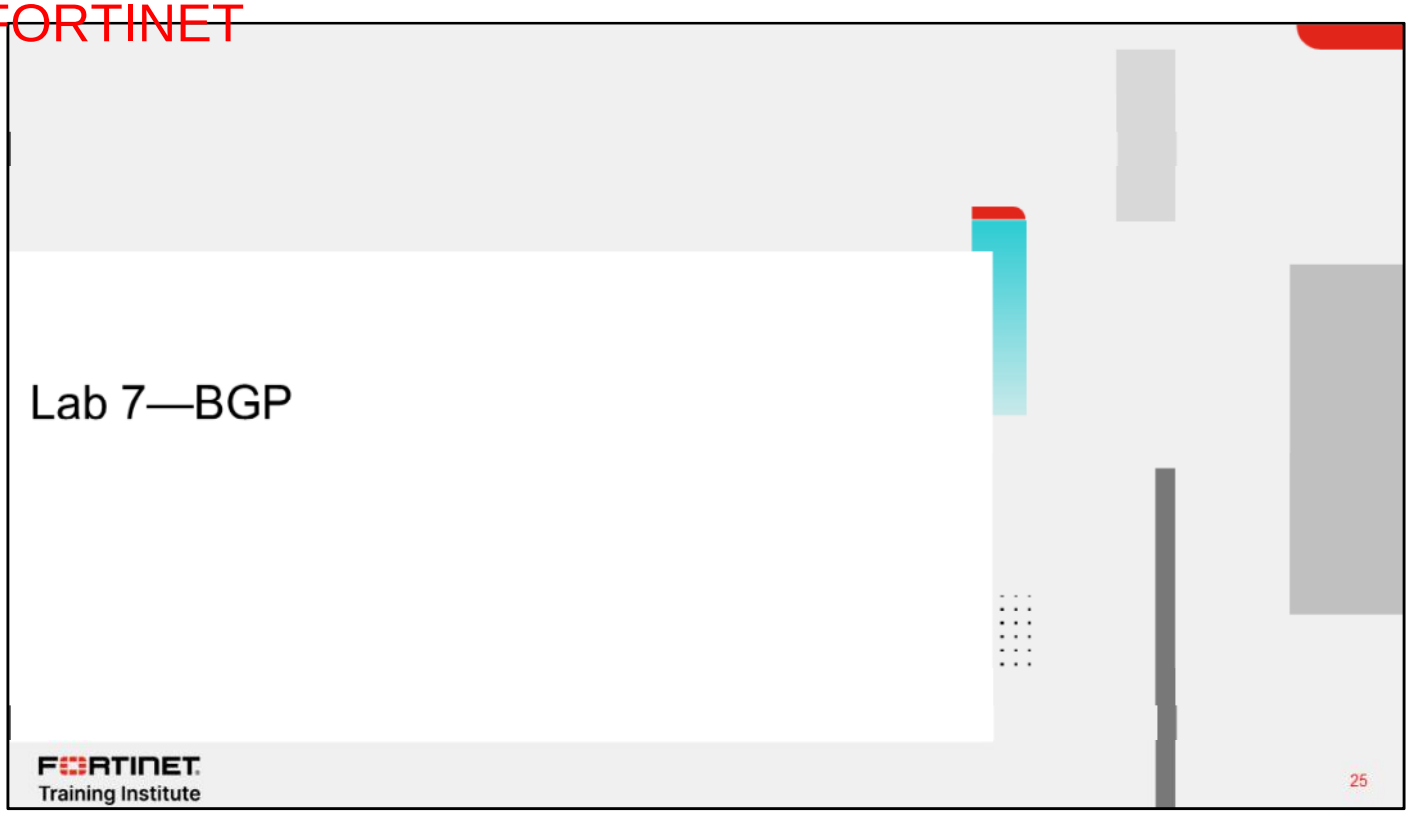
© Fortinet Inc. All Rights Reserved.

24

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

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



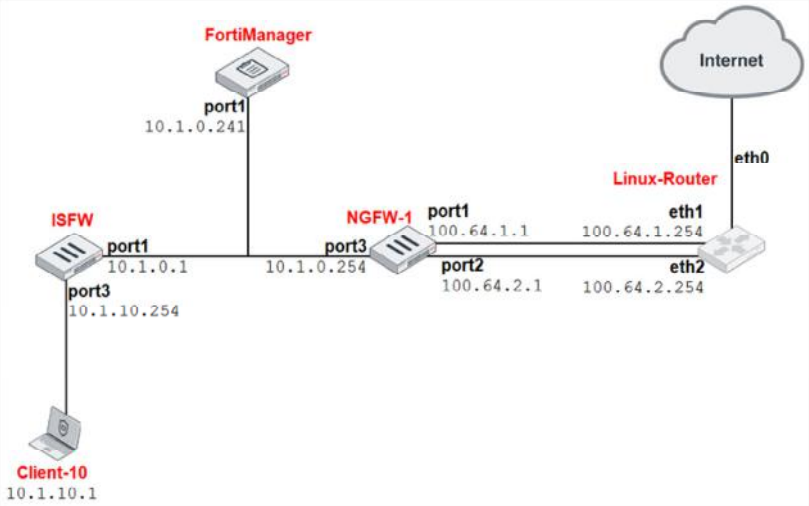
Now you will work on *Lab 7–BGP*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 7—BGP

- BGP prefix list
- Loopback interface as a BGP source



FORTINET Training Institute

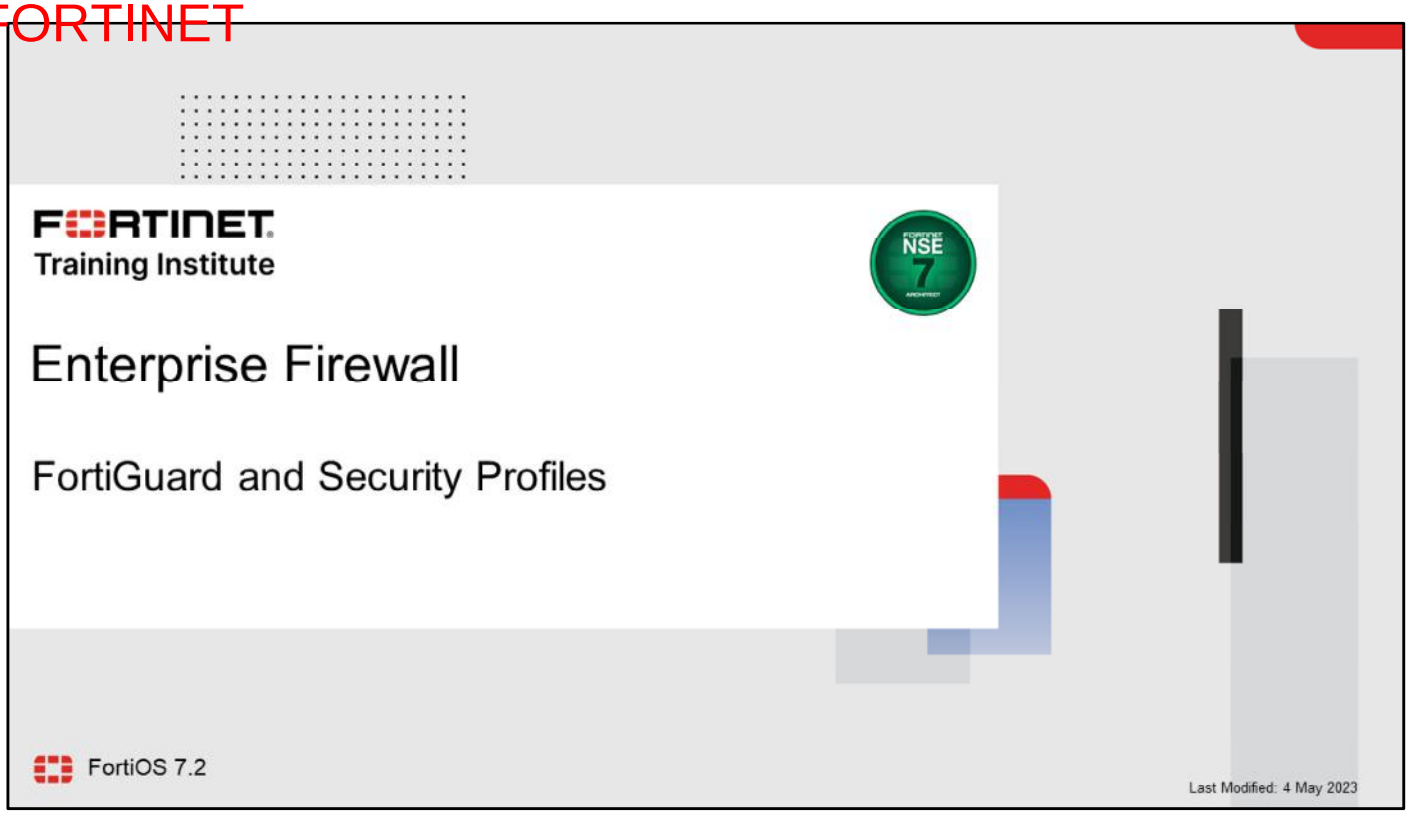
© Fortinet Inc. All Rights Reserved.

26

In this lab, you will configure BGP prefix lists and a loopback interface as a BGP source.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiGuard, web filtering, antivirus, and application control. You will also learn how FortiManager is acting as a local FortiGuard server and use with web filtering.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Monitor the status of FortiGuard updates
- Use FortiManager as a local FortiGuard server
- Test a web filter configuration
- Inspect HTTPS traffic using SSL inspection methods
- Check web filtering statistics
- Evaluate the impact on firewall performance
- Understand hardware acceleration to improve performance
- Understand NGFW modes in application control

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

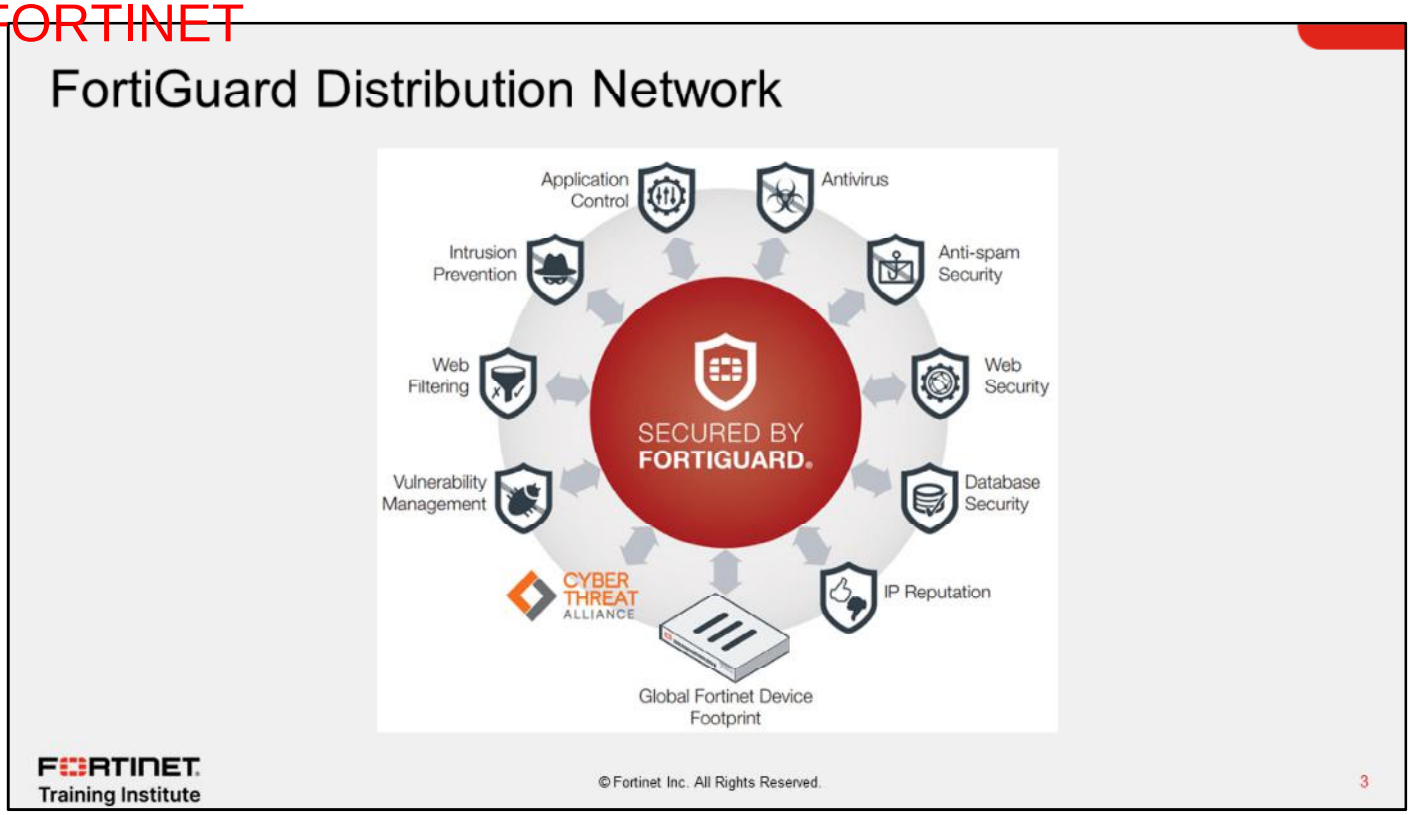
2

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

By demonstrating competence in FortiGuard, web filtering, antivirus, and application control, you will be able to implement and maintain security profiles and policies on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system, as well as its managed FortiGate devices and FortiClient agents. It provides updates and rating services for:

- Antivirus
- Intrusion prevention system (IPS)
- Web filtering
- Antispam
- Application control
- Vulnerability scanning
- IP reputation
- Web security
- Database security
- Geographic IP addresses

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGuard Ports

- Web filtering and antispam
  - When using public FortiGuard servers:
    - UDP/8888, UDP/53, HTTPS/8888, HTTPS/53, or HTTPS/443
  - When using FortiManager as a local FortiGuard server:
    - UDP/8888, UDP/53, HTTP/53, or HTTPS/8888
- Antivirus and IPS updates:
    - HTTPS/443
- To configure FortiGate to use servers worldwide, or only servers located in the USA:

```
config system fortiguard
   set update-server-location [automatic | usa | eu]
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

FortiGate uses different ports for rating services (such as web filtering and antispam) and for update services (such as antivirus and IPS).

In the case of rating services, and when communicating with public FortiGuard services, FortiGate uses one of these ports:
- UDP port 8888
- UDP port 53
- HTTPS port 8888
- HTTPS port 53
- HTTPS port 443

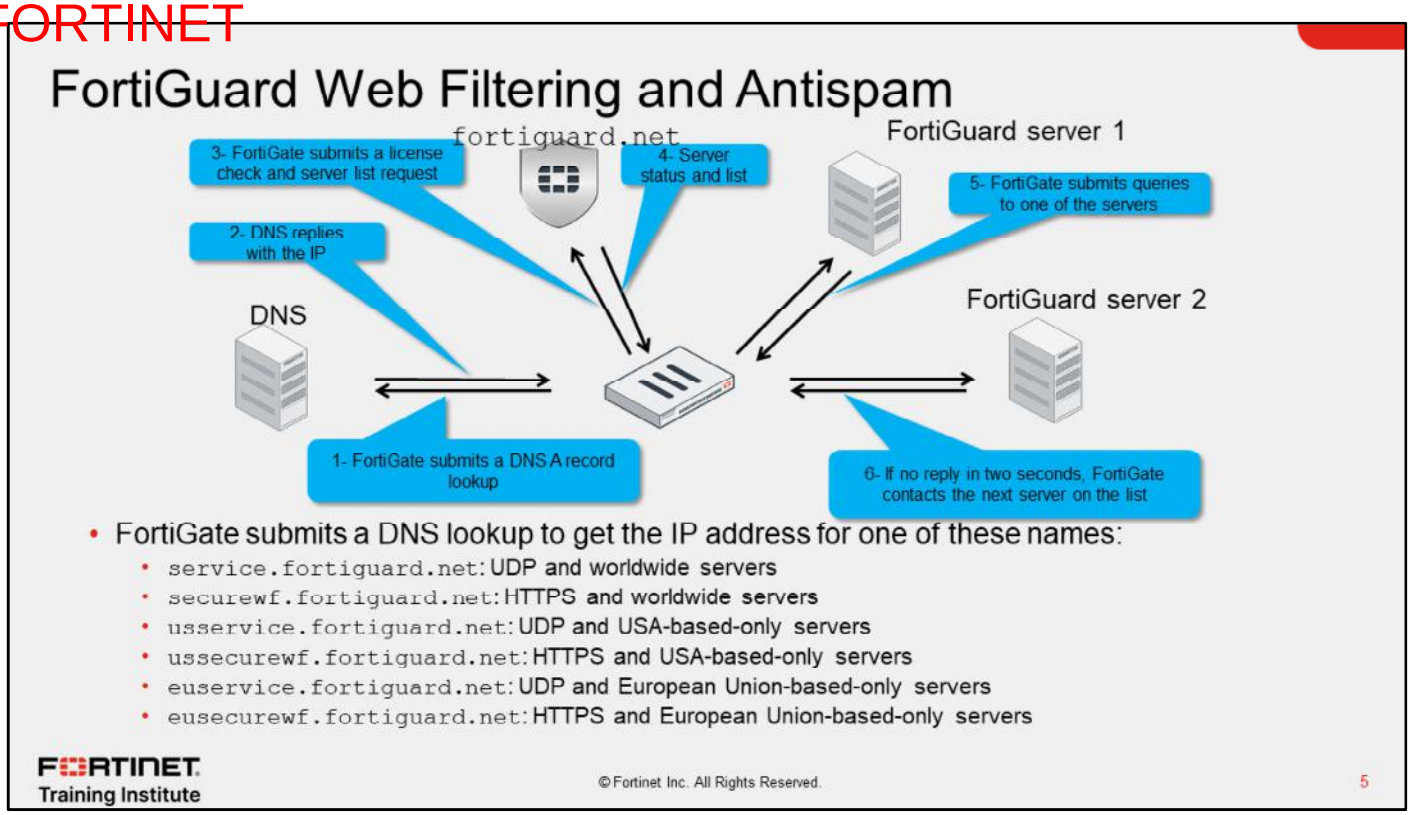
In the case of rating services, and when communicating with a FortiManager configured as a local FortiGuard server, FortiGate uses one of these ports:
- UDP port 8888
- UDP port 53
- HTTP port 8888
- HTTPS port 53

In the case of update services, FortiGate uses HTTPS port 443.

By default, FortiGuard servers location is automatic that servers chosen based on closet proximity to FortiGate device. You can configure FortiGate to use public FortiGuard servers located only in the USA or European union.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To learn how to troubleshoot FortiGuard problems, you need to understand how FortiGuard communication works. The communication between FortiGate and FortiGuard for web filtering and antispam is different from the communication for antivirus and IPS. First, you will look at how FortiGuard web filtering and antispam work:

1. FortiGate contacts the DNS server to resolve the FortiGuard service name.
2. FortiGate gets a list of IP addresses for servers (usually two or three) that can be contacted to validate the FortiGuard license.
3. FortiGate contacts one of those servers to check the license, and obtains a list of servers that can be used to submit web filtering and antispam rating queries.
4. FortiGate gets the list of servers.
5. FortiGate starts sending rating queries to one of the servers in the list. (You will learn how FortiGate chooses the server later in this lesson.)
6. If the chosen server does not reply in two seconds, FortiGate contacts the next server on the list.

The FortiGuard service name depends on the FortiGate configuration:

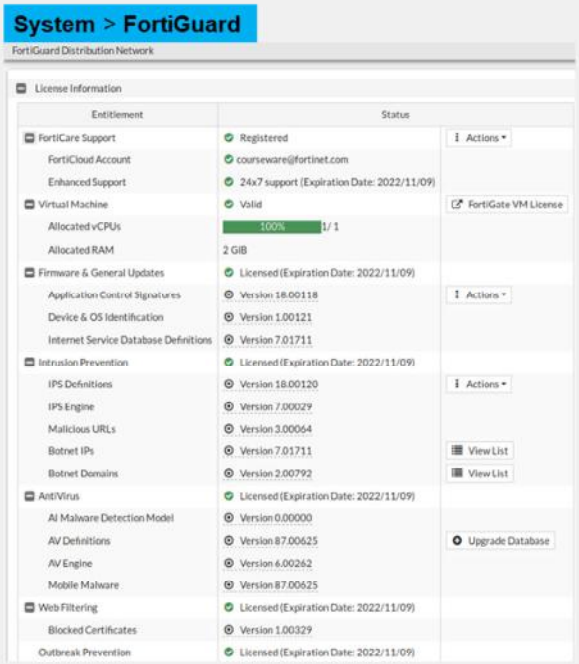
- `service.fortiguard.net`: FortiGate is configured to use UDP and communicate with servers located worldwide.
- `securewf.fortiguard.net`: FortiGate is configured to use HTTPS and communicate with servers located worldwide.
- `usservice.fortiguard.net`: FortiGate is configured to use UDP and communicate with servers located only in the USA.
- `ussecurewf.fortiguard.net`: FortiGate is configured to use HTTPS and communicate with servers located only in the USA.
- `euservice.fortiguard.net`: FortiGate is configured to use UDP and communicate with servers located only in the European Union.
- `eusecurewf.fortiguard.net`: FortiGate is configured to use HTTPS and communicate with servers located only in the European Union.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FDN Status on FortiGate

- Check FDN status on FortiGate under **FortiGuard** settings



FORTINET Training Institute

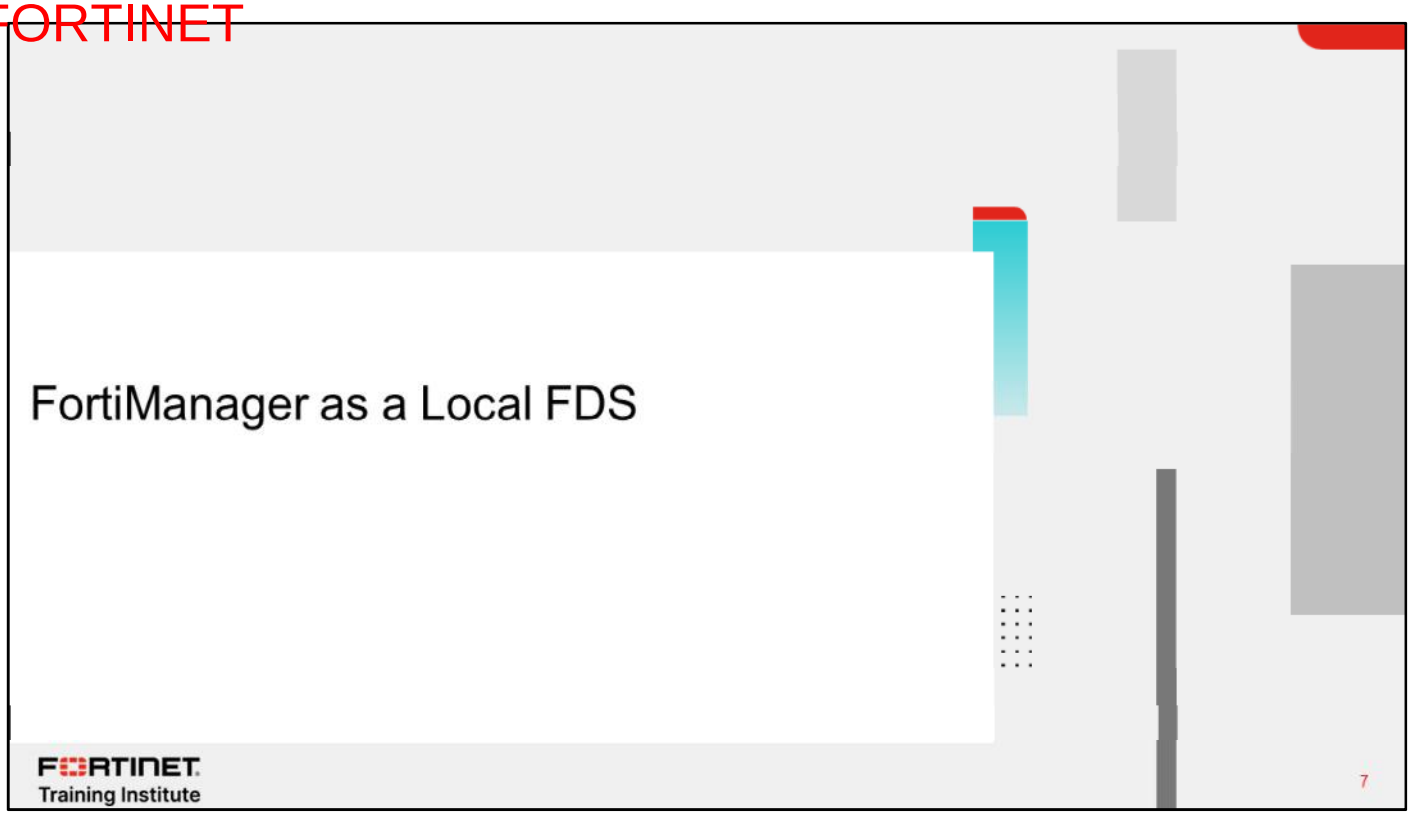
© Fortinet Inc. All Rights Reserved.

6

You can check the status of FortiGuard licenses and the communication to FortiGuard on the FortiGate GUI. You can also check the versions of the locally installed databases for each of the FortiGuard services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about FortiManager acting as a local FortiGuard distribution server (FDS).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager—Your Local FortiGuard Cache

- Periodically downloads from FortiGuard:
  - License information for registered and unregistered devices
  - FortiGuard databases (antivirus, IPS, web filtering, and so on)
- Caches available firmware updates for managed devices
- Can act as a downstream FDS, providing:
  - VM license validation services
  - Update services: antivirus, IPS engines, signatures, and so on
  - Rating services: web filtering, antispam, and so on

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

FortiManager can function as a local FDS. It continuously connects to public FDS servers to obtain managed device license information and check for firmware availability updates.

All FortiManager devices can provide antivirus, IPS, vulnerability scanning, and signature updates to supported devices. FortiManager devices can also provide web filtering and antispam rating services.

You need to configure the service access settings for each interface under **System Settings** > **Network** on FortiManager. FortiManager supports requests from registered (managed) devices and unregistered (unmanaged) devices. After you enable the FortiManager built-in FDS, you can configure FortiGate devices to use FortiManager FortiGuard services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate Configuration—Use FortiManager FDS

- FortiGate can use different FortiManager devices for central administration, FortiGuard updates, and FortiGuard rating services

```
# config system central-management
    ...
    config server-list
        edit 1
            set server-type update rating
            set server-address 10.0.1.241
        next
    end
    set include-default-servers disable
end
```

Configure server list to override default FDS servers

Server that FortiGate can use for updates and ratings

Enable or disable inclusion of public FortiGuard servers in the override server list

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Now, you will take a look at what is required on FortiGate in order to use FortiManager for FortiGuard services. You need to configure the `server-list`. This is where you define the `server-address`, which is the IP of FortiManager where FortiGate will query ratings and package updates.

You can also define the following options in the `server-type` setting:

- `rating`: web filtering, antispam, and so on
- `update`: antivirus, IPS, and so on

By default, `include-default-servers` is enabled. This allows FortiGate to communicate with the public FortiGuard servers, if the FortiManager devices (configured in `server-list`) are unavailable. If it is disabled, FortiGate devices will never go to the public FDSs, even when the FortiManager devices are down.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Licenses Status

FortiManager: **FortiGuard > Licensing Status**

Refresh | Push Update | Show License Expired Devices | Check License | More

Device Name	Serial Number	ADOM	Firmware Version	Support Contract	FortiGuard Subscriptio	Service Status
DCFW	FGVM010000077648	DC	7.2.4, build1396 (Feature)	24x7	All Valid	Up to Date
NGFW-1 (Primary)	FGVM010000077649	Core	7.2.4, build1396 (Feature)	24x7	All Valid	Up to Date
Spoke-1	FGVM010000077651	Core	7.2.4, build1396 (F			
Spoke-2	FGVM010000077652	Core	7.2.4, build1396 (F			
ISFW	FGVM010000077646	Access	7.2.4, build1396 (F			

IPS & Application Control	[Expires on 2025-11-12]
AntiVirus	[Expires on 2025-11-12]
Web Filtering	[Expires on 2025-11-12]
Email Filtering	[Expires on 2025-11-12]
Outbreak Protection	[Expires on 2025-11-12]
Industrial DB	[Expires on 2025-11-12]

```
#diagnose fmupdate dbcontract
FGVM010000077652 [SERIAL_NO]
...
Contract:  13
     AVDB-1-06-20251112
     AVEN-1-06-20251112
     COMP-1-20-20251112
     ENHN-1-20-20251112
…
Contract Raw Data:
Contract=AVDB-1-06-20251112:0:1:1:0*AVEN-1-06-20251112:0:1:1:0*COMP-1-20-20251112:0:1:1:0*ENHN-1-20-
20251112:0:1:1:0*FGSA-1-06-20251112:0:1:1:0*FMWR-1-06-20251112:0:1:1:0*FRVS-1-06-20251112:0:1:1:0*FURL-1-06-
20251112:0:1:1:0*ISSS-1-06-20251112:0:1:1:0*NIDS-1-06-20251112:0:1:1:0*SPAM-1-06-20251112:0:1:1:0*SPRT-1-20-
20251112:0:1:1:0*ZHVO-1-06-20251112:0:1:1:0|AccountID=courseware@fortinet.com|Industry=Technology|Company=Fortinet
```

FORTINET Training Institute

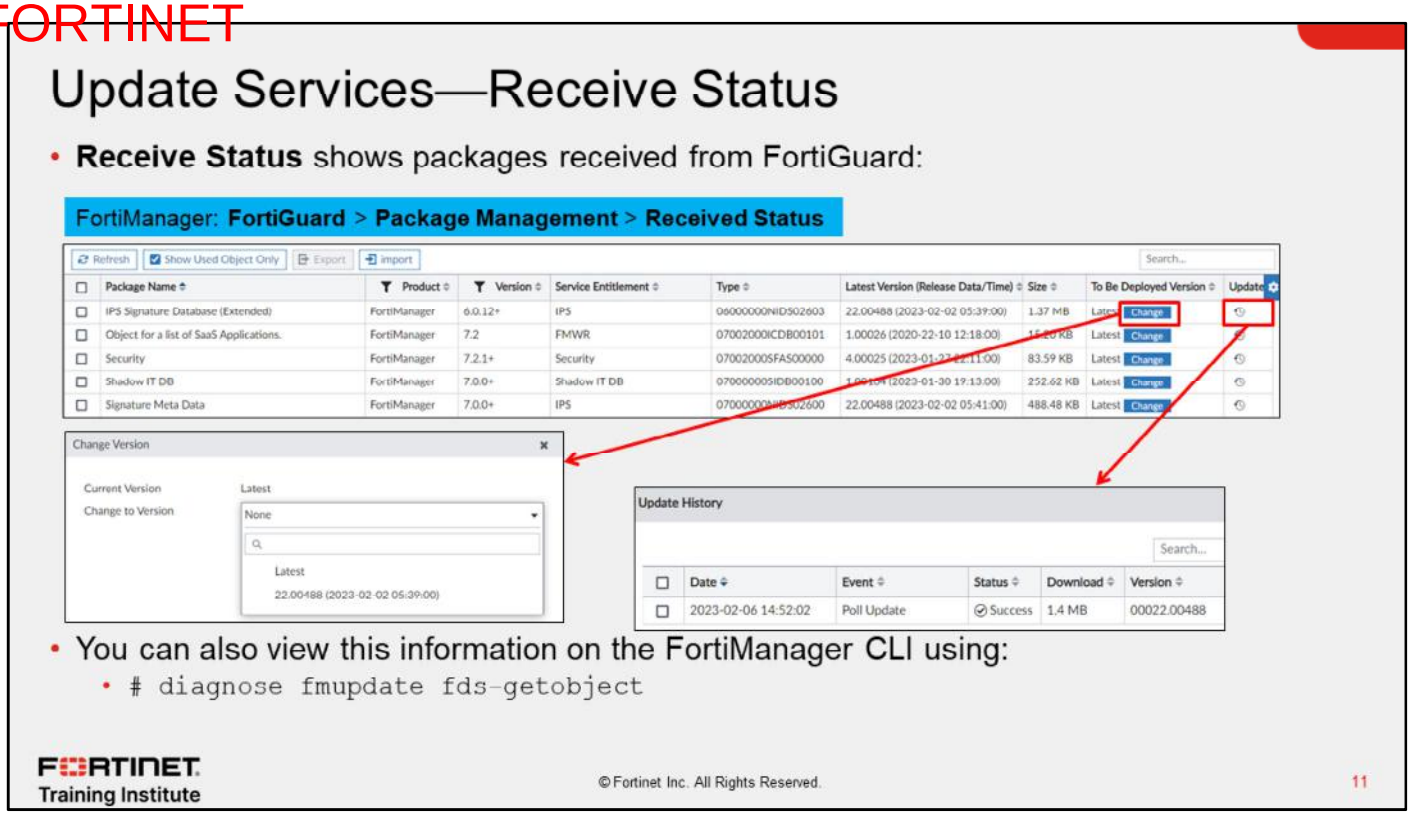
© Fortinet Inc. All Rights Reserved.

10

The GUI section shown on this slide, and related CLI commands, show the status of FortiGuard licenses for all FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You manage the antivirus and IPS signature packages in **FortiGuard** > **Package Management**. Packages received from FortiGuard are listed under **Receive Status**. It displays the package received; version; size; version to be deployed; and update history for FortiGate, FortiMail, FortiAnalyzer, and FortiClient.

Click **Update History** to open the update history page for a package. It shows the update times, the events that occurred, the status of the updates, and the versions downloaded.

You can change the version of the package that will be deployed by selecting **Change** in the **To Be Deployed Version** column.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Update Services—Service Status

- Shows list of managed FortiGate devices, their last update, and status
- Five possible statuses:
  - **Up to Date**
  - **Never Updated**
  - **Pending**
  - **Problem**
  - **Unknown**

FortiManager: **FortiGuard > Package Management > Service Status**

Push Pending | Refresh | Display Options | All ADOMs

Device Name	Serial Number	Platform	firmware_version	Status
Spoke-2	FGVM010000077652	FortiGate-VM64-KVM	7.2.4, build1396	Pending
Spoke-1	FGVM010000077651	FortiGate-VM64-KVM	7.2.4, build1396	Pending
NGFW-1 (Primary)	FGVM010000077649	FortiGate-VM64-KVM	7.2.4, build1396	Up to Date
ISFW	FGVM010000077646	FortiGate-VM64-KVM	7.2.4, build1396	Up to Date
FGVM010000077650	FGVM010000077650	FortiGate-VM64	7.2.0, build1396	Never Updated
DCFW	FGVM010000077648	FortiGate-VM64-KVM	7.2.4, build1396	Up to Date

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

Click **Package Management** > **Service Status** to see a list of all the managed FortiGate devices, their last update time, and their status.
There are five possible statuses:

- **Up to Date**: The latest package was received by FortiGate.
- **Never Updated**: FortiGate never requested or received the package.
- **Pending**: FortiGate has an older version of the package for an acceptable reason (such as a pending scheduled update).
- **Problem**: FortiGate missed the scheduled query, or did not correctly receive the latest package.
- **Unknown**: The FortiGate status is not currently known.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Update Services—FortiGate Databases

- Show the update status (pending or up-to-date) of the databases on each FortiGate:

```
# diagnose fmupdate show-dev-obj
DEVICE(SN:FGVM010000077651):
ID                  Status      DeviceVer    ServerVer    PreferVer    License     LicenseType    Description
--                  ------      ---------    ---------    ---------    -------     -----------    -----------
07002000AFDB00100   up-to-date  00001.00012  00001.00012  00000.00000  valid       FMWR           AntiPhishing DB
07002000CIDB00000   up-to-date  00001.00146  00001.00146  00000.00000  valid       FMWR           Client ID DB
07002000CRDB00000   up-to-date  00001.00040  00001.00040  00000.00000  valid                      Certificate Bundle
07002000FFDB02008   up-to-date  00007.03024  00007.03024  00000.00000  valid       FMWR           Internet Service DB
07002000ICDB00101   up-to-date  00001.00026  00001.00026  00000.00000  valid       FMWR           ICDB
07002000IPGO00000   up-to-date  00003.00162  00003.00162  00000.00000  valid       FMWR           GeoIP Country Level
07002000MADB00200   up-to-date  00001.00152  00001.00152  00000.00000  valid       FMWR           MAC Address DB
07002000MCDB00100   up-to-date  00001.00413  00001.00413  00000.00000  valid       FURL           Malicious Certificat
07002000SFAS00000   up-to-date  00004.00025  00004.00025  00000.00000  valid       FGSA           Security
07002000UWDB00100   pending     00003.00766  00003.00767  00000.00000  valid       FMWR           URL Whitelist DB ...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

The command shown on this slide contains details about which updates were installed or will be installed on devices managed by FortiManager (displayed by S/N).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Update Services—Logging

- FortiManager can log all update services activities
- Enable the logging `debug` level for troubleshooting:

```
# config sys localog disk setting
  set severity debug
end
# config fmupdate fds-setting
  set linkd-log debug
  set umsvc-log debug
end
```

- You can retrieve these internal log files through SFTP or FTP with the following command:

```
FortiManager # diagnose system export umlog <SFTP| FTP> . <FTP Server>
<username> <password> <destination directory> <filename>.tgz
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

FortiManager can log update services events. They are useful for troubleshooting. Set the logging level to debug first. The next slide shows the command you must use to display the logs. Alternatively, you can export the logs to an SFTP or FTP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Update Services—Logging (Contd)

- Display the update services logs:
  - Includes updates from FortiGuard to FortiManager, and from FortiManager to FortiGate

```
# diagnose fmupdate view-linkd-log fds
2023/03/16_04:14:09.013 info    fds_svrd[936]: Process client 10.1.0.1:0 request SUCCESS
2023/03/16_04:14:09.013 notice  fds_worker[1291]: process remote(::ffff:10.1.0.1) SUCCESS!
2023/03/16_04:19:02.326 notice  fds_worker[1291]: accept connection from ::ffff:10.1.0.254.
2023/03/16_04:19:02.541 info    fds_svrd[936]: Start fds server session from 127.0.0.1
2023/03/16_04:19:02.542 info    fds_svrd[936]: [FGT-->FMG] Request:
Protocol=3.2|Command=Update|Firmware=FGVMK6-FW-7.02-
1396|SerialNumber=FGVM010000077649|UpdateMethod=1|AcceptDelta=1|Uid=464f5254495044f483387249179e7500|DataIt
em=07002000DBDB00100-00003.00176-2302031155*07002000CIDB00000-00001.00146-
2301122352*07002000IPGO000000316223020117 05*00000000FCNI00000-00000.00000-0000000000*00000000FDNI00000-
00000.00000-0000000000*01000000FSCI00100-00000.00000-0000000000*07002000FFDB02008-00007.03024-
2302032246*07002000UWDB00100-00003.00767-2302060805*07002000CRDB00000-00001.00040-
2301111910*07002000SFAS00000-00004.00025-2302160419*07002000MCDB00100-00001.00413-
2302020845*01000000ALCI00000-00000.00000-0000000000*07002000MADB00200-00001.00152-
2023/03/16_04:19:02.553 info    fds_svrd[936]: [FMG-->FGT] Response: Protocol=3.2|Firmware=FMG-VM64-KVM-FW-
7.02-1334|SerialNumber=FMG-
VM0A16003351|Response=200|Persistent=false|ResponseItem=07002000DBDB00100:204*07002000CIDB00000:204*0700200
0IPGO00000:204*00000000FCNI00000:204*00000000FDNI00000:204*01000000FSCI00100:200*07002000FFDB02008:204*0700
2000UWDB00100:204*07002000CRDB00000:204*07002000SFAS00000:204*07002000MCDB00100:204*01000000ALCI00000:204*0
7002000MADB00200:204*07002000AFDB00100:204*07002000ICDB00101:204^M ^M
2023/03/16_04:19:02.553 info    fds_svrd[936]: Process client 127.0.0.1 request SUCCESS
2023/03/16_04:19:02.553 notice  fds_worker[1291]: process remote(::ffff:10.1.0.254) SUCCESS!
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

The update services logs display the FortiGate requests made to FortiManager, and the FortiManager requests made to the public FortiGuard servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Rating Services—Receive Status

- Shows information about rating packages received from FortiGuard:

FortiManager: **FortiGuard** > **Query Server Management** > **Receive Status**

Refresh | Export | import

Package Received	Latest Version (Release Data/Time)	Size	Update History
Antispam(HASH)	00081.49075(2021-09-17 05:51:01(PDT))	38.32M	
Antispam(IP)	00103.10258(2021-09-17 05:50:01(PDT))	905.63M	
Antispam(URI)	00095.34392(2021-09-17 05:48:01(PDT))	27.88M	
AntiVirus Query	0.000(- -)	0B	
File Query	0.000(- -)	0B	

Date	Event	Status	Download	Version
2021-09-17 14:56:36	Poll Update	Success	38.3 MB	00081.49075
2021-09-17 14:38:09	Poll Update	Success	38.3 MB	00081.49071
2021-09-17 14:25:52	Poll Update	Success	38.3 MB	00081.49069
2021-09-17 14:09:56	Poll Update	Success	38.3 MB	00081.49066
2021-09-17 13:57:28	Poll Update	Success	38.3 MB	00081.49064

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

The web filtering and antispam databases are managed under **FortiGuard Management** > **Query Server Management**. The databases received from FortiGuard are listed under **Receive Status**.

This page displays the date and time when updates were received from the server, the update version, the size of the update, and the update history.

Select **Update History** to open the update history page for a package. It shows the update times, the events that occurred, the status of the updates, the version number, and size of the download.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Rating Services—Statistics

- Displays number (and rate) of web filtering and antispam queries received:

```
# diagnose fmupdate fgd-wfas-rate
        Webfilter:
        0 queries, 0 rated in 60 minutes
        114 queries, 80 rated in 60 minutes
        ...
        Antispam_ip:
        Antispam_url:
        Antispam_hash:
        Antivirus:
        0 queries, 0 rated in 60 minutes
        ...
        FileQuery:
        0 queries, 0 rated in 60 minutes
        ...
```

- Rate interval can be configured:

```
# config fmupdate web-spam fgd-setting
# set stat-log-interval <integer>
```

  - These statistics are also periodically logged to the event log

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

You can view statistics about rating requests made by FortiGate to FortiManager using the command shown on this slide. By default, this command displays the request rates for the last 60 minutes. However, the time period can be changed using the command shown on this slide. This information is also periodically logged in the event log.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Rating Services—Logging

- FortiManager can log all rating services activities
- Enable the logging `debug` level for troubleshooting:

```
# config sys locallog disk setting
  set severity debug
end
# config fmudate web-spam fgd-setting
  set linkd-log debug
  set update-log enable
end
```

- To display the logs:

```
# diagnose fmupdate view-linkd-log fgd
```

FORTINET Training Institute

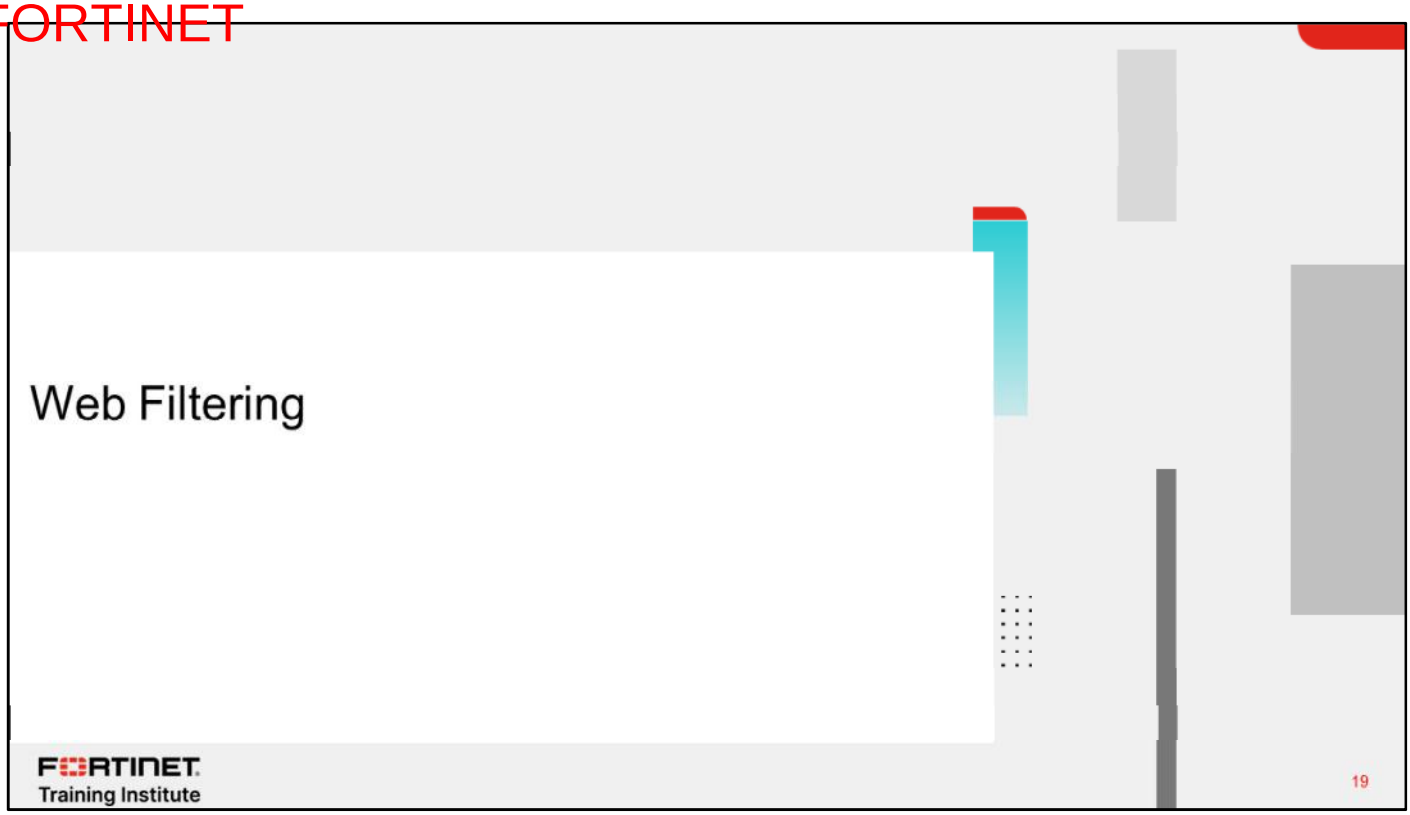
© Fortinet Inc. All Rights Reserved.

18

FortiManager can log rating services events in the same way that it logs update services events. For troubleshooting, it is recommended that you enable the debug level first.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about web filtering.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Web Filtering Review

- Supports proxy and flow inspection modes
- FortiGate queries FortiGuard to get the URL category
  - Caches the FortiGuard answer
  - Cache TTL value is configurable

```
#config system fortiguard
webfilter-cache     : enable
webfilter-cache-ttl : 3600
...
```

FORTINET Training Institute

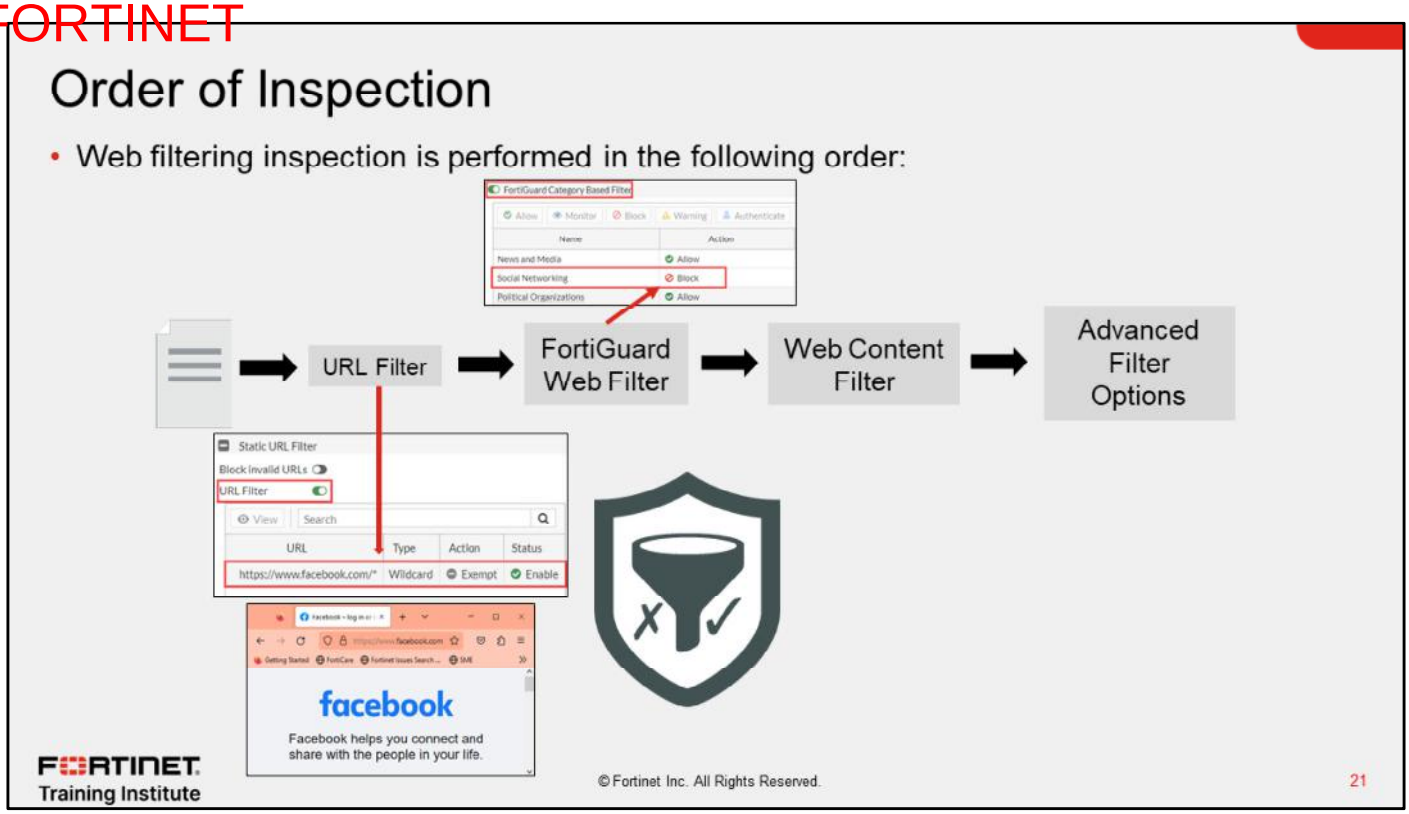
© Fortinet Inc. All Rights Reserved.

20

Web filtering in FortiOS operates in one of two inspection modes: proxy and flow. By default, FortiGate caches the rating results it receives from FortiGuard. So, before it sends rating requests to FortiGuard, FortiGate checks that the website category isn't already in the local cache. You can configure the time-to-live (TTL) of the entries in the web filtering cache.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



During web filtering inspection, FortiGate first checks the static URL filter list, then the FortiGuard categories, and then the content filtering list. In the example on this slide, **Social Networking** category is blocked by FortiGuard category filter in the web filter profile to block facebook. However, based on the URL filter when user access the www.facebook.com, website will be allowed

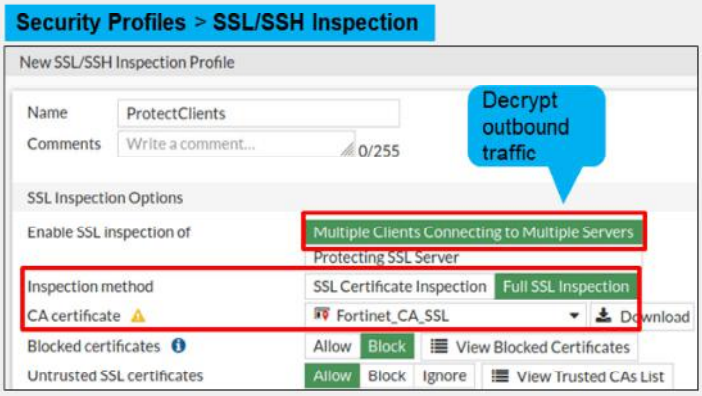
Finally, FortiGate can execute some advanced options, such as manipulation of HTTP headers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL Inspection

- Two methods of inspecting outbound encrypted sessions
  - SSL certificate inspection
  - SSL full inspection



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

With encrypted traffic making up between 60% to 80% of most organizations' traffic, it has become critical that encrypted traffic is inspected in order to maintain a secure network. In the context of web filtering, FortiGate has two methods of inspecting outbound encrypted sessions: SSL certificate inspection and full SSL inspection.

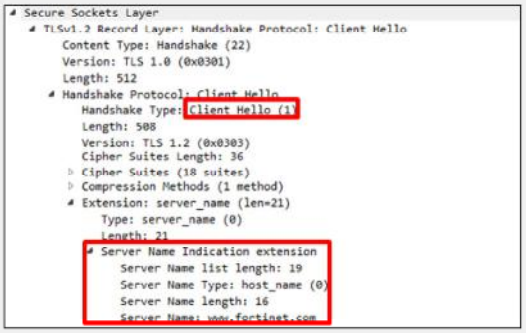
You can configure an SSL/SSH inspection profile to use either method of inspection.

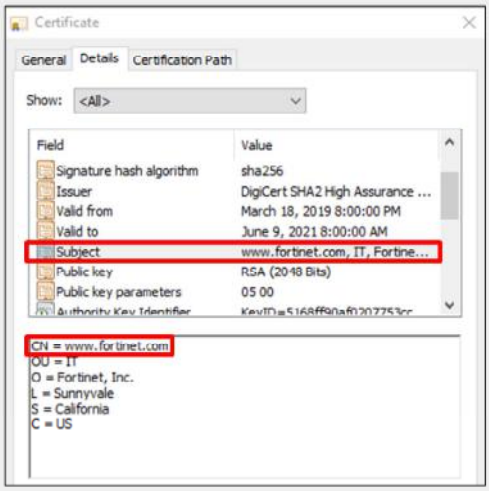
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SSL Certificate Inspection

- If server name identification (SNI) is not present, FortiGate uses the CN field in the server certificate to obtain the FQDN
- Uses the SNI extension from the Client Hello of the SSL handshake, to obtain the FQDN





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

When using SSL certificate inspection, FortiGate doesn't decrypt or inspect any encrypted traffic. Using this method, FortiGate inspects only the initial unencrypted SSL handshake. If the SNI field exists, FortiGate uses it to obtain the FQDN to rate the site. If the SNI isn't present, FortiGate retrieves the FQDN from the CN field of the server certificate.

In some cases, the CN server name might not match the requested FQDN. For example, the value of the CN field in the digital certificate of youtube.com is google.com. So, if you connect to youtube.com from a browser that doesn't support SNI, and FortiGate uses the SSL certificate inspection method, FortiGate assumes, incorrectly, that you are connecting to google.com, and uses the google.com category instead of the category for youtube.com.

Note that SSL certificate inspection will work only with web filtering, and with some application signature detection when doing application control. It *does not* work with antivirus, IPS, or DLP scanning, where the full payload needs to be inspected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SSL Certificate Inspection and SNI Check

```
config firewall ssl-ssh-profile
  edit <profile_name>
    config https
      set sni-server-cert-check [enable* | strict | disable]
```

- `enable`: If the `SNI` does not match the `CN` or `SAN` fields in the returned server's certificate, FortiGate uses the `CN` field instead of the `SNI` to obtain the FQDN
- `strict`: If the `SNI` does not match the `CN` or `SAN` fields in the returned server's certificate, FortiGate closes the connection
- `disable`: FortiGate does not check the `SNI`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

When doing certificate-based inspection, by default, FortiGate validates the information in the `SNI` field of the client's request against the information in `CN` and `SAN` fields of the server's certificate. If the domain in the `SNI` field does not match any of the domains listed in the `CN` and `SAN` fields, FortiGate uses the domain in the `CN` field instead of the domain in the `SNI` field.

You can configure FortiGate to be more strict, so it closes the client connection if the domain in the `SNI` field does not match any of the domains listed in the `CN` and `SAN` fields.

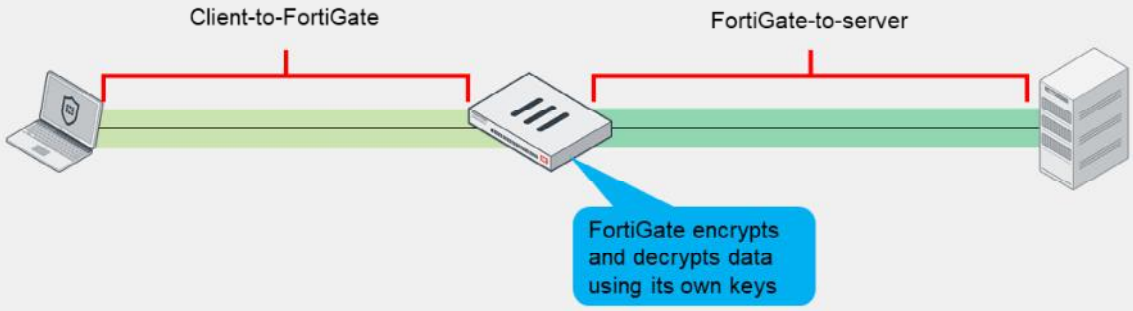
You can also configure FortiGate to disable SNI checking altogether, so that FortiGate always rates URLs based on the FQDN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Full SSL Inspection

- FortiGate acts as a man-in-the middle proxy
- Maintains two separate SSL sessions—client-to-FortiGate and FortiGate-to-server
- FortiGate encrypts and decrypts packets using its own keys



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

You can configure full SSL inspection to inspect all of the packet contents, including the payload. FortiGate performs this inspection by proxying the SSL connection. Two SSL sessions are established—client-to-FortiGate and FortiGate-to-server. The two established sessions allows FortiGate to encrypt and decrypt packets using its own keys, which allows FortiGate to fully inspect all data inside the encrypted packets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Web Filtering Categories

- To check the list of web filtering categories and their corresponding numerical values

These numerical values can be used to create web filtering profiles using the FortiGate CLI or using scripts on FortiManager

```
# get webfilter categories
  g01 Potentially Liable:
      1 Drug Abuse
      3 Hacking
      4 Illegal or Unethical
      ...
  g02 Adult/Mature Content:
      2 Alternative Beliefs
      7 Abortion
      ...
```

- You can also use category numbers to test whether a specific category or subcategory is allowed or blocked

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

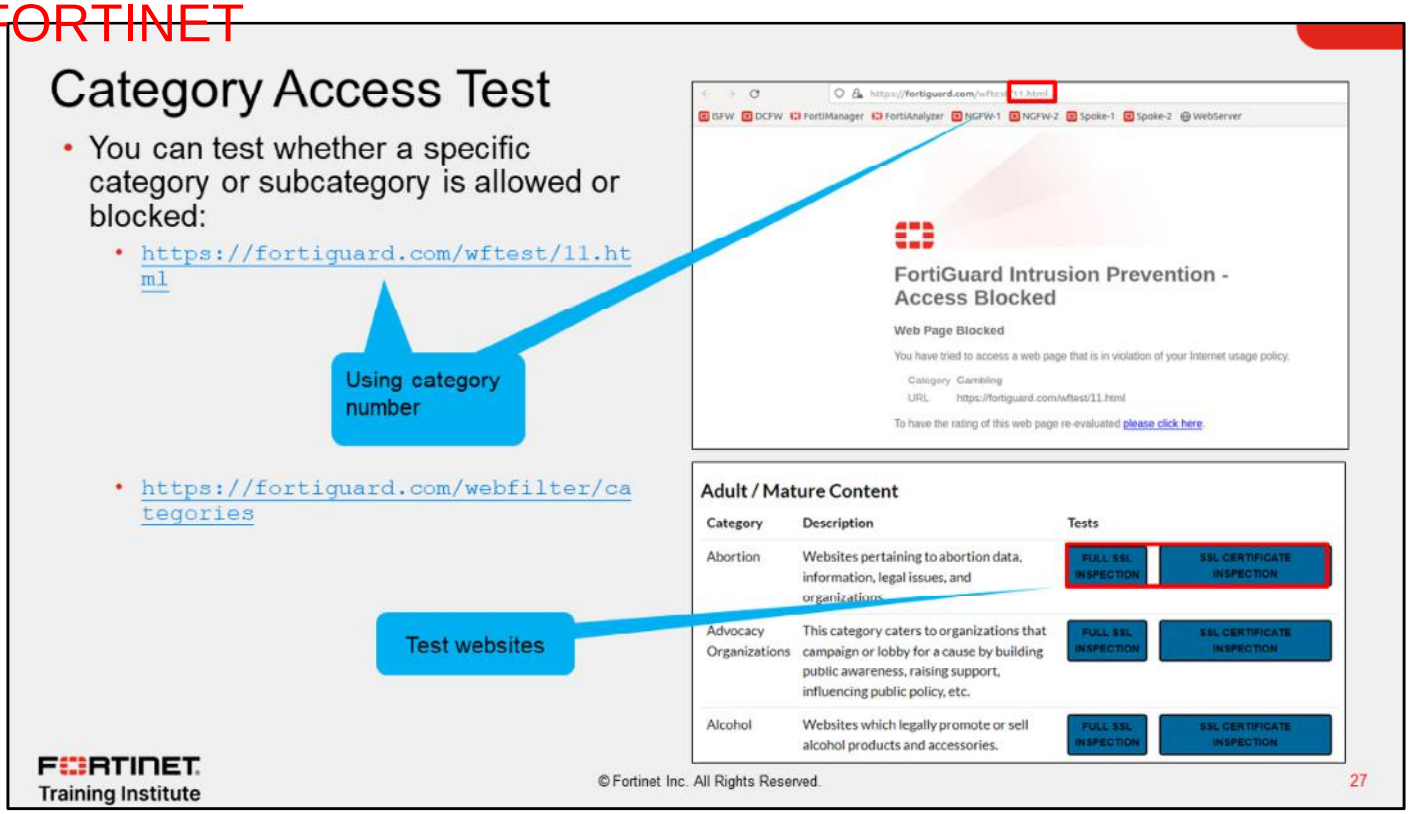
26

You can use the FortiOS CLI to display the list of FortiGuard categories and their numerical values.

You can use FortiGuard category numbers when you create web profiles using the FortiOS CLI, or using scripts on FortiManager. Similar to using the GUI, you can configure different actions for each category using the CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can use category numbers to test whether a specific category or subcategory is allowed or blocked. Use the URL format shown on this slide for that purpose.

In the example shown on this slide, the category 11 is gambling. The test confirms that all sites listed in this category will be blocked. The replacement message page displays the category that is blocked, with other information, such as client IP, server IP, and user information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Session Flags and Inspection Mode

- Proxy-based inspection adds the redir flag in the session table:
  `state=redir local may_dirty none app_ntf`
- Flow-based inspection adds the ndr flag in the session table:
  `state=may_dirty ndr none app_ntf`
- Additionally, proxy-based inspection contains the following line in the debug flow:
  `func=av_receive line=254 msg="send to application layer"`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

Two session flags indicate whether the traffic is inspected in proxy-based mode or flow-based mode. The flag `redir` means the traffic is inspected in proxy-based mode. The flag `ndr` means the traffic is inspected in flow-based mode. In the case of proxy-based inspection, the debug flow contains the message `"sent to the application layer"`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Security Profiles—Device Performance

- Enabling profiles has an impact on firewall throughput
  - FortiGate kernel inspect sessions to enforce filtering (for example, web filter)
- Selecting the FortiGate inspection modes:
  - Flow-based
    - Default mode
    - Optimize performance
  - Proxy-based
    - Processed by FortiGate Proxy or CPU
    - Provides thorough inspection
    - Support advanced features like *safe search*
- Encrypted traffic that requires SSL inspection can also impact throughput
  - SSL deep inspection can cause high CPU and memory usage
  - All traffic needs to decrypt, inspect and re-encrypt.
  - Use hardware acceleration (content processor) to offload SSL processing

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

Enabling the security profiles on the FortiGate impacts on firewall resources and throughput. Packets are sent to the kernel or main CPU to enforce filtering. FortiOS supports flow-based and proxy-based inspection in firewall policies and security profiles.

Depending on your requirements, you can select inspection mode, but it is useful to know some differences and how it can impact the firewall performance. Flow-based inspection identifies and blocks threats in real time as FortiOS identifies them typically requires lower processing resources than proxy-based inspection. It is recommended to apply flow-based inspection to policies that prioritize traffic throughput

Proxy-based inspection involves buffering traffic and examining it as a whole before determining an action. Having all the data to analyze allows for the examination of more data points than flow-based inspection. Some advanced features like usage quota, safe search, and web-profile override are also supported in proxy-based inspection.

You learned that FortiGate requires SSL inspection to apply web filtering. Because of this, the overall performance of FortiGate can be reduced when enabling SSL deep inspection on FortiGate. This is because all traffic needs to be decrypted, inspected, and re-encrypted. There are some best practices to reduce the impact:

1. You can limit the number policies that allow encrypted traffic.
2. Use the flexibility of a FortiGate device security policy to gradually deploy SSL inspection, rather than enabling it all at once.
3. Apply SSL deep inspection only where it is needed. For example, exempt known and trusted traffic from SSL inspection.
4. Use hardware acceleration, such as content processor (CP8 or CP9) to offload SSL content scanning.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Security Profiles—Device Performance (Contd)

- Hardware acceleration can offload resource-intensive processing from main CPU
  - If supported by FortiGate model
- Network processor (NP)
  - Offload high volume of network traffic
  - Offloads firewall sessions that include flow-based security profiles
  - Does not support proxy-based profile
- Firewall policy with mixed (flow-based and proxy-based) security profiles does not offload
- There are some cases where sessions may not be offloaded even if NP acceleration is available:
  - NP acceleration is disabled on the policy
  - Firewall policy includes proxy-based security profiles
  - Firewall session requires FortiOS session-helpers
  - Tunnelling is enabled (except IPSec VPN sessions)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

The firewall sessions that require flow-based security features can be offloaded to network processors (NP6 or NP7) if the FortiGate supports. Network processors reduce the workload on the FortiGate CPU and improve overall throughput.

Note that a firewall policy that includes a mix of flow-based and proxy-based profiles never offloads to NP and is always processed by the FortiGate CPU.

There are some cases where firewall sessions may not offload even when NP acceleration is enabled and sessions are handled by the FortiGate CPU. These are:

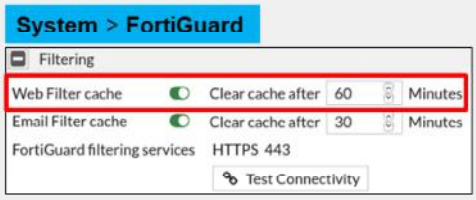
1. NP acceleration is disabled on the policy.
2. Firewall policy includes proxy-based security profiles.
3. Firewall session requires FortiOS session helper.
4. Tunneling is enabled, including traffic to or from a tunnelled interface (SSL VPN, GRE, and so on), except IPSec VPN sessions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Web Filter Cache

- Improves performance by reducing requests to FortiGuard
- Cache is checked before sending a request to the FortiGuard server
  - FortiGate remembers response of visited websites
  - TTL settings control the number of seconds the query results are cached
  - Request is considered a rating error after timeout (15 seconds as default)
- HTTPS port 443 enforced by default FortiGuard or FortiManager communications
  - Disable FortiGuard anycast setting on CLI to use UDP ports 443, 53, or 8888
- Enabled by default—default TTL is 60 minutes (3600 seconds)




```
config system fortiguard
    set fortiguard-anycast {enable|disable}
    set protocol {udp|https}
    set port {8888|53|443}
    set webfilter-timeout {<1> - <30>}
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

FortiGate can maintain a list of recent website rating responses in memory. So, if the URL is already known, FortiGate doesn't send back a rating request.

By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI. These ports and protocols to query the servers (FortiGuard or FortiManager) HTTPS port 53 and port 8888, UDP port 443, port 53, and port 8888. If you are using UDP port 53, any kind of inspection reveals that this traffic is not DNS and prevents the service from working. In this case, you can switch to the alternate UDP port 443 or port 8888, or change the protocol to HTTPS, but these ports are not guaranteed to be open in all networks, so you must check beforehand.

Caching responses reduces the amount of time it takes to establish a rating for a website. Also, memory lookup is much quicker than packets travelling on the internet.

The timeout defaults to 15 seconds, but you can set it as high as 30 seconds, if necessary.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Web Filtering Cache

```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urcCache.t
Cache Contents:
-=-=-=-=-=-=-=-
Cache Mode:   TTL
Cache DB Ver: 23.6106

Domain   |IP        DB Ver   T URL
34000000|34000000 23.6106  P Bhttp://training.fortinet.com/
25000000|25000000 23.6106  E Bhttps://twitter.com/…

# get webfilter categories
…
g07 General Interest - Business:
     31 Finance and Banking
     …
     51 Government and Legal Organizations
     52 Information Technology
```

FortiGuard category for the domain in hexadecimal

34 Hex = 52 decimal

FortiGuard category for the IP address in hexadecimal

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

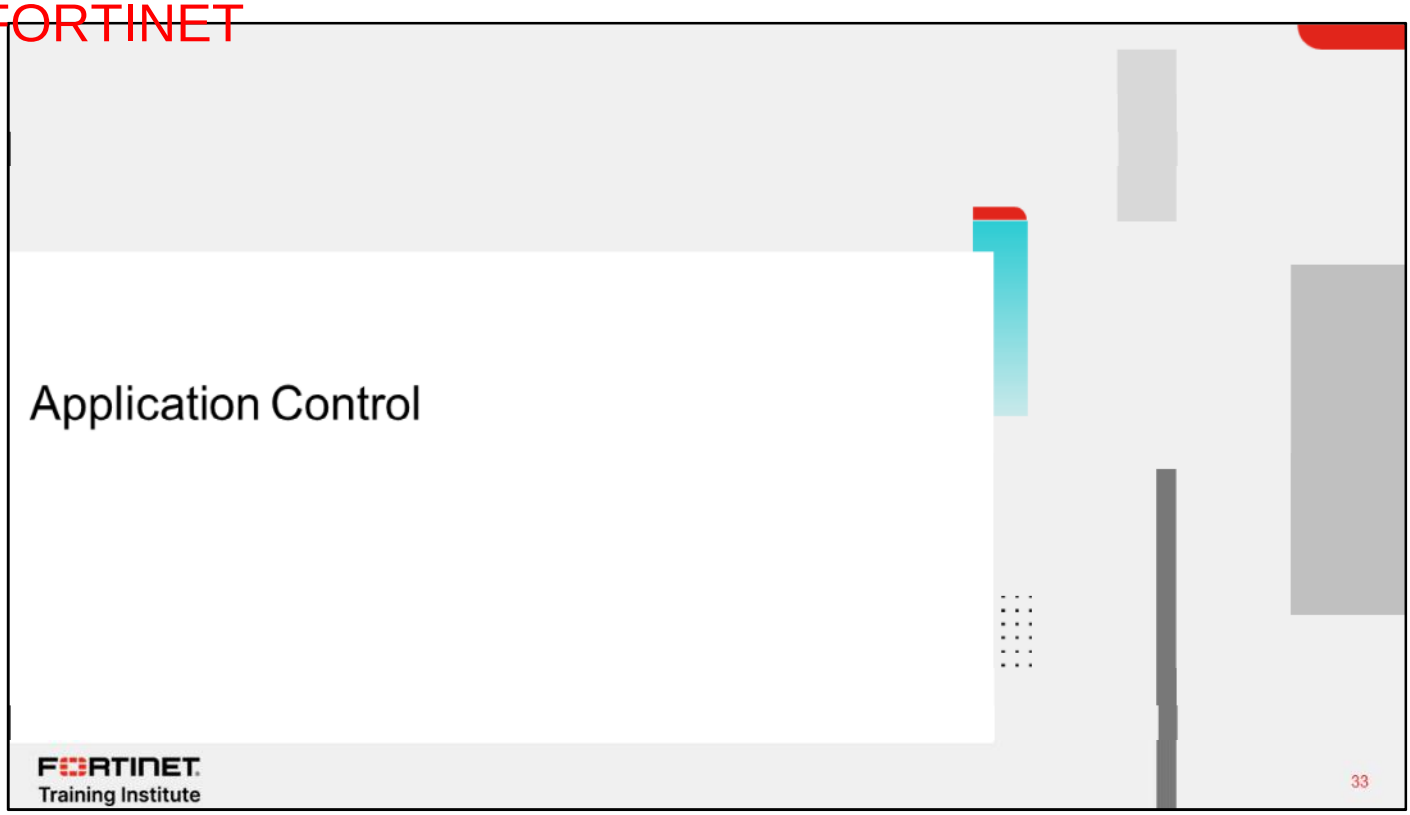
32

To list the content of the FortiGuard web filtering cache, use the command `diagnose webfilter fortiguard cache dump`. For each URL, the output lists its rating by domain name and IP address. The rating by domain name is the first two digits of the first number from left to right. It is the category ID represented in hexadecimal. The rating by IP address is the first two digits of the second number. It is also the category ID represented in hexadecimal.

The command `get webfilter categories` lists all the categories with their respective ID numbers. In this list, the IDs are represented in decimal. So, if you want to find the category name for a URL in the cache, use the first command to list the cache, and convert the ID number from hexadecimal to decimal. Then, use the second command to find the category name for that ID number.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about application control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Application Control Profiles

- Configured when FortiGate NGFW mode is set to profile-based
- Uses flow-based scanning techniques in both inspection modes
- Allows you to filter application traffic based on:
  - Categories
    - Similar applications are grouped together
    - Can view application control signatures for that category
    - Can configure actions for predefined categories
  - Application overrides
    - Allows you to configure actions for specific signatures or applications
  - Filter overrides
    - Provides a more flexible way to create application categorization based on behavior, popularity, protocol, risk, and so on
- Must be applied to a firewall policy

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

When FortiGate or a VDOM is operating in flow-based (NGFW mode set to profile-based, policy set to flow-based) inspection mode or policy set to proxy-based inspection mode, to configure application control, administrators must create an application control *profile* and apply that profile to a firewall policy.

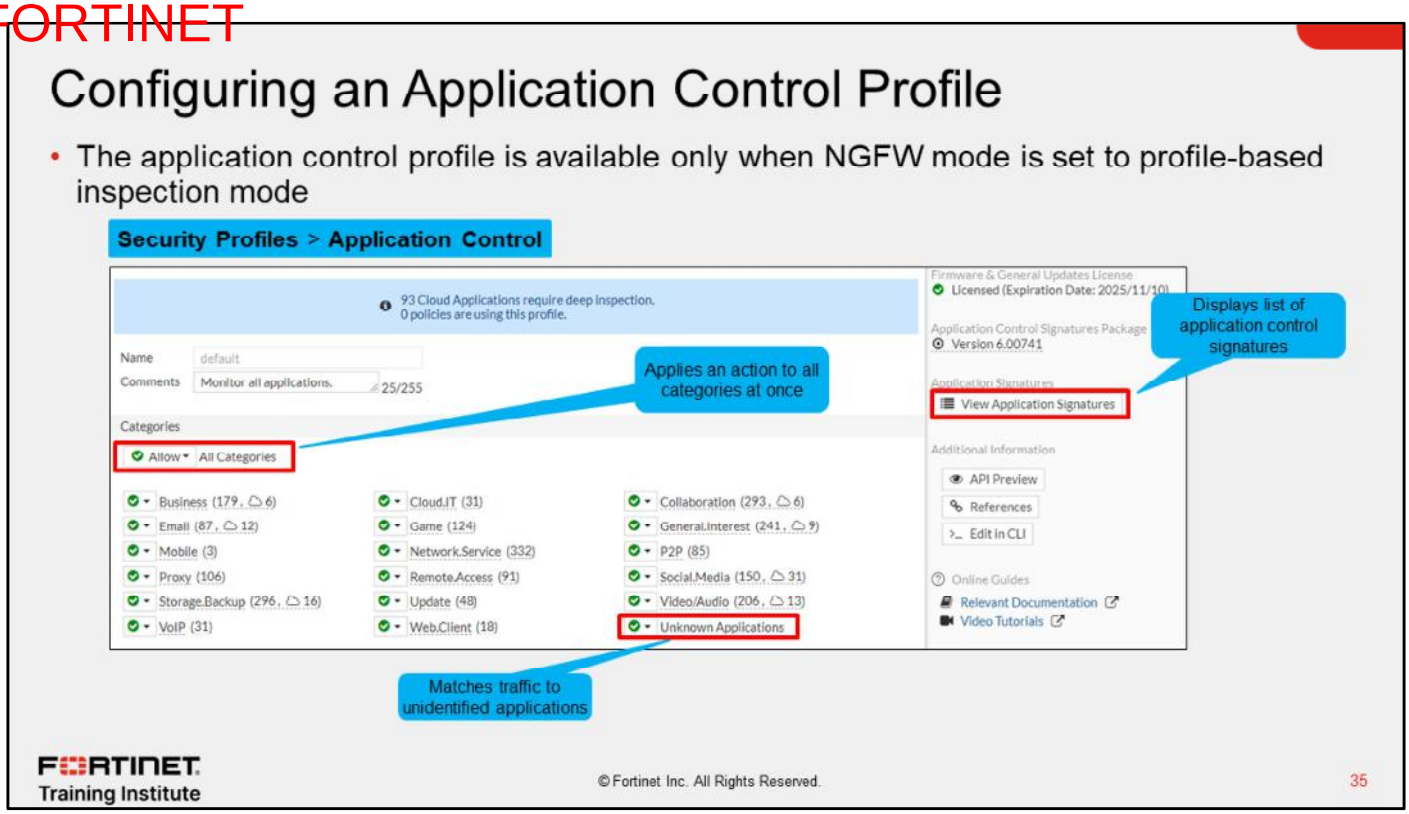
It is important to note that the application control profile uses flow-based scanning techniques, regardless of which inspection mode is used on the policy.

The application control profile consists of three different types of filters:

- Categories: Groups applications based on similarity. For example, all applications that are capable of providing remote access are grouped in the **Remote Access** category. You can view the signatures of all applications in a category or apply an action to a category as a whole.
- Application overrides: Provides the flexibility to control specific signatures and applications.
- Filter overrides: Useful when a predefined category does not meet your requirements and you want to block all applications based on criteria that is not available in categories. You can configure the categorization of applications based on behavior, popularity, protocol, risk, vendor, or the technology used by the applications, and take action based on that.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The application control profile is configured on the **Application Control** page. You can configure actions based on categories, application overrides, and filter overrides. You can also view the list of application control signatures by clicking **View Application Signatures**.

At the top of the **Application Control** profile page, you will see a summary of how many cloud applications require deep inspection. Cloud applications that use SSL encryption cannot be scanned without a deep inspection profile. FortiGate must decrypt the traffic in order to perform inspection and control application traffic.

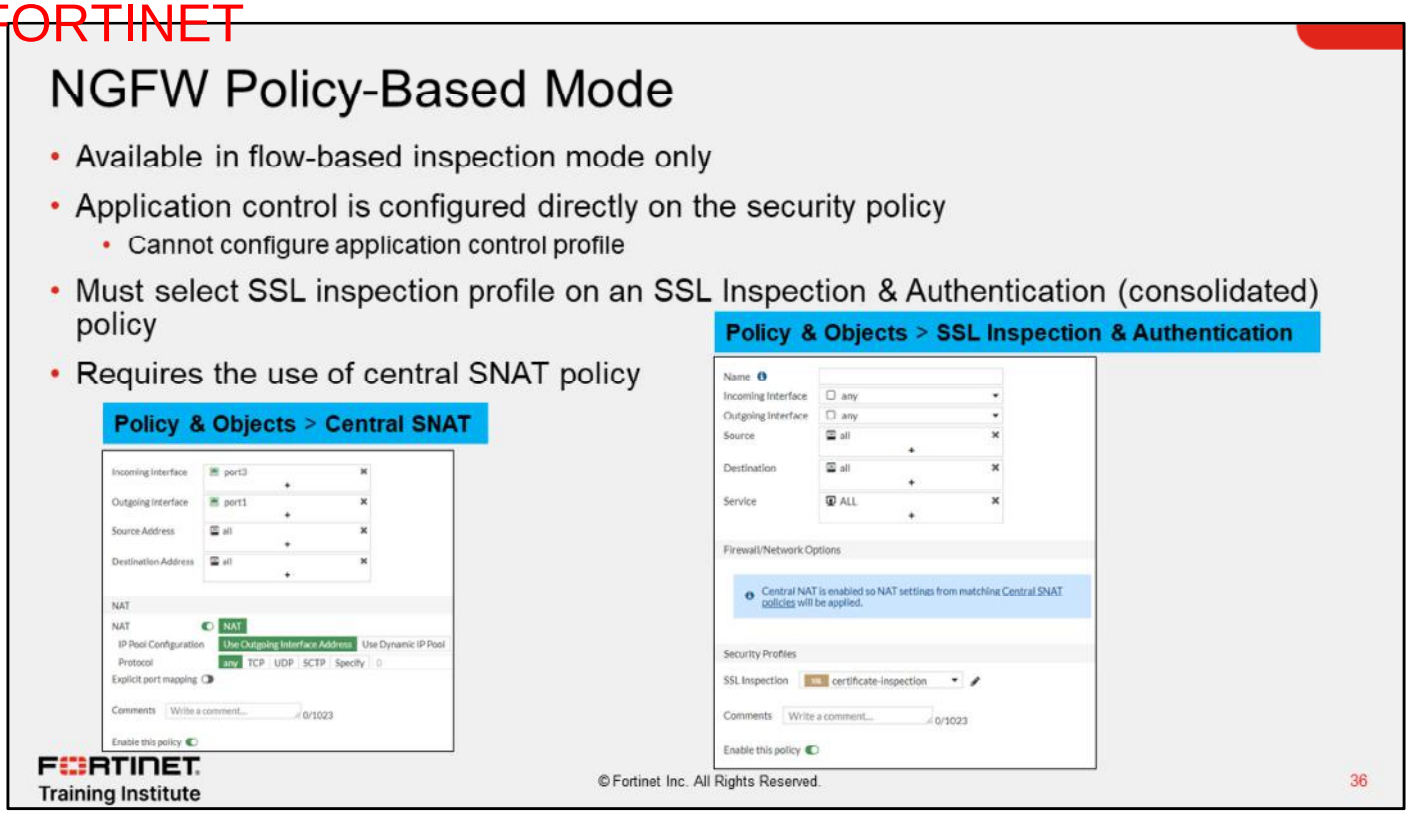
The **Unknown Applications** setting matches traffic that can't be matched to any application control signature and identifies the traffic as `unknown application` in the logs. Factors that contribute to traffic being identified as `unknown application` include:

- How many rare applications your users are using
- Which IPS database version you are using

Identifying traffic as unknown can cause frequent log entries. Frequent log entries decrease performance.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

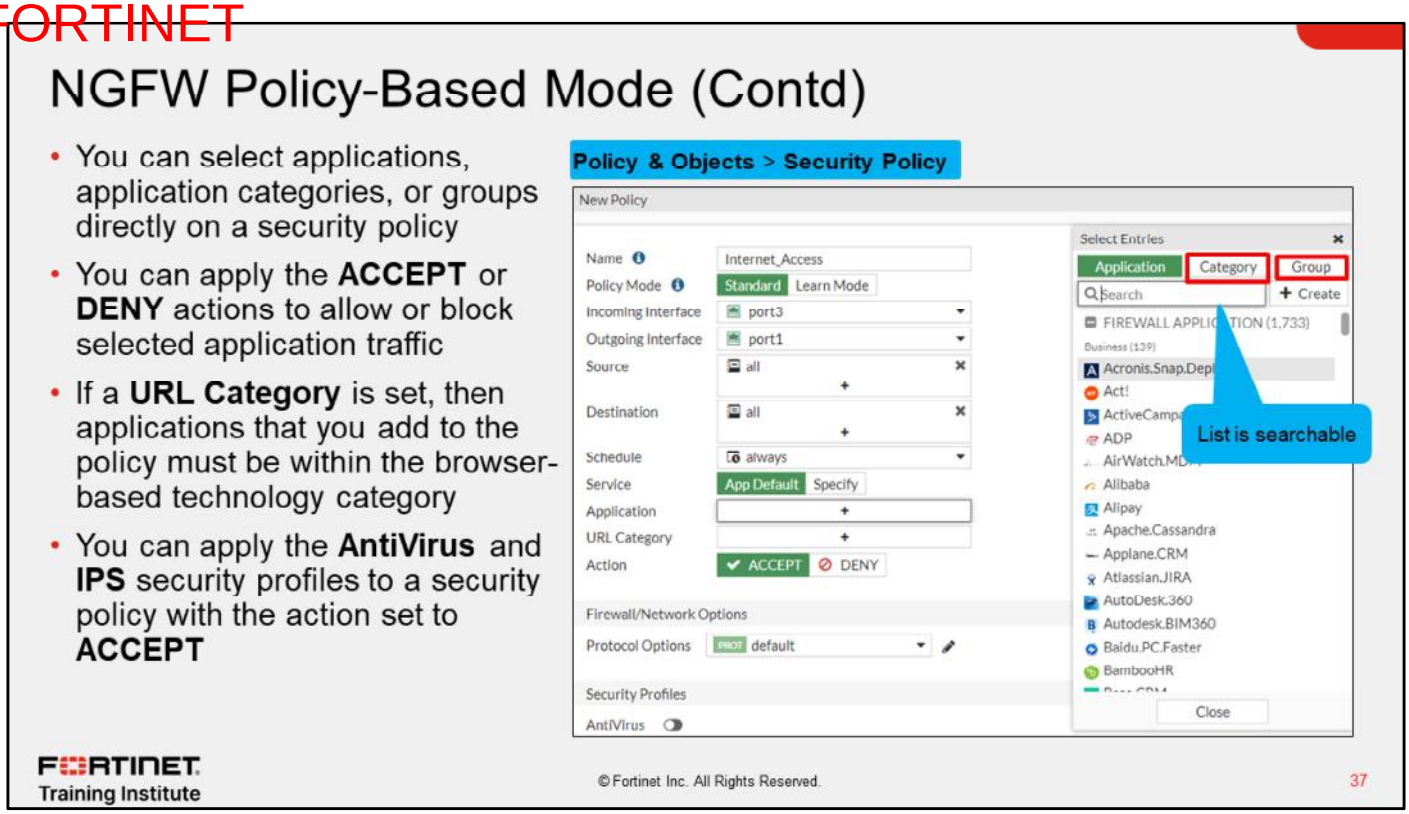


When FortiGate is operating in NGFW policy-based mode, administrators can apply application control to a security policy directly, instead of having to create an application control profile first, and then apply that to a firewall policy. Eliminating the need to use an application control profile makes it easier for the administrator to select the applications or application categories they want to allow or deny in the firewall policy.

It is important to note that all security policies in an NGFW policy-based mode VDOM or FortiGate must specify an SSL/SSH inspection profile on a consolidated policy. NGFW policy-based mode also requires the use of central source NAT (SNAT), instead of NAT settings applied within the firewall policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can select one or more applications, application groups, and application categories on a security policy in the **Application** section. After you click the **+** icon for an application**,** a pop-up window opens. In that window, you can search for and select one or more application signatures, application groups, or application categories. Based on the applications, groups, and application categories applied to the policy, FortiOS applies the security action to the application traffic.

You can configure the **URL Category** within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website.

You can also configure the **Group** with multiple applications and application categories. This allows the administrator to mix multiple applications and categories.

In addition to applying a URL category filter, you can also apply **AntiVirus** and **IPS** security profiles to application traffic that is allowed to pass through.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

How Does NGFW Policy-Based Filtering Work?

- It is a three-step process:
  - Step 1–Allow all applications until they can be identified:
    - Uses only the IPv4 header information to match the policy
    - Accepts the traffic
    - Creates an entry in the session table with the `may_dirty` flag
    - Forwards all the packets to the IPS engine for inspection
  - Step 2–As soon as the IPS engine identifies the application, it adds the following to the session:
    - `dirty` flag - instructs the kernel to re-evaluate session entry
    - `app_valid` flag - indicates that IPS engine has validated the traffic
    - Application ID
  - Step 3–The dirty flag instructs the kernel to look up the security policy again:
    - This time the kernel uses the Layer 4 headers *and* the Layer 7 information to match the traffic
    - The action configured in the security policy is applied to the identified application traffic

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

FortiOS uses a three-step process to perform NGFW policy-based application filtering. Here is a brief overview of what happens at each step.

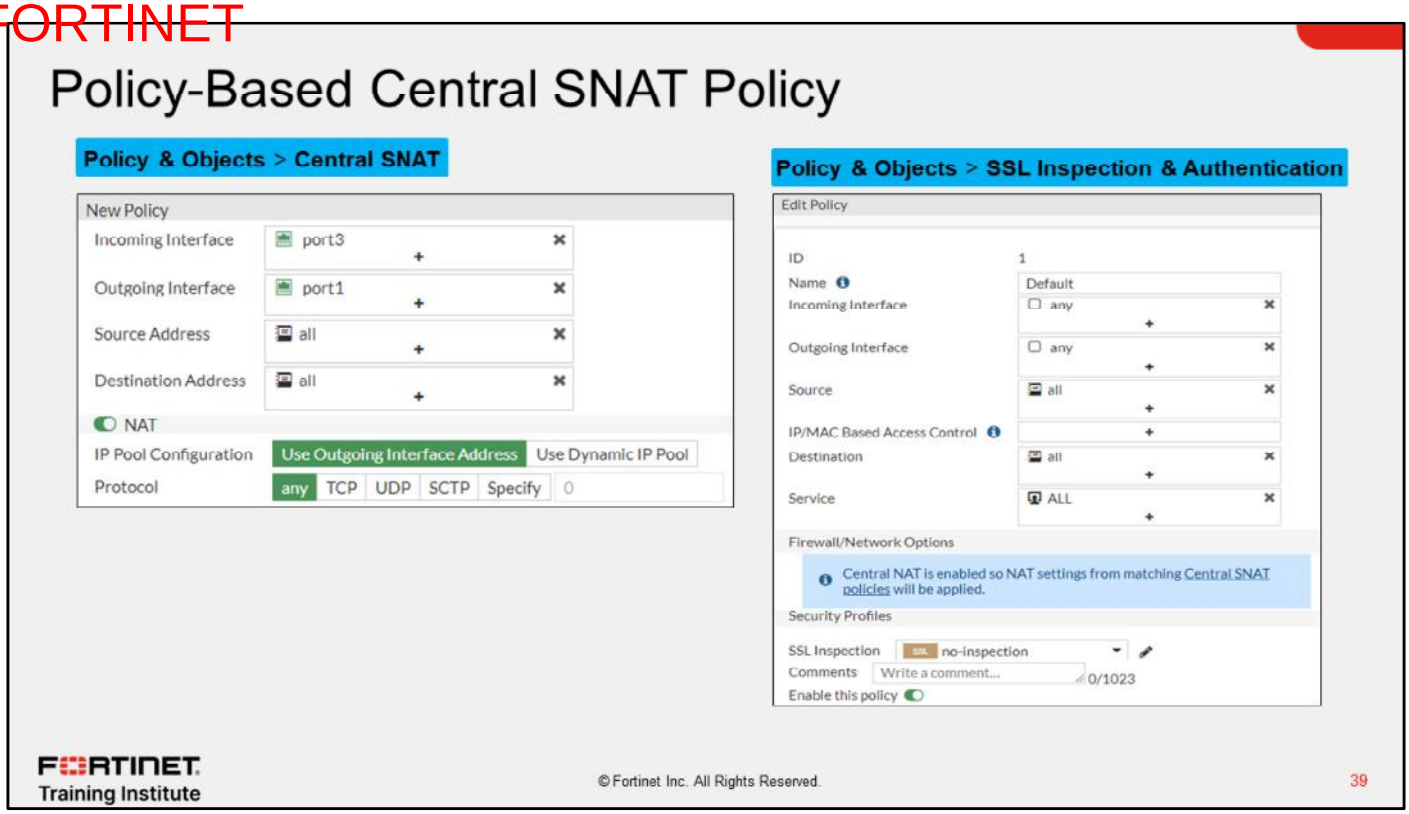
In step 1, FortiOS allows all traffic while forwarding packets to the IPS engine for inspection and identification of the traffic. At the same time, FortiOS creates an entry in the session table allowing the traffic to pass and it adds a `may_dirty` flag to it.

In step 2, as soon as the IPS engine identifies the application, it updates the session entry with the following information: `dirty` flag, `app_valid` flag, and an application ID.

In step 3, the FortiOS kernel performs a security policy lookup again, to see if the identified application ID is listed in any of the existing security policies. This time the kernel uses both Layer 4 and Layer 7 information for policy matching. After the criteria matches a firewall policy rule, the FortiOS kernel applies the action configured on the security policy to the application traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



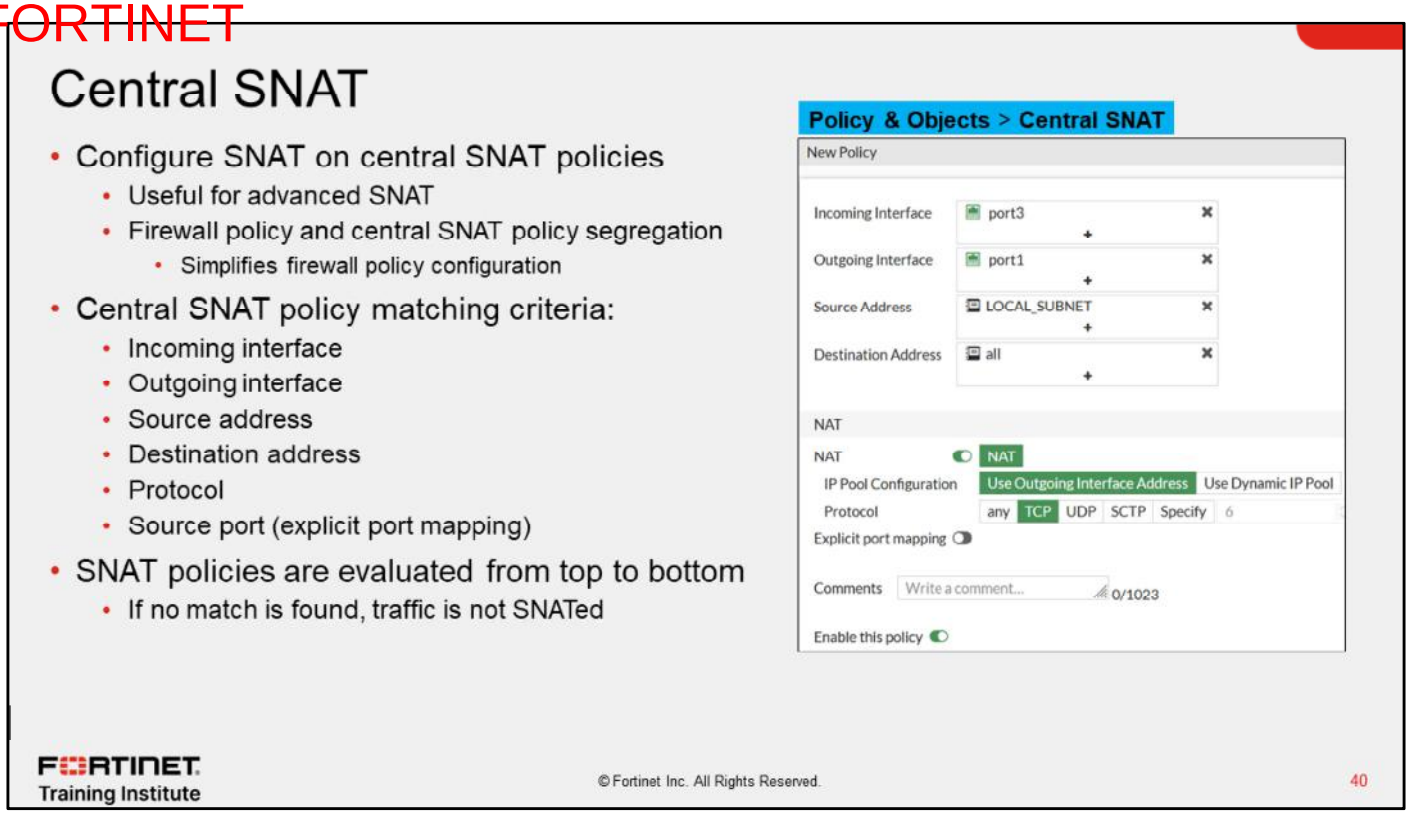
You must have a matching central SNAT policy in NGFW policy-based mode to be able to pass traffic. FortiGate applies NAT on the traffic based on the criteria defined in the central SNAT policy.

It is extremely important to arrange security policies in **Policy & Objects**, so that the more specific policies are located at the top to ensure proper use of application control.

A default **SSL Inspection & Authentication** policy inspects traffic accepted by any of the security firewalls, and by using the **certificate-inspection** SSL inspection profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you enable central NAT, you configure SNAT on the central SNAT page on the FortiGate GUI.

The main benefit of using central NAT for SNAT is firewall policy and central SNAT policy segregation. This is particularly useful for advanced SNAT configurations comprising multiple networks and IP pools. Instead of enabling NAT and selecting IP pools on firewall policies, you configure SNAT policies for all the accepted traffic by the firewall policies. This way, you focus your firewall policy configuration on what kind of traffic to accept, and your SNAT policies on what portion of the accepted traffic to translate and the SNAT mapping to follow. The result is that you simplify your firewall policy configuration by removing the SNAT settings from it.

When you configure SNAT policies, you can configure the following matching criteria:

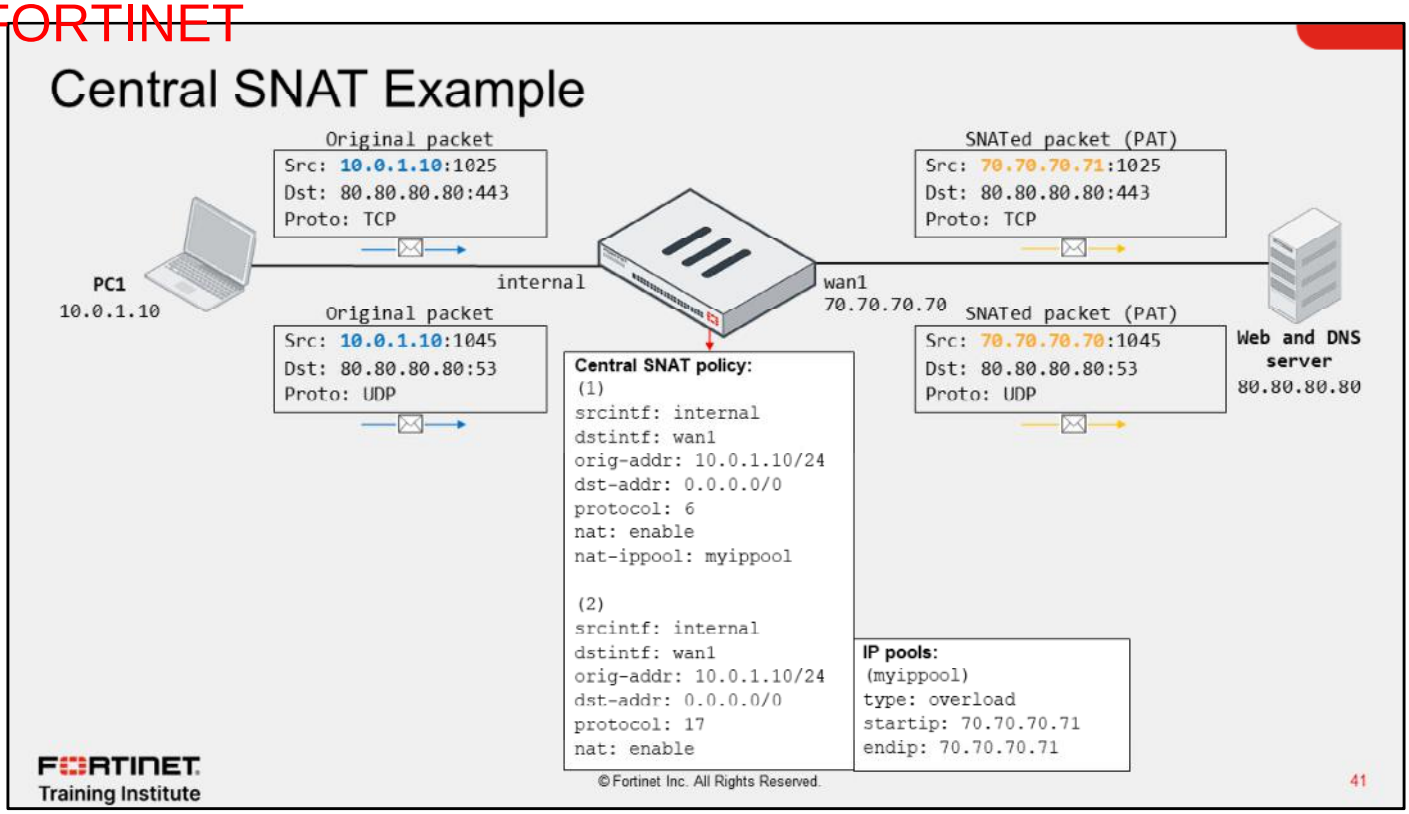
- Incoming interface
- Outgoing interface
- Source address
- Destination address
- Protocol
- Source port (explicit port mapping)

You must also indicate whether you want to perform SNAT using the outgoing interface address or an IP pool. Note that if you enable central NAT mode, FortiGate doesn't perform SNAT on traffic unless you configure the corresponding matching central SNAT policy. Similarly, if the traffic doesn't match any of the configured SNAT policies, FortiGate doesn't perform SNAT on the traffic either.

Like firewall policies, SNAT policies are processed from *top to bottom* and, if a match is found, the source address and source port are translated based on the central SNAT policy mapping settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In the example shown on this slide, PC1 (`10.0.1.10`) initiates two connections to the external server (`80.80.80.80`). The HTTPS connection matches central SNAT policy ID 1 and, therefore, the source address is translated to the IP pool address (`70.70.70.71`). The DNS connection matches central SNAT policy ID 2, which doesn't reference an IP pool. The result is that the source address of the DNS connection is translated to the external interface address (`70.70.70.70`).

Although not shown on this slide, there are firewall policies configured that accept both connections.

Now, what if PC1 initiates an ICMP connection to the server? Because there is no matching central SNAT policy, then FortiGate wouldn't perform SNAT for the ICMP connection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

NGFW Policy Matching

- Based on the configuration shown in the screenshot:
  - Facebook, Flickr, Instagram, and Pinterest application traffic is blocked by policy ID 1
  - All other Social.Media (for example, LinkedIn) application traffic is allowed by policy ID 2
  - All applications that belong to the P2P application category are blocked by policy ID 3
  - All other traffic and applications are allowed by policy ID 4

Policy & Objects > Security Policy

ID	Name	Source	Destination	Schedule	Service	Applications	Action	Security Profiles	Log
port3 → port1 4									
1	Blocking apps	all	all	always	App Default	Facebook Flickr Instagram Pinterest	DENY		All
2	Allow social media	all	all	always	App Default	Social.Media	ACCEPT	default	All
3	Blocking P2P Apps	all	all	always	App Default	P2P	DENY		Disabled
4	Allow all	all	all	always	App Default		ACCEPT	default	UTM

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

42

NGFW policy matching works using a top-to-bottom approach. You must have a specific policy above a more broad or open policy. For example, if you would like to block Facebook but allow the **Social.Media** category, you must place the policy blocking Facebook traffic above the policy allowing the **Social.Media** category.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Monitor the status of FortiGuard updates
- ✓ Use FortiManager as a local FortiGuard server
- ✓ Understand order of inspection
- ✓ Configure HTTPS inspection
- ✓ Test web filtering
- ✓ Examine web filtering statistics
- ✓ Evaluate the impact on firewall performance
- ✓ Understand hardware acceleration to improve performance
- ✓ Understand NGFW modes in application control

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

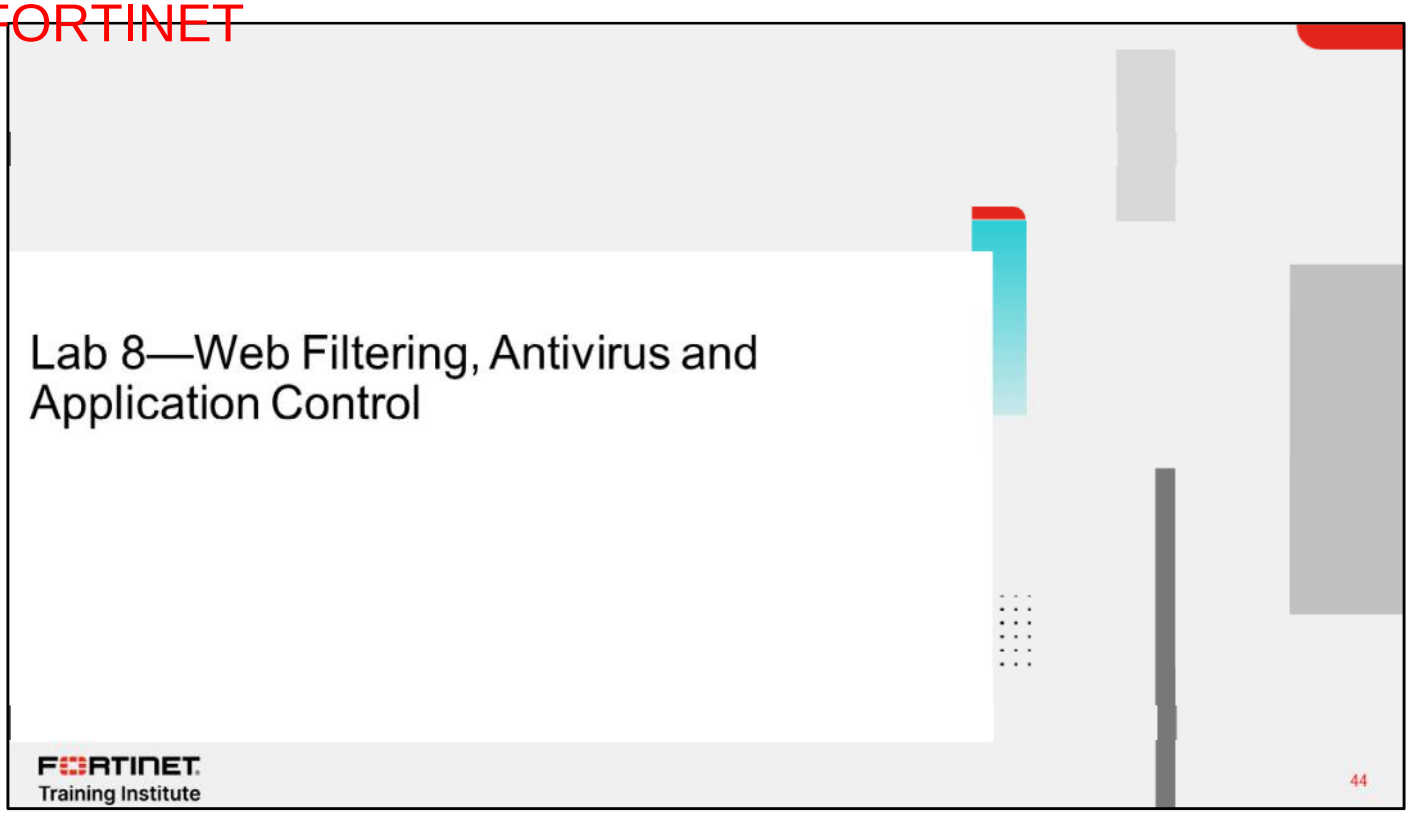
43

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

By mastering the objectives covered in this lesson, you learned how to implement and maintain web filtering, antivirus and application control on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



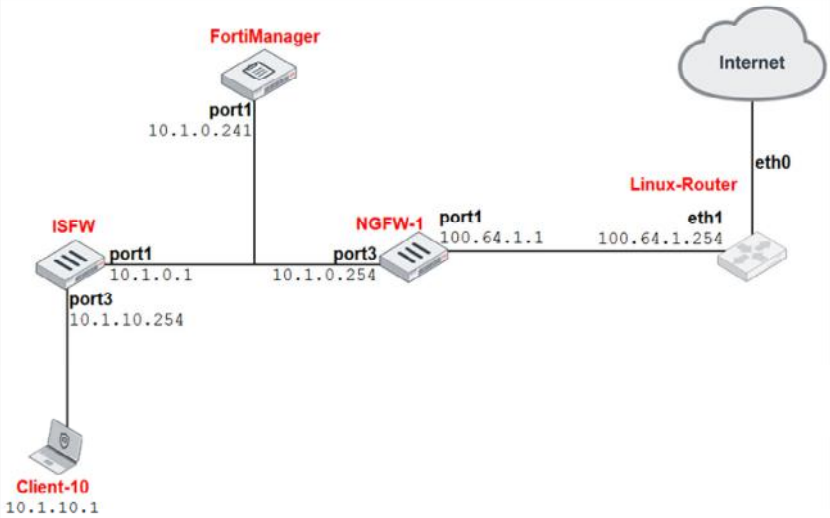
Now, you will work on *Lab 8–Web Filtering, Antivirus and Application Control*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 8—Web Filtering, Antivirus and Application Control

- On ISFW:
  - Create web filter profile
  - Create antivirus profile
  - Create firewall policy
  - Create security policy
- Analyzing:
  - Web filtering traffic
  - Antivirus traffic
  - Application traffic



FORTINET Training Institute

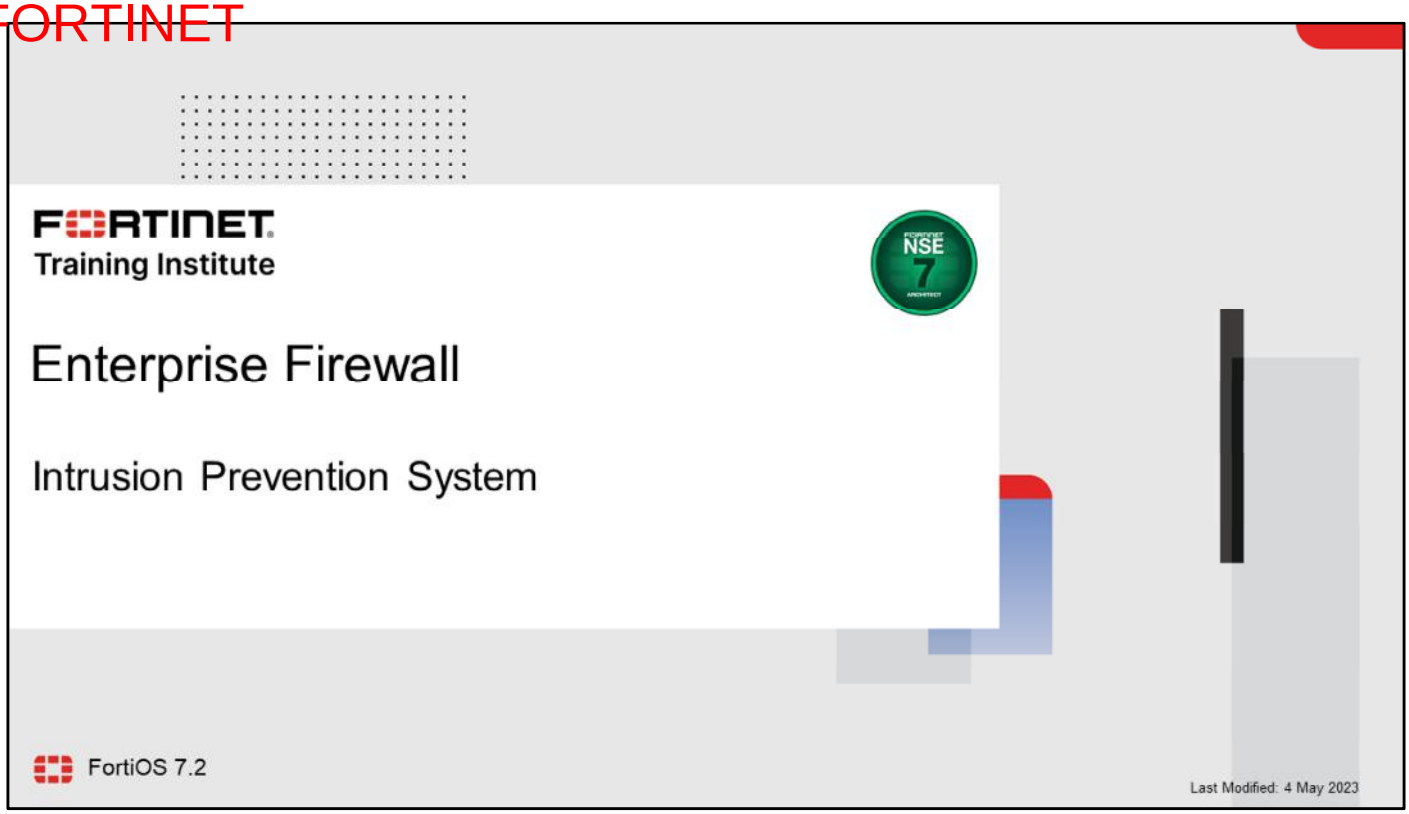
© Fortinet Inc. All Rights Reserved.

45

In this lab, you will configure web filtering, antivirus and application control using FortiManager. After that, you will test it by generating traffic from a client behind ISFW. Additionally, you will analyze a web filtering, antivirus and application control traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn about the intrusion prevention system (IPS).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Deploy IPS protection in an enterprise network
- Tune an IPS solution
- Accelerate IPS inspection using hardware offloading

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

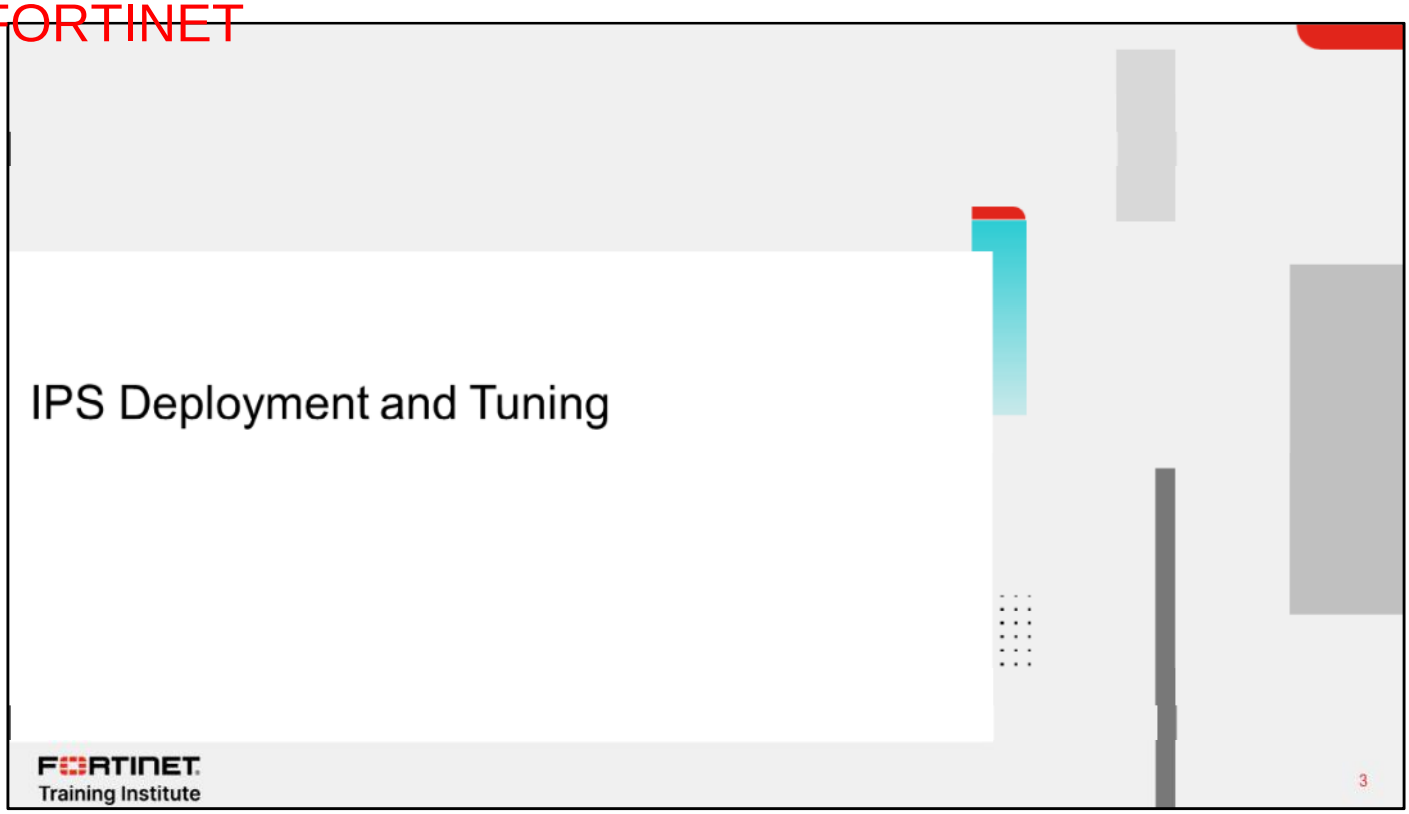
2

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

By demonstrating competence in IPS, you will be able to deploy and tune IPS in an enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

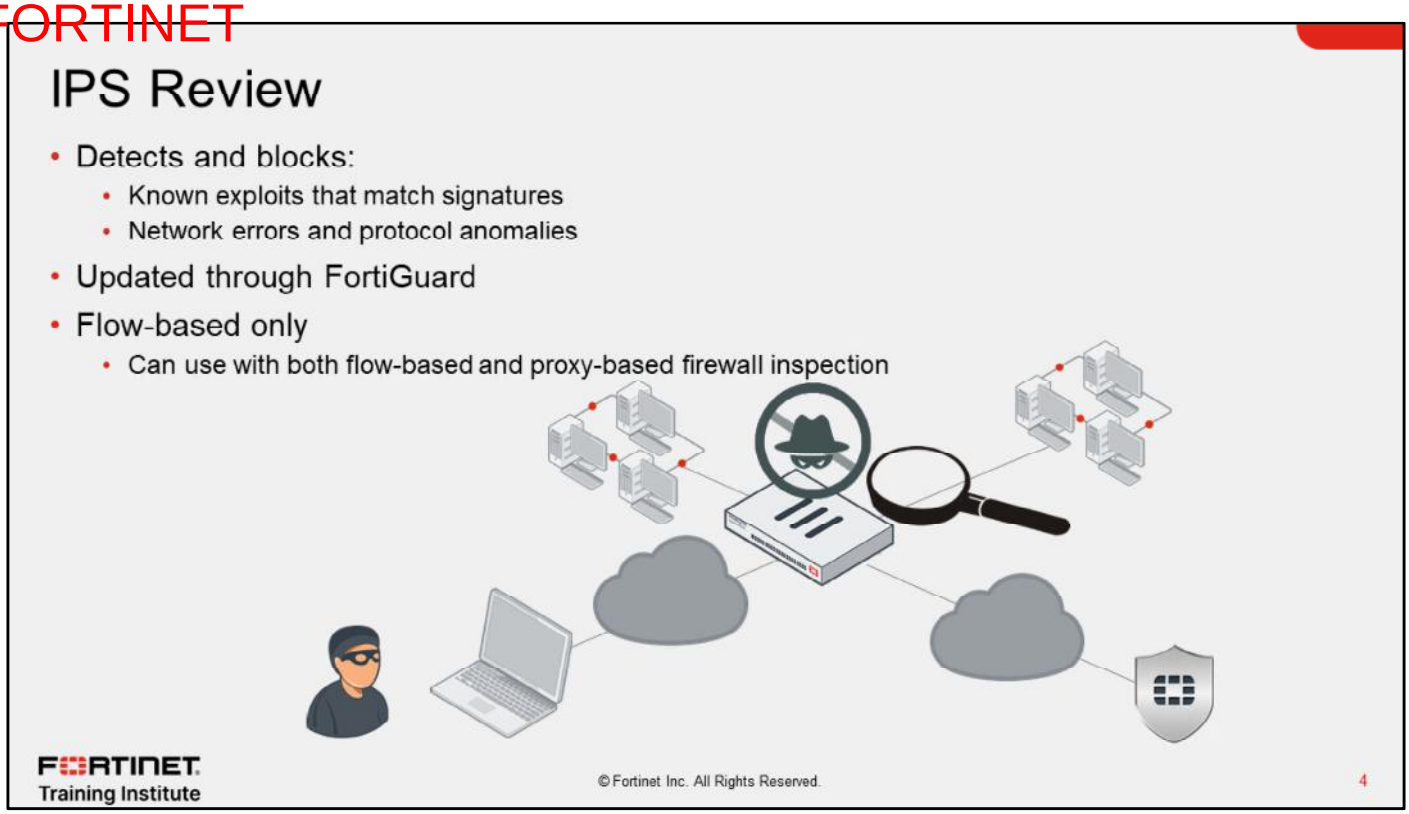
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn how to deploy and tune IPS inspection in an enterprise network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

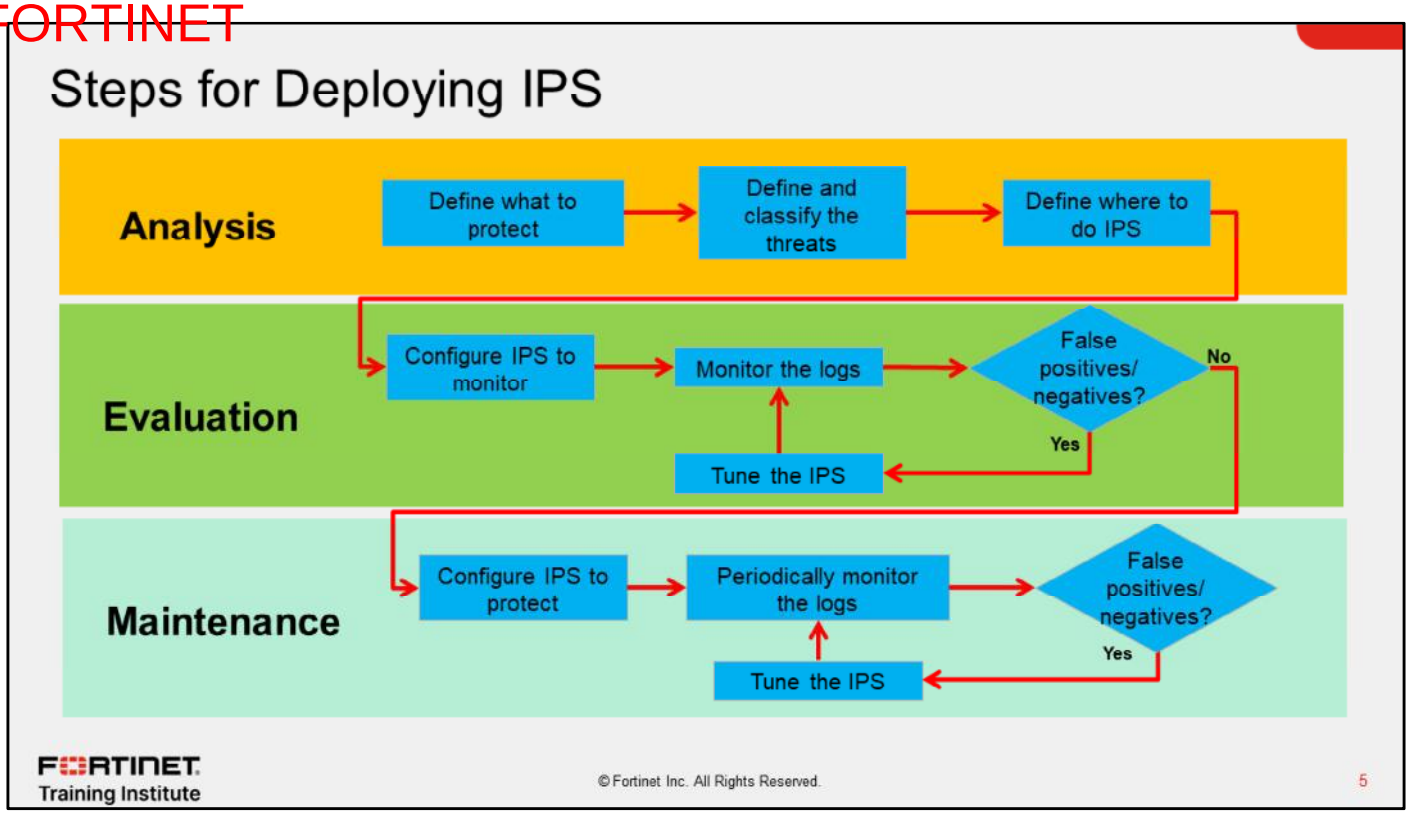


IPS uses signature databases to detect known attacks. You can also use IPS signatures to detect network errors and anomalies.

Like the antivirus signature databases, the IPS signature databases are also updated through FortiGuard. Although IPS uses flow-based techniques to identify threats but you can apply profile in both flow-based and proxy-based firewall inspection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



There is no single correct way to deploy an IPS solution. It depends greatly on the network and application requirements. However, in most cases, you will follow the steps shown on this slide.

There are usually three stages in the deployment of an IPS solution:

- **Analysis**: The administrator defines what to protect and where.
- **Evaluation**: After an initial IPS configuration, the administrator makes further adjustments based on the IPS logs. During this stage, you configure the IPS only to monitor traffic, not block it.
- **Maintenance**: After the IPS configuration is working correctly, the administrator sets IPS to protect. The administrator must continue to monitor the logs, and make further adjustments if any false positives or negatives occur.

You will learn more about each stage in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Identify What to Protect

- Don't set unrealistic expectations about protecting everything from the beginning
- Set priorities:
  - Start with the most business-critical services
- After you know the services to protect, you can define the threats and where to implement IPS:
  - Understand your deployment requirements
  - Classify the threats into groups

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

During the analysis stage, you must identify:
- What services to protect
- The threats to those services
- Where to enable IPS inspection

Set realistic expectations. Focus on protecting the services that need protection. Start with the most critical services, and classify the threats into groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configure IPS to Monitor

- One approach is to enable just one group of signatures at a time:
  - Start with the signatures that have more priority
  - Analyze the logs and either tune the IPS or enable another group
- Repeat until it's clear that the IPS is correctly tuned:
  - Monitor the network for one to two weeks
- You will learn about your network during this process!

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

During the evaluation stage, enable just one group of signatures at a time, starting with the more critical ones. Wait and analyze the logs. If the logs indicate any problems, fine tune the IPS configuration. After you feel comfortable with one signature group, enable IPS protection for the next group. This process can take from one to two weeks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configure the IPS to Protect

- Make the list of signatures that you set to block small and precise:
  - Minimizes false positives
  - Include the attacks that are most dangerous to critical services
- Continue to monitor IPS events:
  - IPS implementations are not *configure once and forget*
  - Tuning is an ongoing process

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

To minimize the number of false positives, make the list of signatures that you set to block small and precise. The list should include the attacks that are most dangerous to critical services.

After you deploy the IPS solution, you must continue to monitor IPS events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IPS Tuning

- Check the events that:
  - Have been generated most
  - Have high priority
- Analyze the event:
  - Who is that source IP address?
  - Who is that destination IP address?
  - What is the service being attacked?
  - What type of attack is it?

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

When you check IPS events, start with the events that have been generated the most, or have high priority.

For each event type, analyze the IP addresses, services, and type of attack. The analysis should help you identify whether the event is a genuine attack or a false positive.

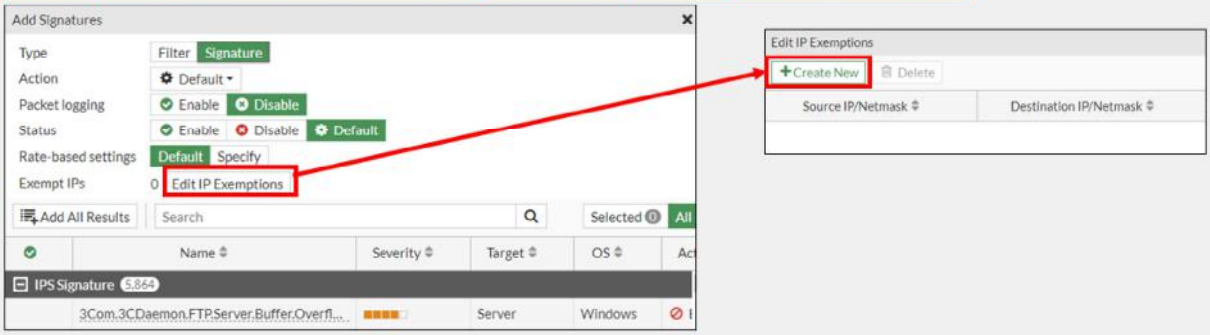
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IPS Tuning

- Eliminate as many false positives as possible
- For each false positive, do one of the following to fix the problem:
  - Make changes to the source or destination
  - Create exemptions
  - Adjust the thresholds (for the case of rate-based signatures)

Security Profiles > Intrusion Prevention > [profile-name] > IPS Signatures and Filters



FORTINET Training Institute

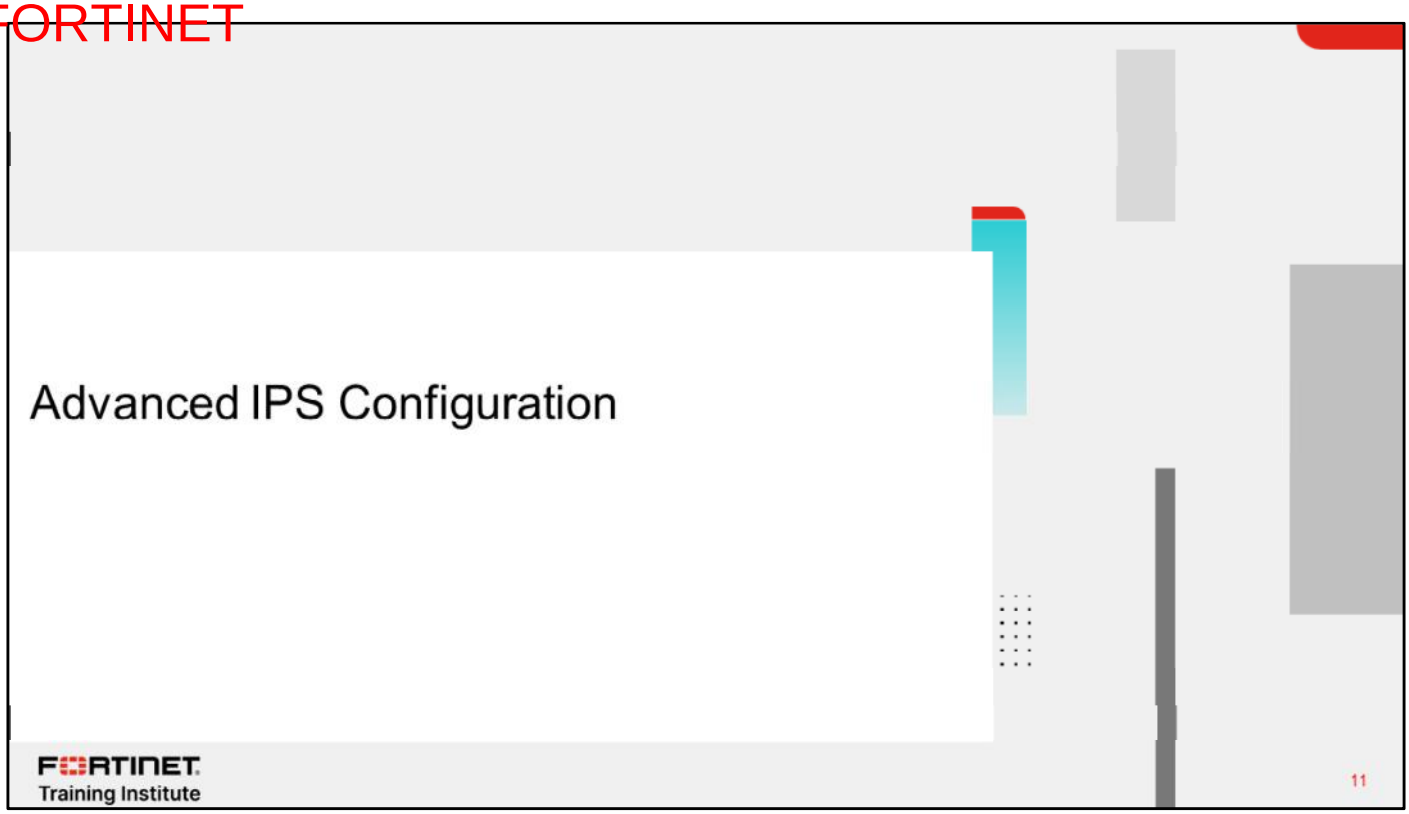
© Fortinet Inc. All Rights Reserved.

10

Eliminate as many false positives as possible. For each false positive, try to fix the problem by making changes in either the source or destination of the traffic first. You can also use IPS exemptions on the IPS profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn about advanced IPS configuration settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Global IPS Configuration

- Affects IPS engine operations for the whole FortiGate device
- The default values work well in most cases
- The most commonly used options are:

```
# config ips global
      set fail-open {enable | disable}
      set socket-size <ips_buffer_size>
      set traffic-submit {enable | disable}
      ...
  end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

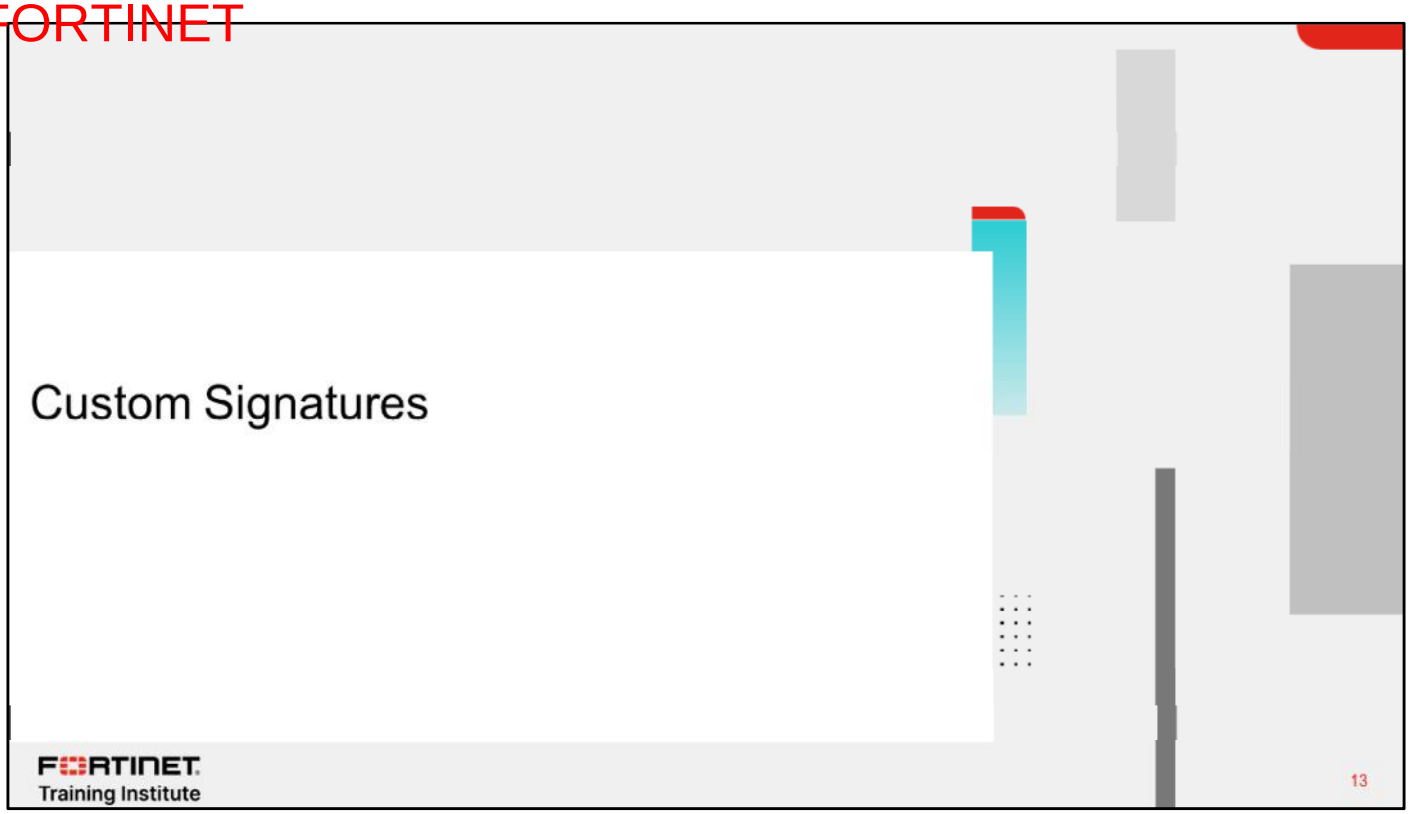
12

The global IPS configuration settings affect the IPS engine operations for the whole FortiGate device. Most of the time, you don't need to modify these values because the default ones work well in most scenarios. However, under certain circumstances, changes to these settings may be beneficial.

By default, `set fail-open` setting is set as disable and IPS traffic is blocked when the IPS buffer is full. You change the setting to enable to allow traffic. The default socket size value depends on the available memory on the device. The `traffic-submit` option allows FortiGate to submit attack data to FortiGuard, and it is disabled by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

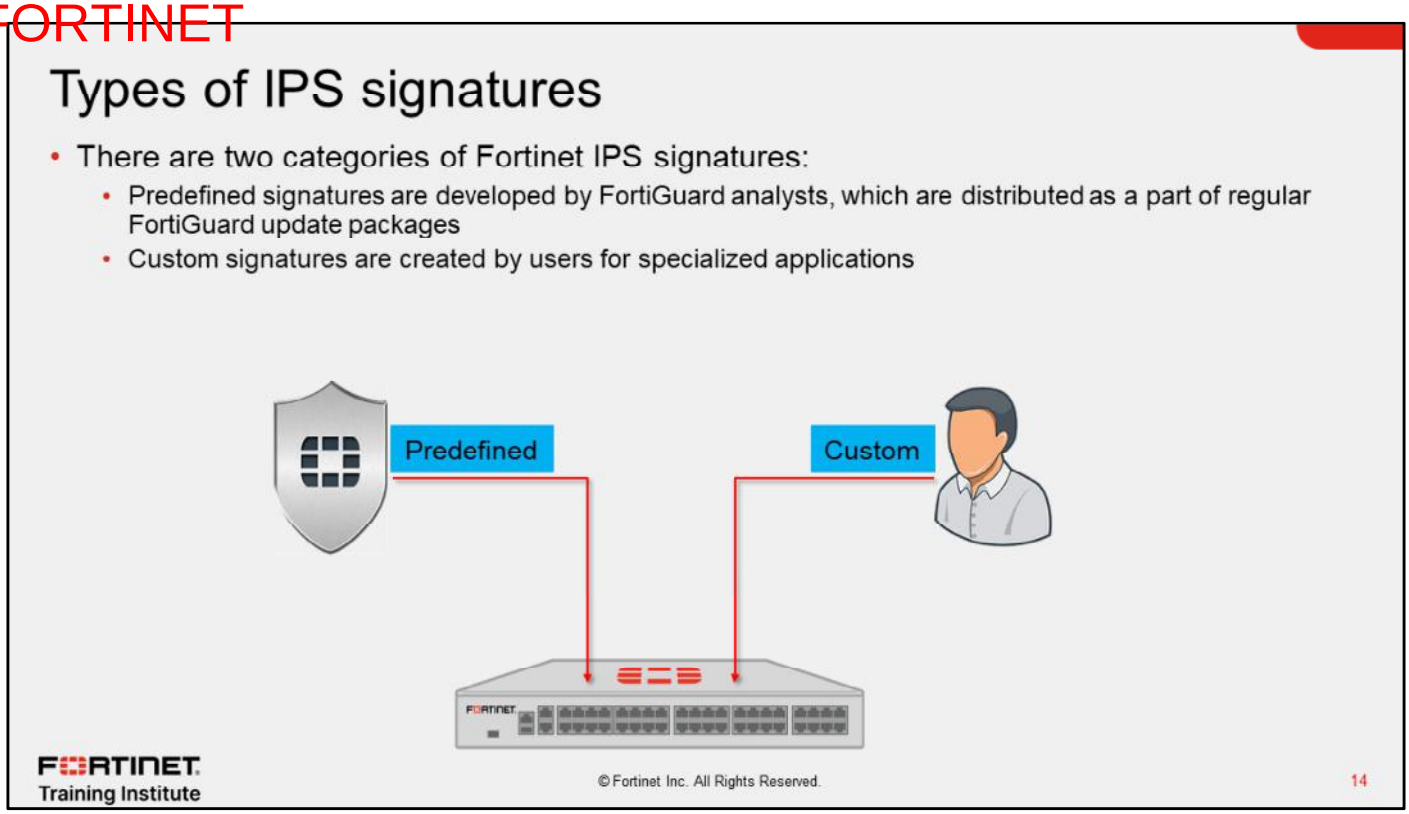
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn how to create custom signatures.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



There are two categories of Fortinet IPS signatures:

- Predefined signatures that are developed by FortiGuard analysts, which are distributed as a part of regular FortiGuard update packages
- Custom signatures that are created by users for specialized applications

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Syntax

- A custom signature is made up of a type header and a series of option and value pairs

Header Option Value

```
F-SBID (--KEYWORD VALUE;)
```

All custom signatures require a header of `F-SBID`

An option starts with "--", and identifies a parameter

Followed by a value (if any) of the parameter that will match the signature

- You must enclose the string of option and value pairs in parentheses
- Keywords are case insensitive
- Values are case sensitive

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

A custom signature is made up of a type header, and a series of option and value pairs.

All custom signatures require a header of `F-SBID`. An option starts with "--", followed by the option name, and, sometimes, a value. Some options don't require a value.
You must enclose the string of option and value pairs in parentheses. Also, keywords are case insensitive and values are case sensitive.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Syntax

- You can include multiple options in the rule by separating the options with a semicolon followed by a space

```
F-SBID(--KEYWORD1 VALUE1; --KEYWORD2
VALUE2; ............. --KEYWORDn VALUEn)
```

- The maximum length for user-created rules is 1024 bytes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

You can include multiple options in the rule by separating them with a semicolon. The maximum length is 1024 bytes for custom signatures and 4096 bytes for predefined signatures.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Option Types

```
F-SBID(--KEYWORD VALUE;)
```

- The options used in the IPS signatures are divided into five categories based on their purpose
- There are many different options available within these categories
- You can reference a complete list of options in the *Custom IPS and Application Control Signature Syntax Guide*

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

Now you'll learn about supported option types. The options are divided into five categories based on their purpose.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Basic Options

```
F-SBID(--KEYWORD VALUE;)
```

- All signatures include:
  - `--name`: Signature name that is displayed in the GUI and the CLI (required)
  - `--service`: Specifies the session type associated with a packet (required)
  - `--protocol`: Specifies the type of protocol associated with a signature (optional)
  - `--severity`: Specifies the severity of the vulnerability that a signature covers (optional)
  - `--description`: Specifies signature description (optional)
- Example:

```
F-SBID(--name "Block.HTTP.POST"; --protocol tcp; --service HTTP;
--flow from_client; --pattern "POST"; --context uri; --within
5,context; )
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

When creating a custom signature, you must define the required options, which are name and service.

The signature name must be unique for each custom signature. The maximum length of a signature name is 64 characters.

The service option specifies the session type, such as HTTP or FTP. *You can use the service keyword only once in a signature*. If a signature has neither a *service* keyword nor a *port* keyword, it will be added to all service trees including the *unknown_service* tree.

The protocol option specifies the type of protocol that is associated with the signature. In the example on this slide, TCP is specified in the signature. You can also specify protocols by their protocol numbers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Protocol Options

```
F-SBID(--KEYWORD VALUE;)
```

- Protocol-related options:
  - Used to match different protocol headers
- Example:

```
F-SBID(--name "Block.HTTP.POST"; --protocol tcp; --service HTTP;
--flow from_client; --dst_addr 10.10.10.0/24;
--pattern "POST"; --context uri; --within 5,context; )
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

Use protocol-related options to match protocol (TCP, UDP, ICMP) and IP headers. In the example on this slide, the destination subnet is specified in the IP header.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Payload Options

```
F-SBID(--KEYWORD VALUE;)
```

- Payload-related options:
  - Used to match the packet payload
- Example:

```
F-SBID(--name "Block.HTTP.POST"; --protocol tcp; --service HTTP;
--flow from_client; --pattern "POST"; --context uri; --within
5,context; )
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

Use payload-related options to match portions of the packet payload.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Special Options

```
F-SBID(--KEYWORD VALUE;)
```

- Special options:
  - Used for all other purposes
- Example:

```
F-SBID( --name "Ultraviewer.Custom"; --protocol tcp; --service
ssl; --flow from_client; --pattern "ultraviewer"; --context
host; --app_cat 7;)
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

Use special options for various purposes for more granular filtering.

Similar to the service option, the flow option can appear only once in the signature because it defines flow direction of the detection packet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Application Options

```
F-SBID(--KEYWORD VALUE;)
```

- Application options:
  - `--app_cat`: Specifies the category of the application signature (Required)
  - Used for all other purposes
- Example:

```
F-SBID( --name "Ultraviewer.Custom"; --protocol tcp; --service
ssl; --flow from_client; --pattern "ultraviewer"; --context
host; --app_cat 7;)
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Use application options for various purposes for more granular filtering.

In this example, specifying the application category will result in this signature appearing under application control instead of IPS configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Tips for Creating Custom Signatures

- Before creating a custom signature, gather as many samples of the traffic as possible:
  - It will help identify patterns, for example, source ports, destination ports, specific strings in the body, and so on
- Most of the time, the protocol-related patterns are obvious
- Try to identify payload-related patterns in the captures
- Use payload-related and special options to ensure the least number of false positive or negative matches

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

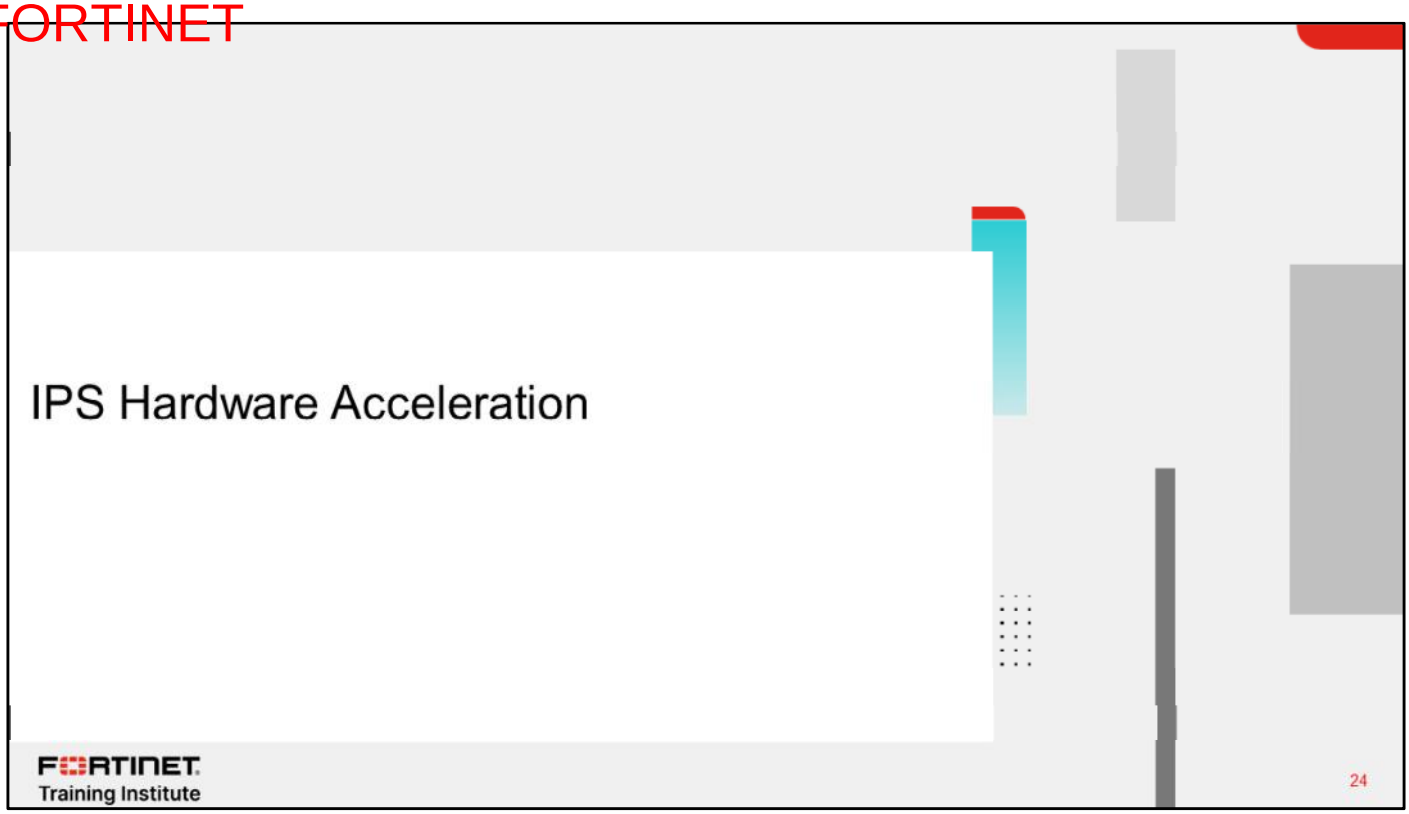
23

If you are planning to create a custom signature, gather as many samples of the traffic as possible. Good samples help you to identify patterns, for example, source ports, destination ports, specific string patterns in the packet payload, and so on.

Try to match payload patterns in addition to protocol patterns, because payload patterns tend to be unique to the specific traffic that you want to match. In this way, you might be able to reduce the number of false positives for the custom signature.

Vouchers & Dumps are Available | WhatsApp +201224560923

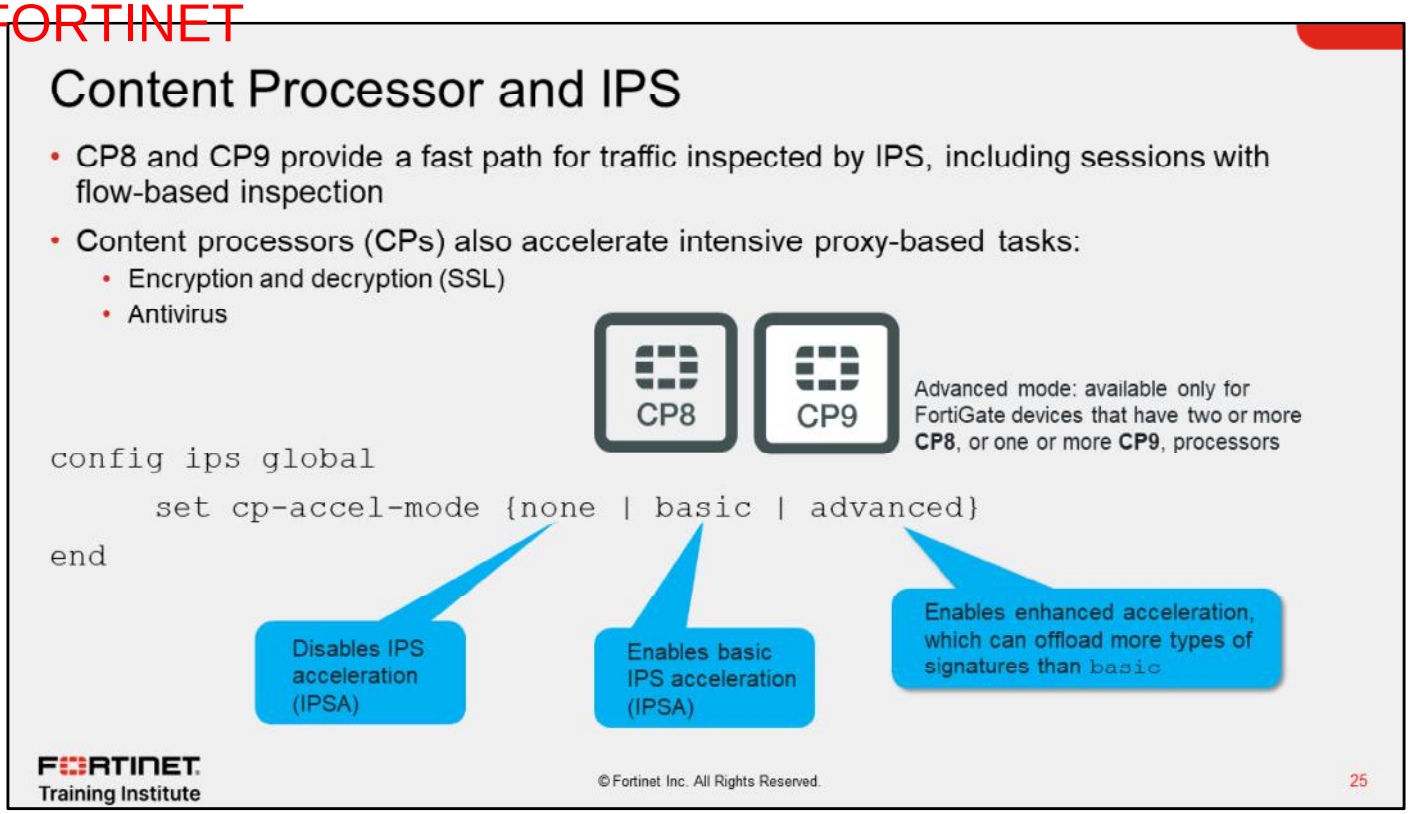
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about hardware acceleration options for IPS inspection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The CP is a co-processor for the CPU. It accelerates many common resource-intensive, security-related processes.

Since the very first FortiGate model, Fortinet has included a CP in the design. The CP works at the system level.

CP8 and CP9 provide a fast path for traffic inspected by IPS, including sessions with flow-based inspection.

CP processors also accelerate intensive proxy-based tasks:
- Encryption and decryption (SSL)
- Antivirus

Most of the time, you don't need to modify these values because the default ones work well in most scenarios.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Network Processor and IPS

- Pre-IPS anomaly filtering and logging
- NP6 leverages NTurbo:
  - Increases the IPS processing performance by distributing the cost of processing to different CPU cores
  - Fast path for traffic inspected by IPS, including sessions with flow-based inspection
- Network processors (NPs) also offload:
  - Packet forwarding
  - IPsec phase 2 and hashing

```
config ips global
  set np-accel-mode {none | basic}
end
```

Disables NTurbo/IPS offloading

Enables NTurbo/IPS offloading

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

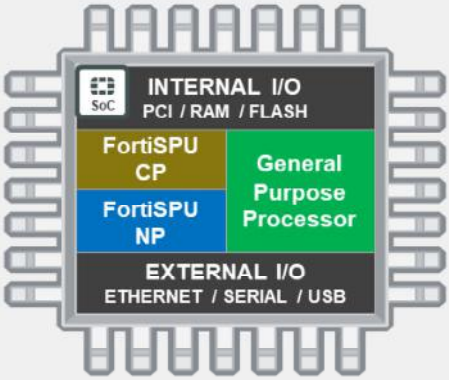
Network processors (NPs) provide the following features:
- Pre-IPS anomaly filtering and logging
- Packet forwarding
- IPsec encryption and decryption

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System on a Chip and IPS

- SPU that includes entire microprocessors, memory blocks, flash memory, and other large building blocks
- Fortinet's system on a chip (SoC) unifies:
  - FortiSPU-NP and FortiSPU-CP
  - General purpose CPU
  - Memories
  - Network interfaces
- SoC4 and SoC3 platforms include NTurbo:
  - Provides a fast path for traffic inspected by IPS



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

SoC combines NPs, CPs, and general-purpose CPU into a single chip. It accelerates IPS-inspected traffic.

SoC is found in desktop or small office models.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Tune IPS configuration
- ✓ Perform advanced IPS configuration
- ✓ Configure custom signatures
- ✓ Configure IPS inspection acceleration

FORTINET Training Institute

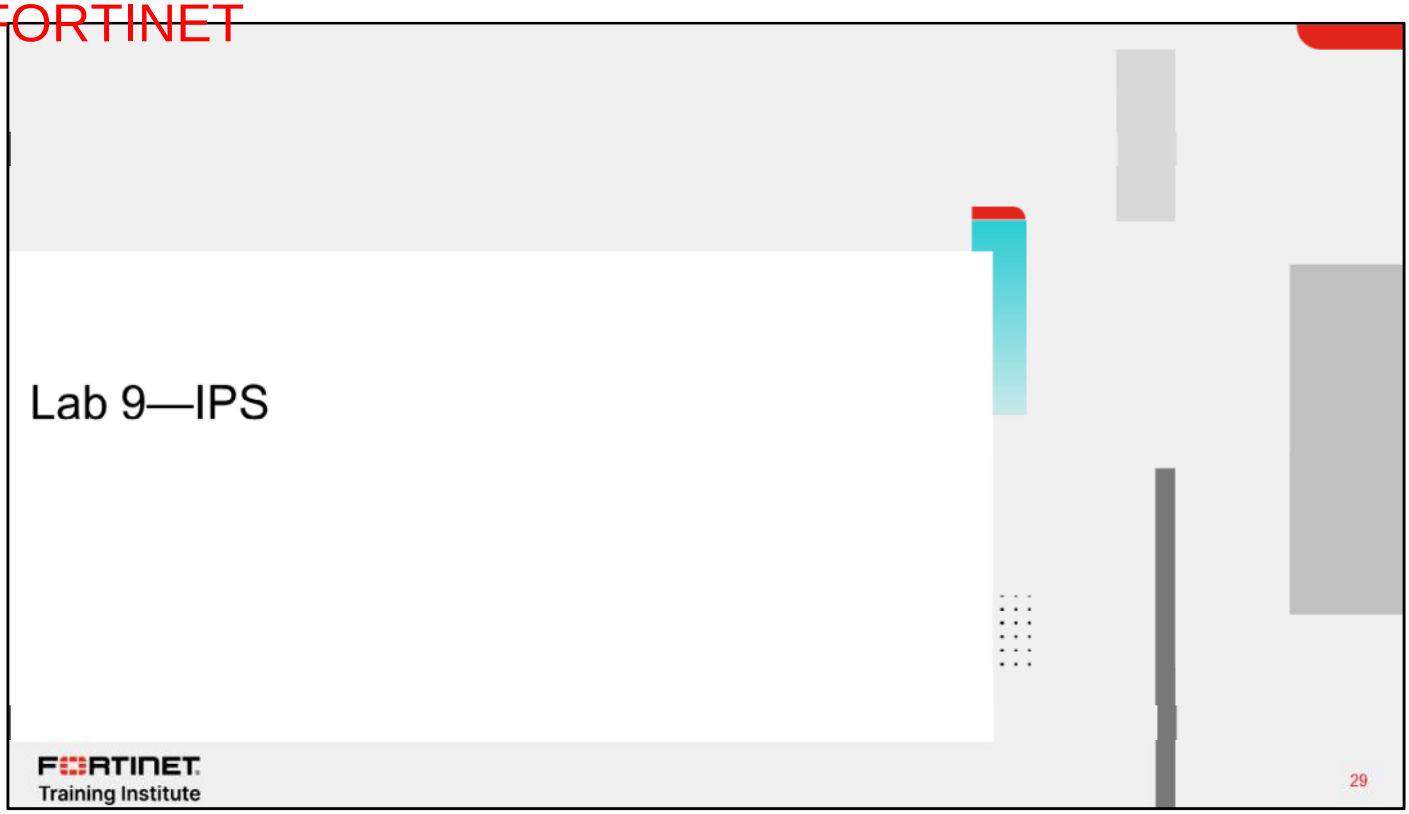
© Fortinet Inc. All Rights Reserved.

28

This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to tune, configure, and troubleshoot IPS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



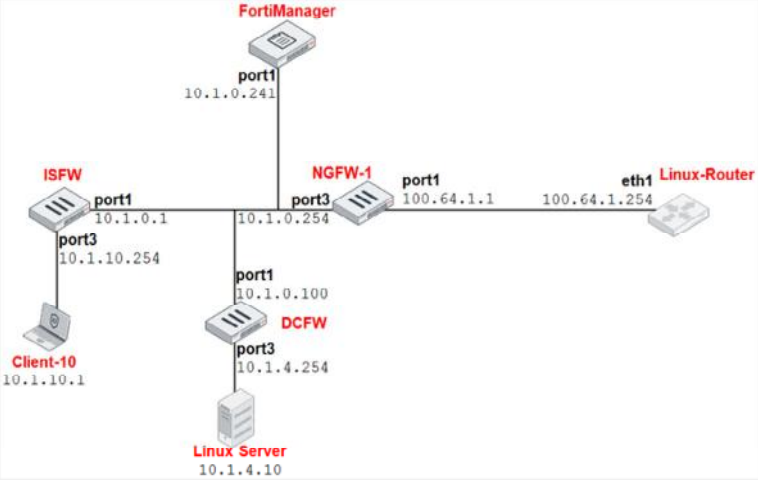
Now, you will work on *Lab 9–IPS*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 9—IPS

- IPS configuration:
  - On DCFW:
    - Add an IPS profile
    - Apply the IPS to the inbound firewall policy
  - On NGFW-1:
    - Add a VIP
    - Add an inbound firewall policy
- IPS custom signature



FORTINET Training Institute

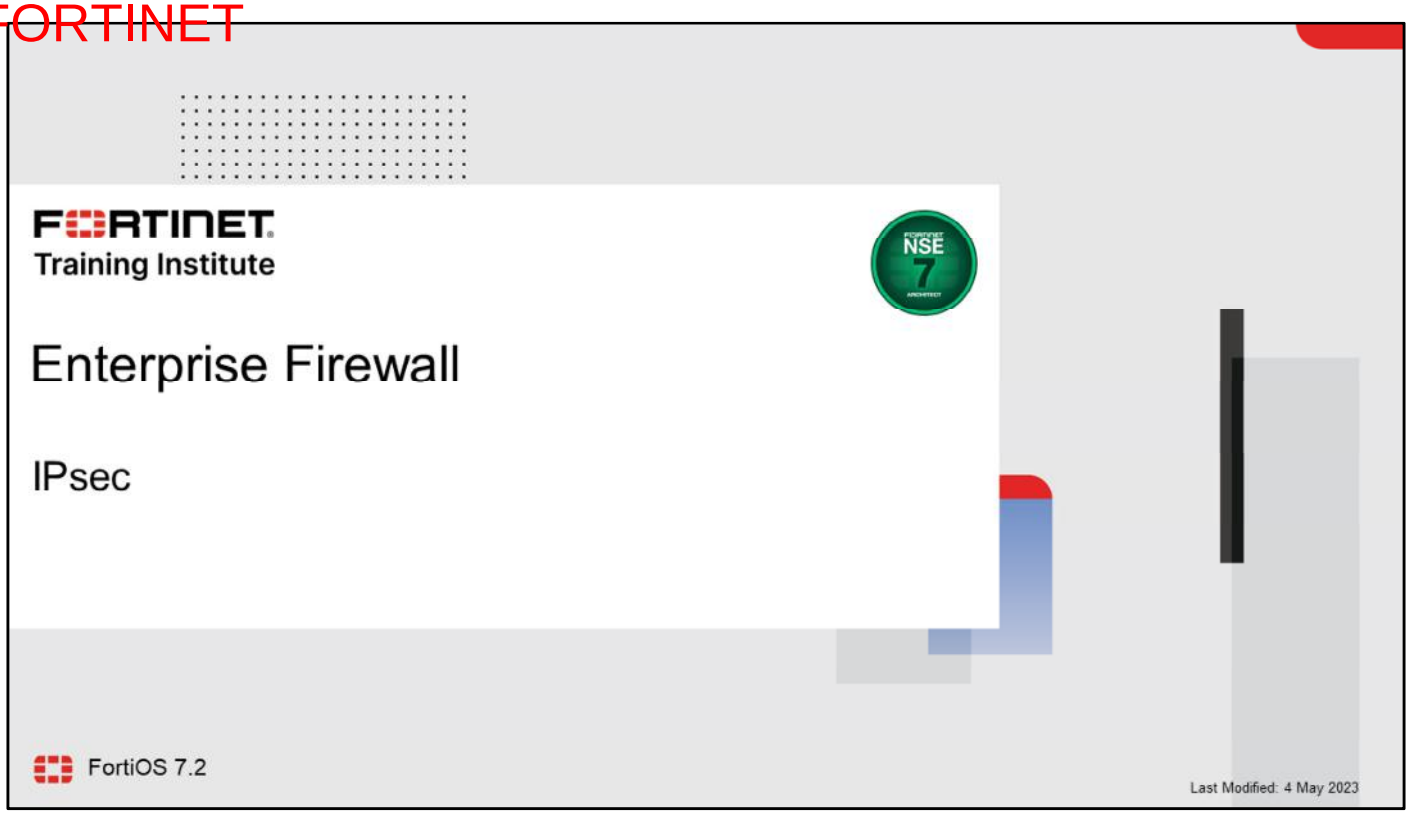
© Fortinet Inc. All Rights Reserved.

30

In this lab, you will configure FortiGate to protect a web server using IPS inspection. Then, you will test the configuration by generating suspicious traffic from outside to the server. Additionally, you will use the information gathered by the built-in sniffer to write a custom IPS signature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn about IPsec.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Review IPsec
- Review IKE
- Route IPsec traffic
- Configure remote IPsec sites with overlapping IP subnets
- Verify that IPsec encryption and decryption is offloaded to hardware
- Monitor the status of an IPsec VPN

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

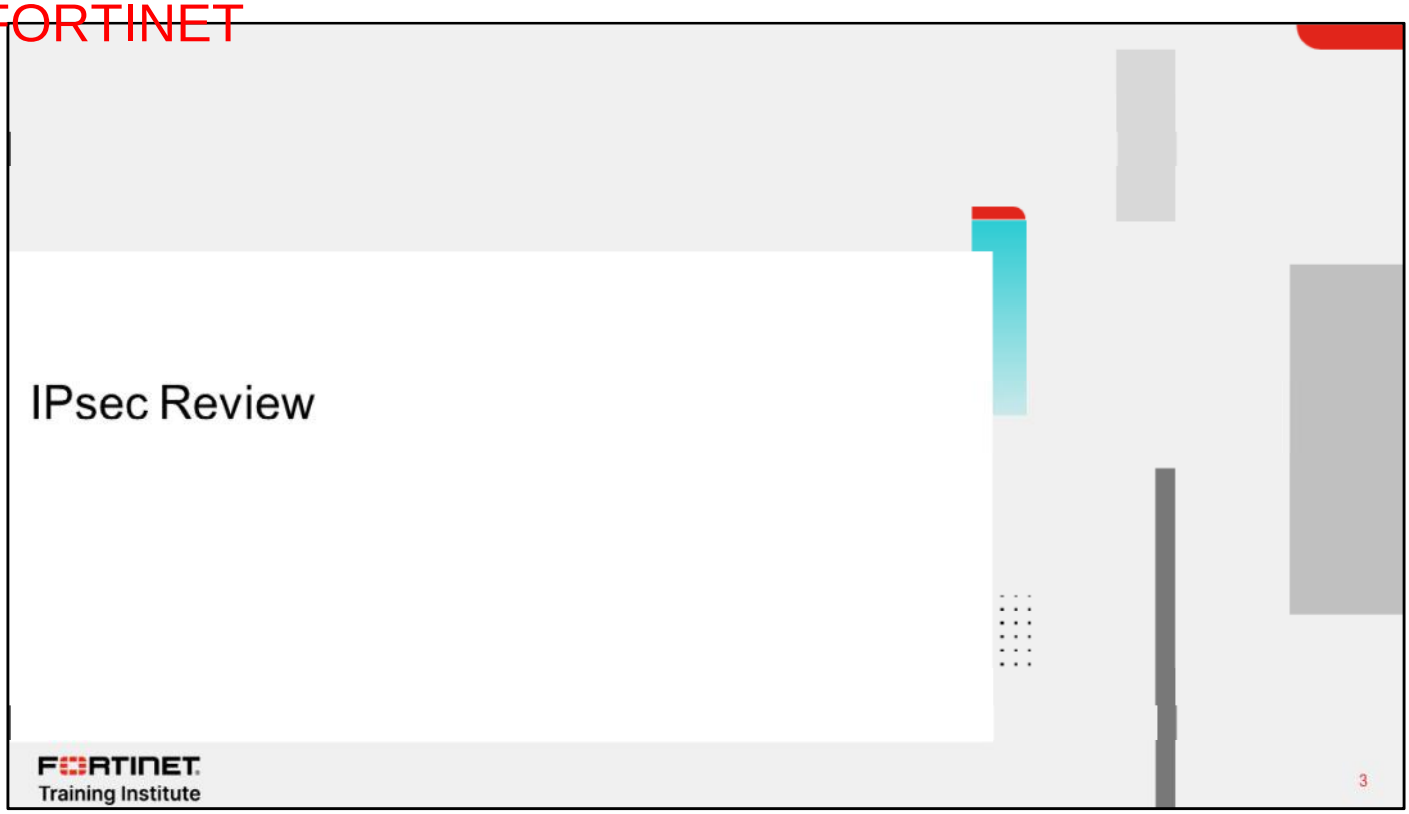
2

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

By demonstrating competence in IPsec, you will be able to configure IPsec using the FortiManager VPN manager, troubleshoot IPsec problems using debug flow, verify IPsec encryption and decryption behavior, capture IPsec traffic, and monitor the IPsec VPN status.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will review some IPsec concepts from the *FortiGate Infrastructure* course.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IPsec Review

- Suite of protocols for securing IP communications
- Authenticates and/or encrypts packets:
  - Internet Key Exchange (IKE)
  - Encapsulating Security Payload (ESP)
    - Provides both data integrity and encryption
- For NAT traversal, ESP is UDP-encapsulated

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

IPsec is a suite of protocols for authenticating and encrypting traffic between two peers. The two most-used protocols in the suite are:

- IKE, which does the handshake, tunnel maintenance, and disconnection
- ESP, which ensures data integrity and encryption

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKE Review

- Negotiates private keys, authentication, 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
- IKEv1 uses two distinct phases:
  - Phase 1: main or aggressive mode
  - Phase 2: quick mode
- IKEv2 has two initial phases of negotiation (known in IKEv1 as phase1)
  - There are no aggressive or main modes
  - IKE_SA_INIT is the initial exchange
  - IKE_AUTH exchange is used to authenticate the remote peer

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

IKE negotiates the private keys, authentications, and encryption that FortiGate uses to create an IPsec tunnel. Security associations (SAs) provide the basis for building security functions into IPsec. There are two distinct phases that IKEv1 uses: phase 1 and phase 2. Phase 1 uses a single bidirectional SA, and phase 2 uses two IPsec SAs, one for each traffic direction. In IKEv2, there is no such concept as phase1 and phase2, however, the FortiOS command line interface (CLI) and web GUI are based on IKEv1 settings. Also, there are no aggressive or main modes to choose in IKEv2. In IKEv2, peers initially establish a secure channel during the initial IKE_SA_INIT exchange, then the IKE_AUTH exchange is used to authenticate the remote peer and create the first IPsec SA.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv1 and IKEv2

IKEv1	IKEv2
Initiator and responder exchange nine messages to establish a secure tunnel.	Initiator and responder exchange four messages to establish a secure tunnel.
No EAP authentication support	EAP authentication support
No asymmetric authentication support	Asymmetric authentication support
No Mobility and Multihoming Protocol (MOBIKE)	Mobility and MOBIKE support
No GCM (Galois/Counter Mode) with an encryption algorithm	GCM with an encryption algorithm support

FORTINET Training Institute

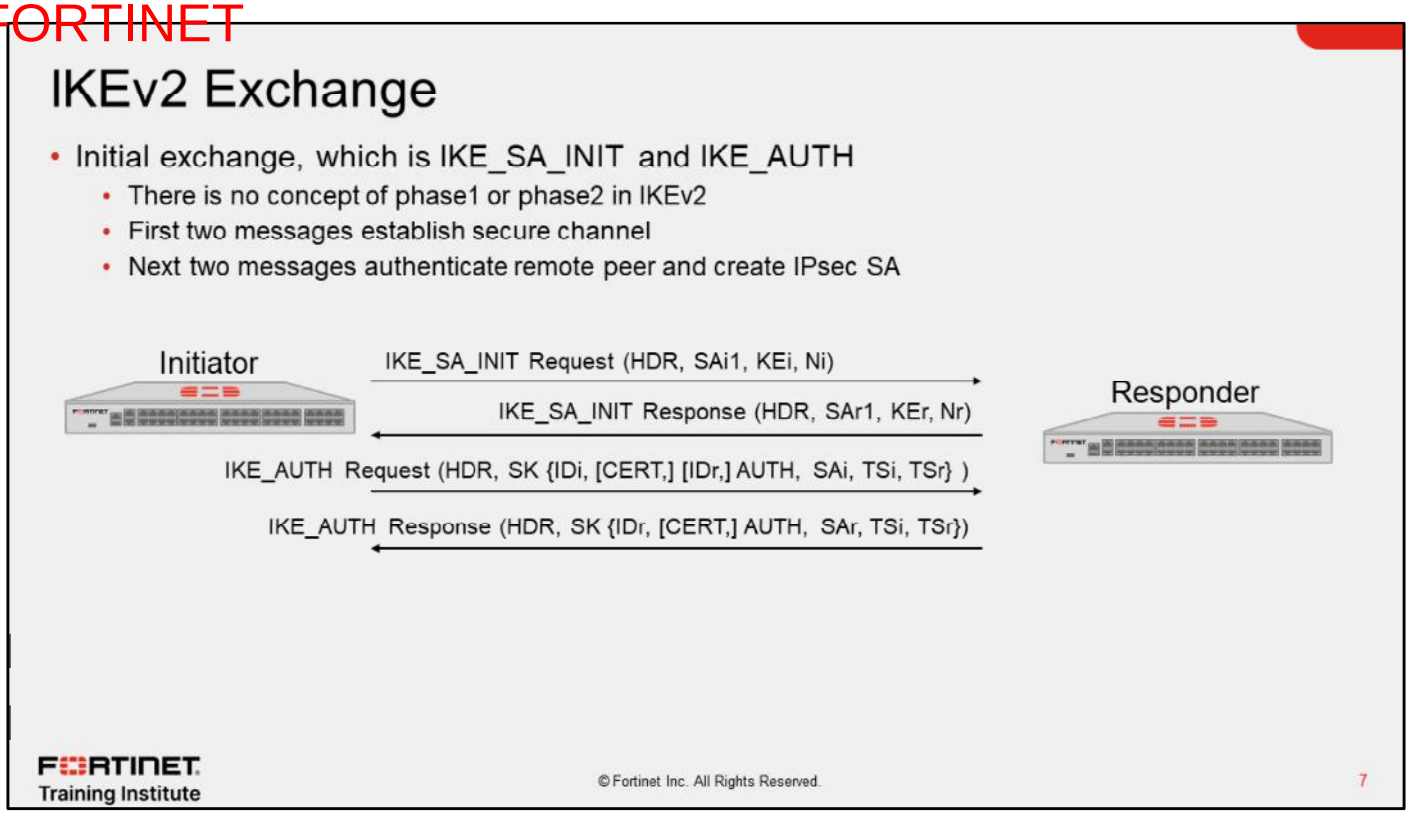
© Fortinet Inc. All Rights Reserved.

6

As shown on this slide, there are fundamental differences between IKEv1 and IKEv2. In this lesson, you will learn only about IKEv2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Now, you will review the initial IKEv2 exchange. This slide shows the initial exchange between the initiator and responder. At first, peers establish a secure channel during the initial IKE_SA_INIT exchange, then IKE_AUTH exchange is used to authenticate the remote peer and create the first IPsec SA. The IKE_SA_INIT is the first round trip of an IKEv2 initial exchange. The peers negotiate a set of cryptographic settings (SAi/SAr), exchange their Diffie-Hellman public keys (KEi/KEr), exchange random numbers (Ni/Nr), and then compute the keys used to protect all the subsequent exchanges, such as IKE_AUTH, CREATE_CHILD_SA, and INFORMATIONAL.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv2 Exchange (Contd)

- IKE_SA_INIT
  - Negotiate the security settings to protect IKE traffic
  - Usually takes one round trip
  - Two round trips are required, if responder requests another KE with invalid payload notification or DoS protection (cookie mechanism)
- IKE_AUTH
  - Authentication of the two IKE endpoints
  - Supported authentication methods are pre-shared keys, signature (certificate), and Extensible Authentication Protocol (EAP)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

In a normal exchange, IKE_SA_INIT takes a round trip. However, if the responder requests another key exchange with invalid payload notification or DoS protection kicks in, it extends to two round trips. IKE_AUTH (authentication) takes place after SA_INIT and is the last stage of the initial exchange. It is protected by the cryptographic algorithms and the keys from the SA_INIT. There are three types of authentication methods available in IKEv2.

IKEv2 has three types of exchange: initial exchanges, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange. By default, a piggyback child (IPsec) SA is negotiated along with the IKEv2 SA during IKE_AUTH. If additional IPsec SAs are needed, for example, multiple FortiOS phase2s are configured, they are negotiated during subsequent CREATE_CHILD_SA exchanges. One CREATE_CHILD_SA exchange creates one pair of IPsec SAs. IKEv2 also uses the CREATE_CHILD_SA exchange to rekey IKE SAs and child SAs. IKEv2 uses the INFORMATIONAL exchange to convey control messages about errors and notifications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv2 Exchange (Contd)

- CREATE_CHILD_SA exchange
  - Create a new or rekey an existing child SA (PFS can be enforced)
  - Rekey an IKE SA
- INFORMATIONAL exchange
  - Convey control messages (Notification, Delete, Configuration) between the IKE endpoints

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

IKEv2 has three types of exchange: initial exchange, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange. By default, a piggyback child (IPsec) SA is negotiated along with the IKEv2 SA during IKE_AUTH. If additional IPsec SAs are needed, for example, multiple FortiOS phase2s are configured, they are negotiated during subsequent CREATE_CHILD_SA exchanges. One CREATE_CHILD_SA exchange creates one pair of IPsec SAs. Based on the IKEv2 design, no Diffie-Hellman public key (KE) is exchanged during an IKE_AUTH exchange. It implies that PFS cannot be enforced for the piggyback child SA negotiated during IKE_AUTH. Diffie-Hellman public keys are only exchanged in CREATE_CHILD_SA. It is the only Child SA negotiation exchange that enforces PFS. The IKEv2 also uses the CREATE_CHILD_SA exchange to rekey IKE SAs and Child SAs. IKEv2 uses the INFORMATIONAL exchange to convey control messages about errors and notifications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv2 Fragmentation

- IKEv2 uses UDP, and messages are small
- When the IKE message size exceeds the path MTU, it gets fragmented at the IP level
  - During the IKE_AUTH exchange
- Most of the NAT devices do not allow IP fragments to pass through
- It blocks IKE communication

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

If fragmentation occurs at the IP layer, during the IKEv2 connection, it is possible that payload sizes may exceed the IP Maximum Transmission Unit (MTU) and packets get fragmented. So, some network devices do not permit the pass-through of small UDP fragments in case they are part of a fragmentation attack. The issue is that if not all the UDP fragments are passed through, the IKE negotiation fails because the intended recipient cannot reconstruct the original IKE packet. IKE SA cannot be established. So, the solution is to fragment packets at the IKE layer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv2 Fragmentation (Contd)

- Based on RFC 7383, the solution is to perform fragmentation by IKEv2
- IP datagram is small enough so no fragmentation at the IP level
- Only some IKEv2 packets are considered fragmentable: AUTH, CREATE_CHILD_SA, and some INFORMATIONAL
- Maximum number of IKEv2 fragments = 64 (for reassembly)
- Reassembly timeout = 15 sec (same as IKEv1)

```
config vpn ipsec phase1(-interface)
edit …
set ike-version 2
set fragmentation { enable* | disable }
set fragmentation-mtu <> // max size for IKEv2 frag packets: default=1200 (range=500-16000)
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

With IKEv2 fragmentation support, the fragmentation occurs at the IKE layer instead of the IP layer. So, with fragmentation occurring at the IKE layer, routers and firewalls do not block packets at the IP layer, and there are no issues with IPsec communication. It is important to know that during the IKEv2 fragmentation, only certain IKEv2 packets are considered as fragmentable. The maximum number of IKEv2 fragments are 64, and the reassembly timeout is 15 seconds. You can use the FortiOS CLI shown on this slide to configure the fragmentation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv2 Fragmentation—Sender Side

- The IKEv2 AUTH message is fragmented
- The AUTH message is bigger than fragmentation-mtu

```
ike 0:toFG2:4: initiator preparing AUTH msg
ike 0:toFG2:4: local cert, subject='test', issuer='CA_VPN'
ike 0:toFG2:4: local CA cert, subject='CA_VPN', issuer='CA_root'
ike 0:toFG2:4: local CA cert, subject='CA_root', issuer='CA_root'
ike 0:toFG2:4: sending INITIAL-CONTACT
ike 0:toFG2:4: splitting payload len=6433 into 7 fragments
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=1136, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=1136, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=1136, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=1136, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=1136, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=1136, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
ike 0:toFG2:4: sent IKE msg (AUTH): 198.51.100.1:500->203.0.113.1:500, len=160, id=3585ea056c0e91e6/836ac8b12dd87897:00000001
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

The example shown on the slide is IKEv2 AUTH message fragmentation on the sender side. The AUTH message is bigger than the fragmentation-mtu.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IKEv2 Fragmentation—Receiver Side

- Receiver side reassembled fragmented message

```
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=1136
ike 0:toFG1:3: encrypted fragment 1 of 7 queued
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=1136
ike 0:toFG1:3: encrypted fragment 2 of 7 queued
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=1136
ike 0:toFG1:3: encrypted fragment 3 of 7 queued
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=1136
ike 0:toFG1:3: encrypted fragment 4 of 7 queued
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=1136
ike 0:toFG1:3: encrypted fragment 5 of 7 queued
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=1136
ike 0:toFG1:3: encrypted fragment 6 of 7 queued
ike 0: comes 198.51.100.1:500->203.0.113.1:500,ifindex=3....
ike 0: IKEv2 exchange=AUTH id=3585ea056c0e91e6/836ac8b12dd87897:00000001 len=160
ike 0:toFG1:3: encrypted fragment 7 of 7 queued
ike 0:toFG1:3: reassembled fragmented message
ike 0:toFG1:3: responder received AUTH msg
ike 0:toFG1:3: processing notify type INITIAL_CONTACT
<...>
```

FORTINET Training Institute

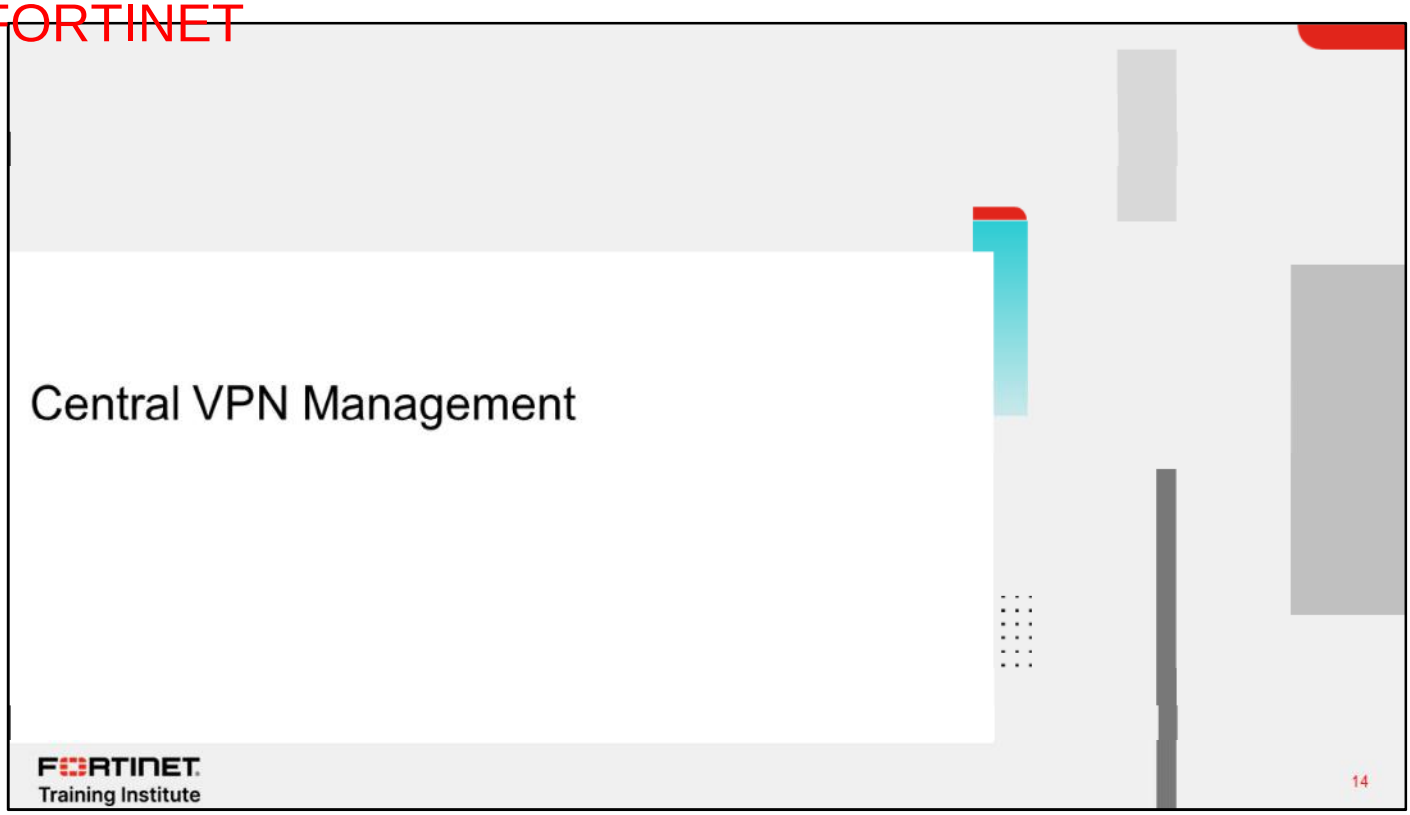
© Fortinet Inc. All Rights Reserved.

13

On the receiver side, all seven messages are successfully reassembled and show the **received AUTH msg**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure IPsec VPNs using the FortiManager VPN manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager VPN Manager

- VPN manager simplifies the administration of multiple VPNs
- You can install common IPsec VPN settings on multiple FortiGate devices at the same time
  - Settings are stored as objects and pushed to the devices as part of the policy packages
- VPN manager is enabled for each ADOM
- Steps:
  1. Create a VPN community
  2. Add gateways (members) to the community
  3. Install the VPN community and gateways configuration
  4. Add the firewall policies
  5. Install the firewall policies

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

On the VPN manager screen, you can configure IPsec VPN settings that you can install on multiple devices. The settings are stored as objects in the objects database. You push the IPsec VPN settings to one or more devices by installing a policy package. Follow these steps to configure VPNs with the VPN manager:

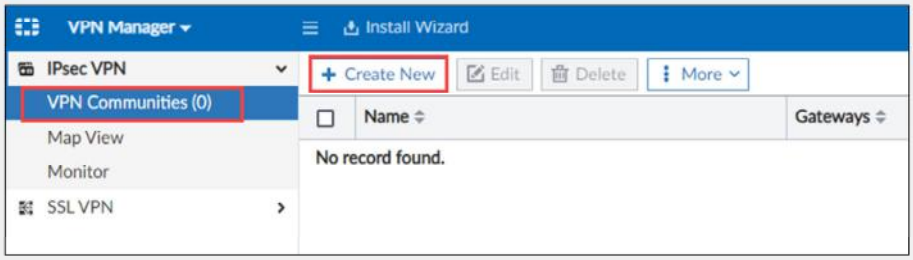
1. Create a VPN community.
2. Add gateways (members) to the community.
3. Install the VPN community and gateways configuration.
4. Add the firewall policies.
5. Install the firewall policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VPN Communities

- Contain the common IPsec settings that are shared by all the IPsec gateway members of the community



- Three types of communities:
  - Site-to-site
  - Hub-and-spoke
  - Remote

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

Depending on the VPN topology you are installing, there are three types of communities:

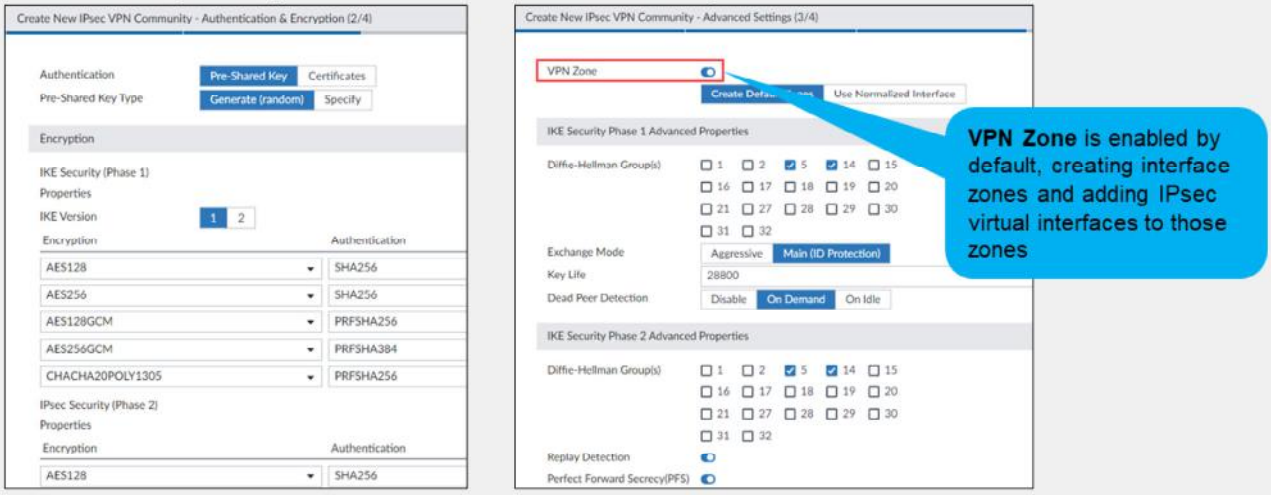
- Site to site
- Hub-and-spoke
- Remote

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VPN Communities Configuration

- Enter the common phase 1 and phase 2settings:
  - These settings are applied to all members in the community



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

The VPN community contains the IPsec phase 1 and 2 settings that are common to all gateways.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VPN Gateways

- After the community is created, it is time to add the VPN gateways
- Two types of gateways:
  - Managed gateways are FortiGate devices managed by FortiManager in the current ADOM
  - External gateways are devices not managed by FortiManager, or devices in a different ADOM
    - VPN configuration must be handled manually by the administrator of that ADOM

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

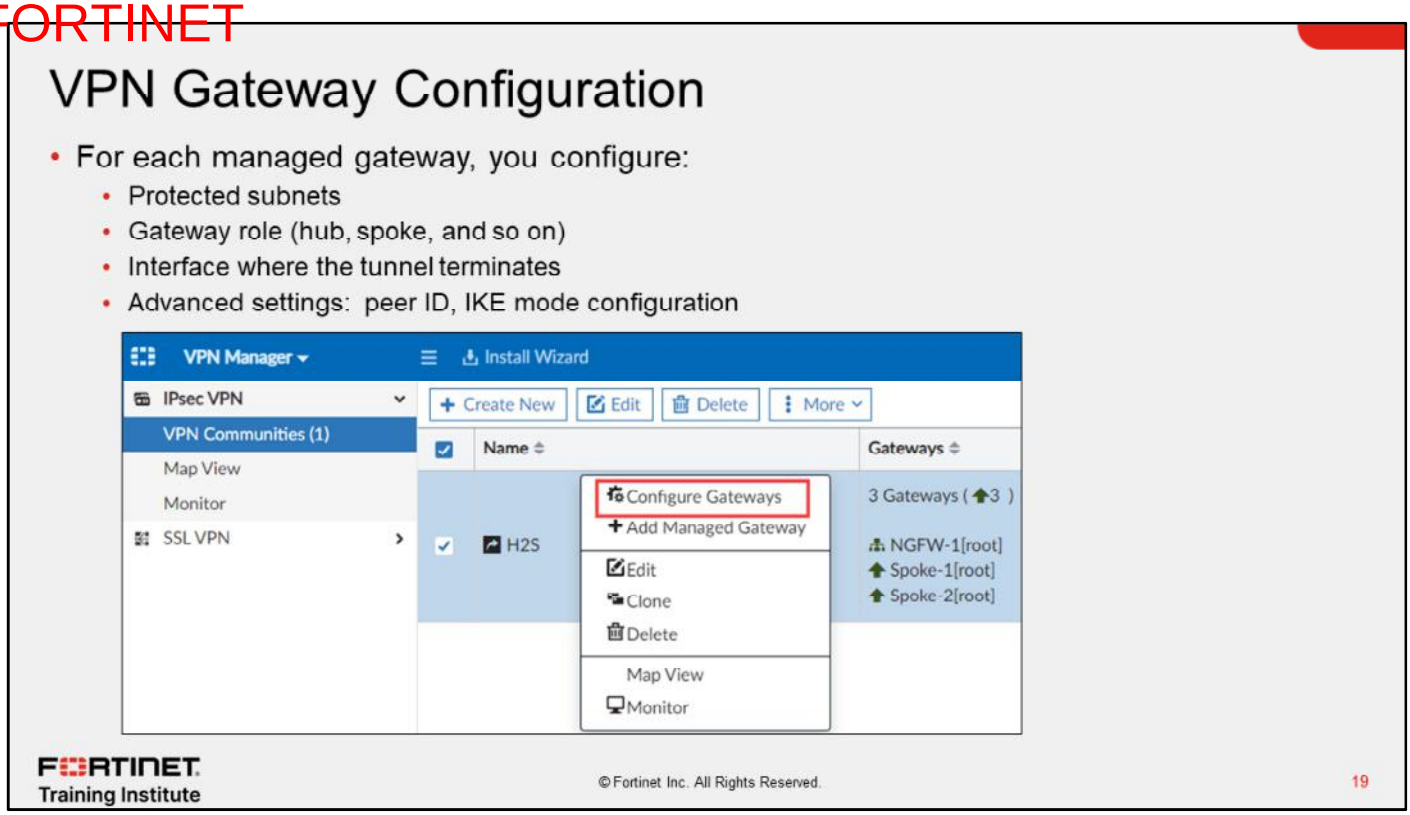
18

The next step is to add gateways to the community. There are two types of gateways:
- Managed gateways
- External gateways

Managed gateways are managed by FortiManager in the current ADOM. You can treat devices in a different ADOM, or other vendor devices, as external gateways. The administrator must handle VPN configuration manually in that ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

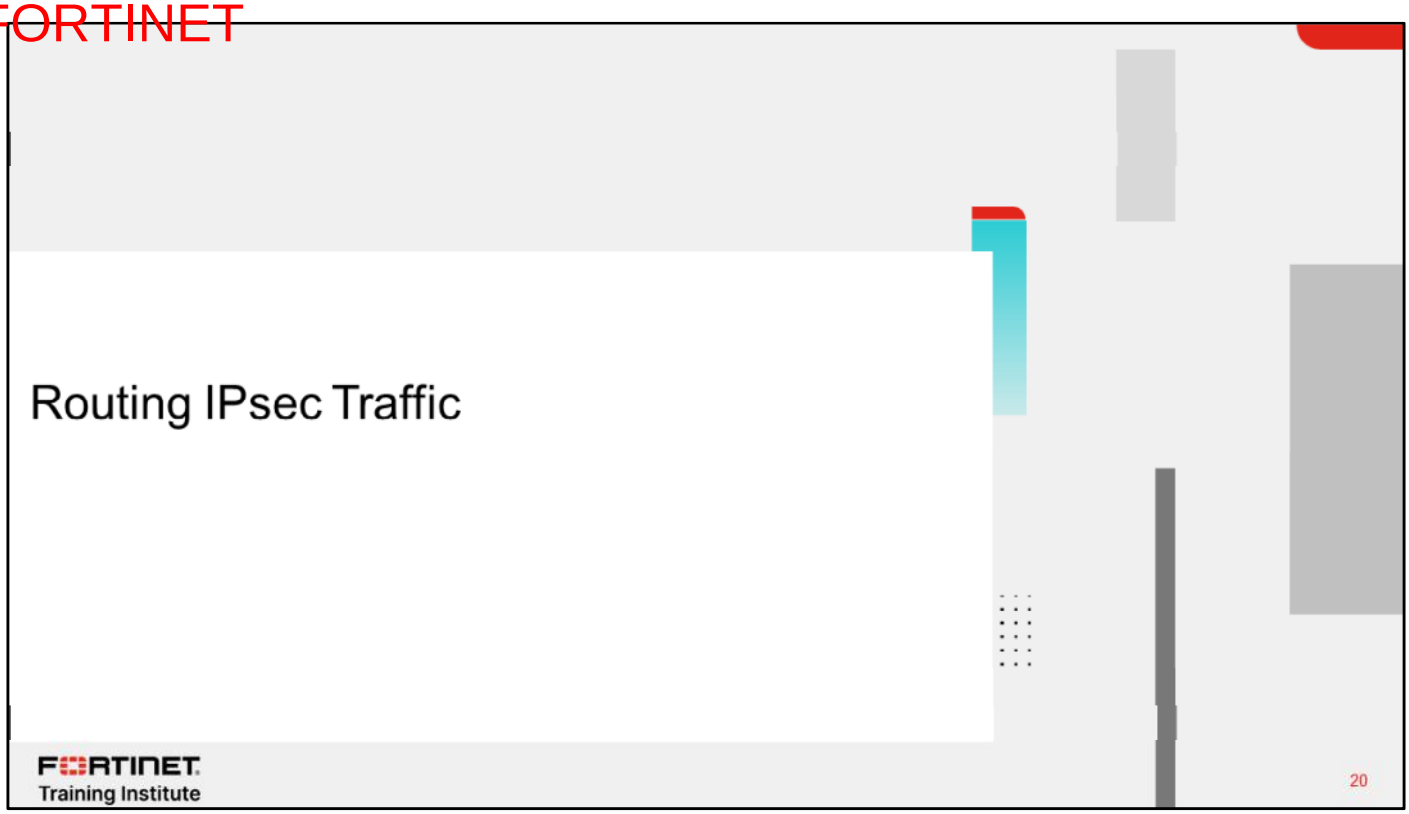


In VPN gateways, you configure the node type (hub, spoke, and so on), depending on the VPN topology you select. For example, hub-and-spoke options are available only in **Hub-and-Spoke** and **Remote** topologies.

For each gateway, you can also configure the protected subnet, interfaces, and some advanced settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn how FortiGate routes IP traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Routing to Dial-Up Connections

- In interface mode, by default, static routes are automatically added to each IPsec dial-up client

```
config vpn ipsec phase1-interface
  edit <phase-1-name>
    set type dynamic
    set add-route [ enable* | disable ]
    set distance <distance>
    set priority <priority>
end
```

Disable `add-route` if you are using a dynamic routing protocol over IPsec and do not want FortiGate to automatically add static routes

Distance and priority assigned to the static routes added automatically

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

If the IPsec VPN has been configured in interface mode, statics routes are automatically added to clients each time a dial-up IPsec connects. The destination subnets of the static routes are the ones received in the phase 2 quick mode selectors. When IKE mode configuration, or DHCP over IPsec is used, those subnets (with a /32 mask) matched the IP addresses assigned to dial-up users.

If you are running a dynamic routing protocol over IPsec, disable add-route. This will prevent FortiGate from dynamically adding the route. The routes do not need to be added dynamically because the dynamic routing protocol updates the routing table after the tunnel is up.

By default, the distance assigned to those dynamic routes is 15, and the priority is 0. You can change those values in the phase 1 configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Routing to Dial-Up Connections (Contd)

- If `net-device` is enabled, FortiGate creates separate virtual interfaces for each dial-up client
  - FortiGate uses the destination subnets in the quick-mode selectors
  - Tunnel name = `phase1Name_index`

```
# config vpn ipsec phase1-interface
      edit Hub
            set add-route   enable
            set net-device  enable
# end
```

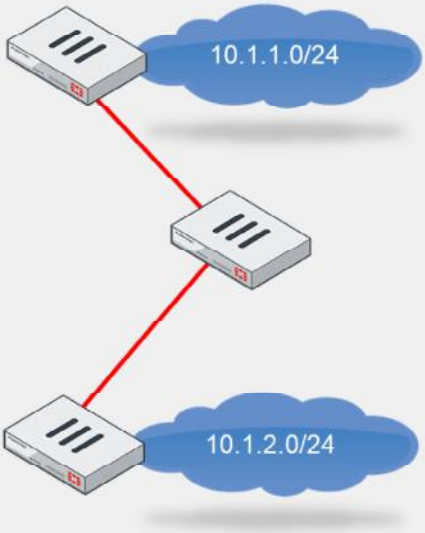
Default value

Default value is `disable`

```
# get router info routing-table all
S 10.1.1.0/24 [15/0] via 100.64.3.1, Hub_1
S 10.1.2.0/24 [15/0] via 100.64.5.1, Hub_0
```

Subnets learned through quick-mode selectors

One virtual interface for each tunnel



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

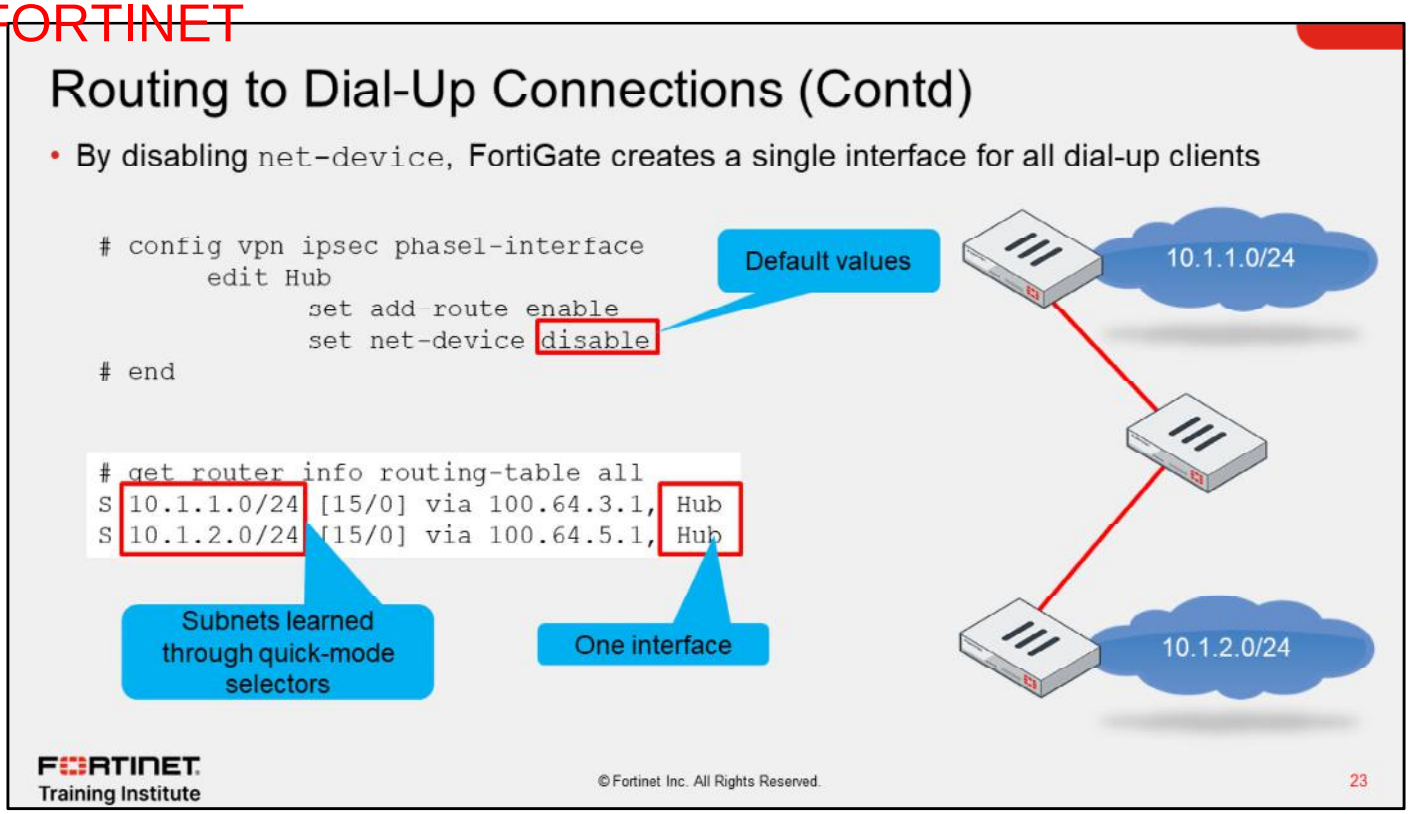
22

When the phase 1 setting net-device is enabled, FortiGate creates separate virtual interfaces for each dial-up client. The names of those interfaces comprise the phase 1 name and an index number.

When you use this configuration, FortiGate uses the information in the destination subnets of the quick-mode selectors to learn the networks behind each remote IPsec client. Each virtual IPsec interface is associated with one client (or one IKE SA).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

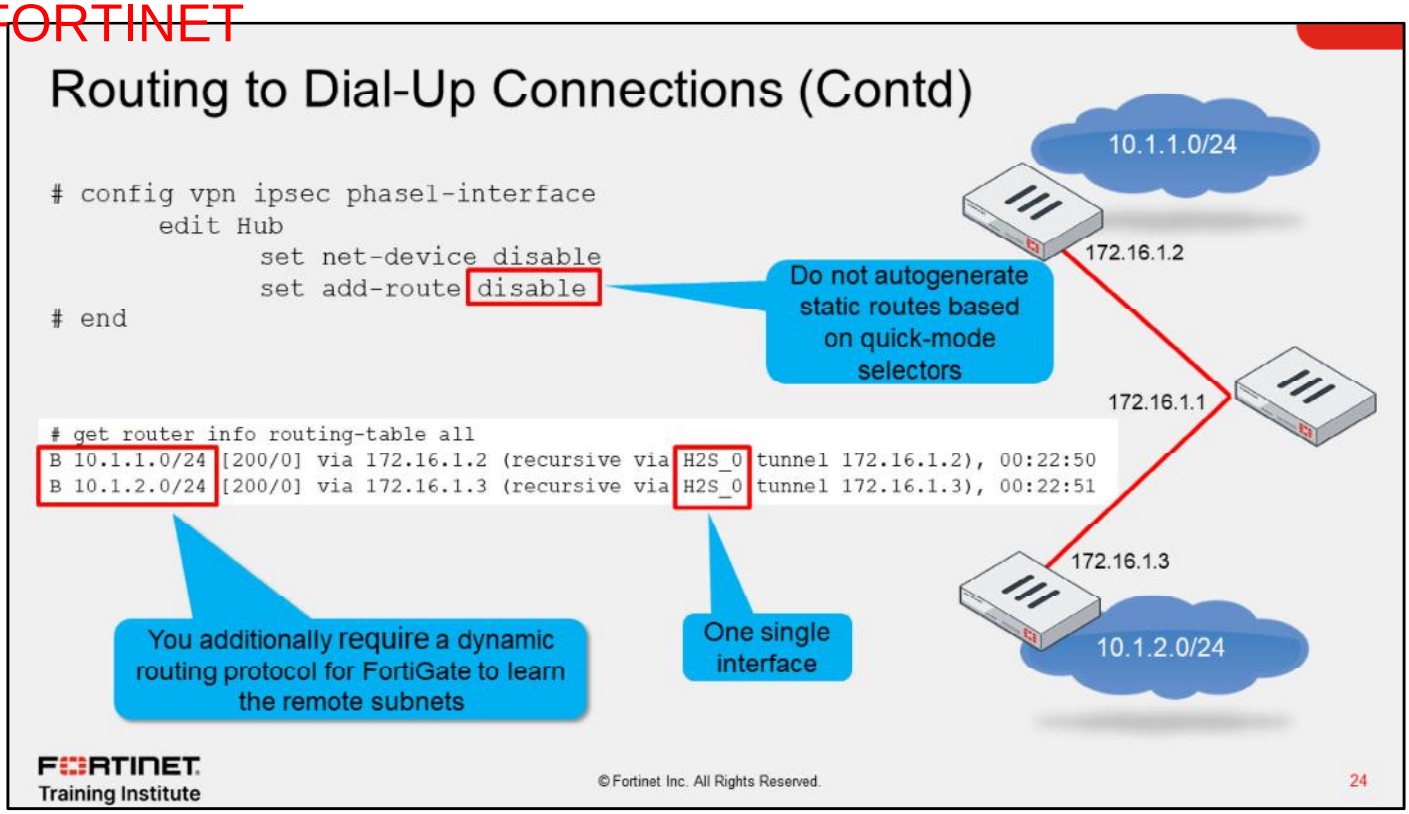


If net-device is disabled, FortiGate creates a single IPsec virtual interface that is shared by all IPsec clients connecting to the same dial-up VPN.

FortiGate uses the destination subnets of the quick-mode selectors to populate the routing table with information about the remote networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

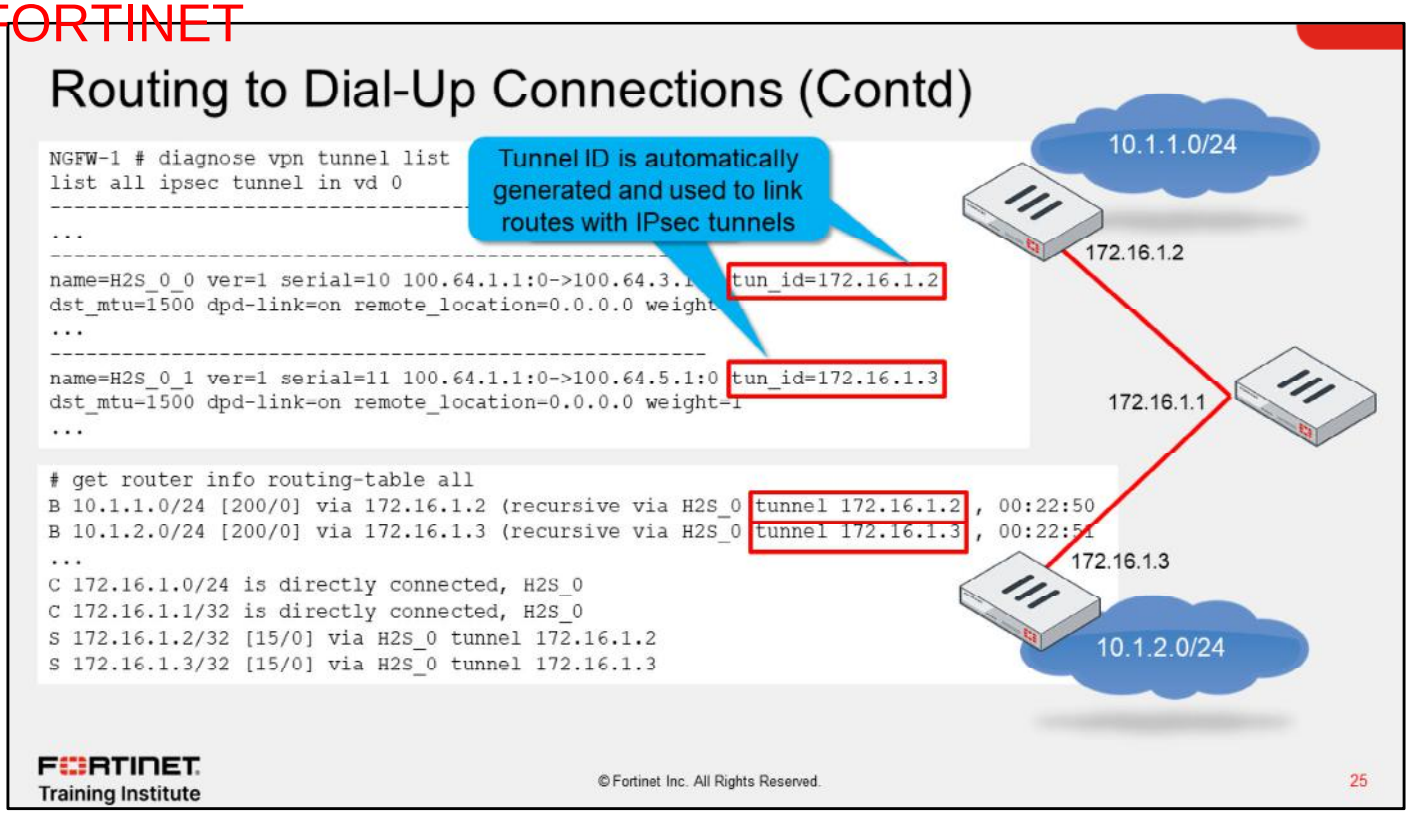
DO NOT REPRINT Brave-dumps.com
© FORTINET



If add-route is set to disable, FortiGate does not use the quick-mode selectors to learn about remote networks. FortiGate will learn those routes with the assistance of a dynamic routing protocol, which must be configured to run over the IPsec tunnels.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

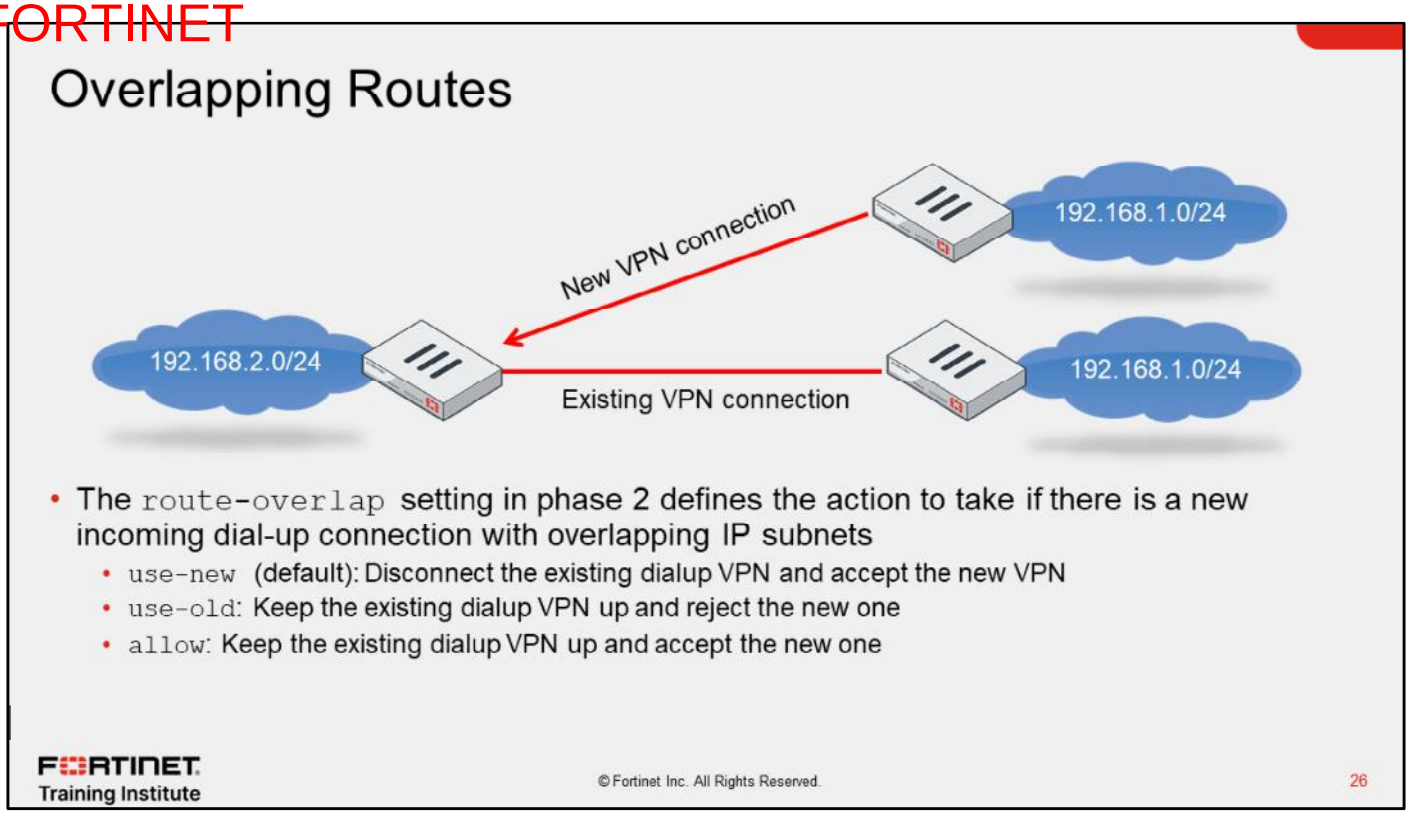


When net-device is disabled, FortiGate creates a single IPsec virtual interface that is shared by all IPsec clients. FortiGate automatically assigns a tunnel id (tun-id) for each IPsec client. FortiGate combines this information with the routes learned through a routing protocol, to properly route the IPsec traffic, selecting the correct outbound IPsec virtual interface and IKE SA.

The output of the `diagnose vpn tunnel list` command shows the list of remote IPs and the associated tunnel ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

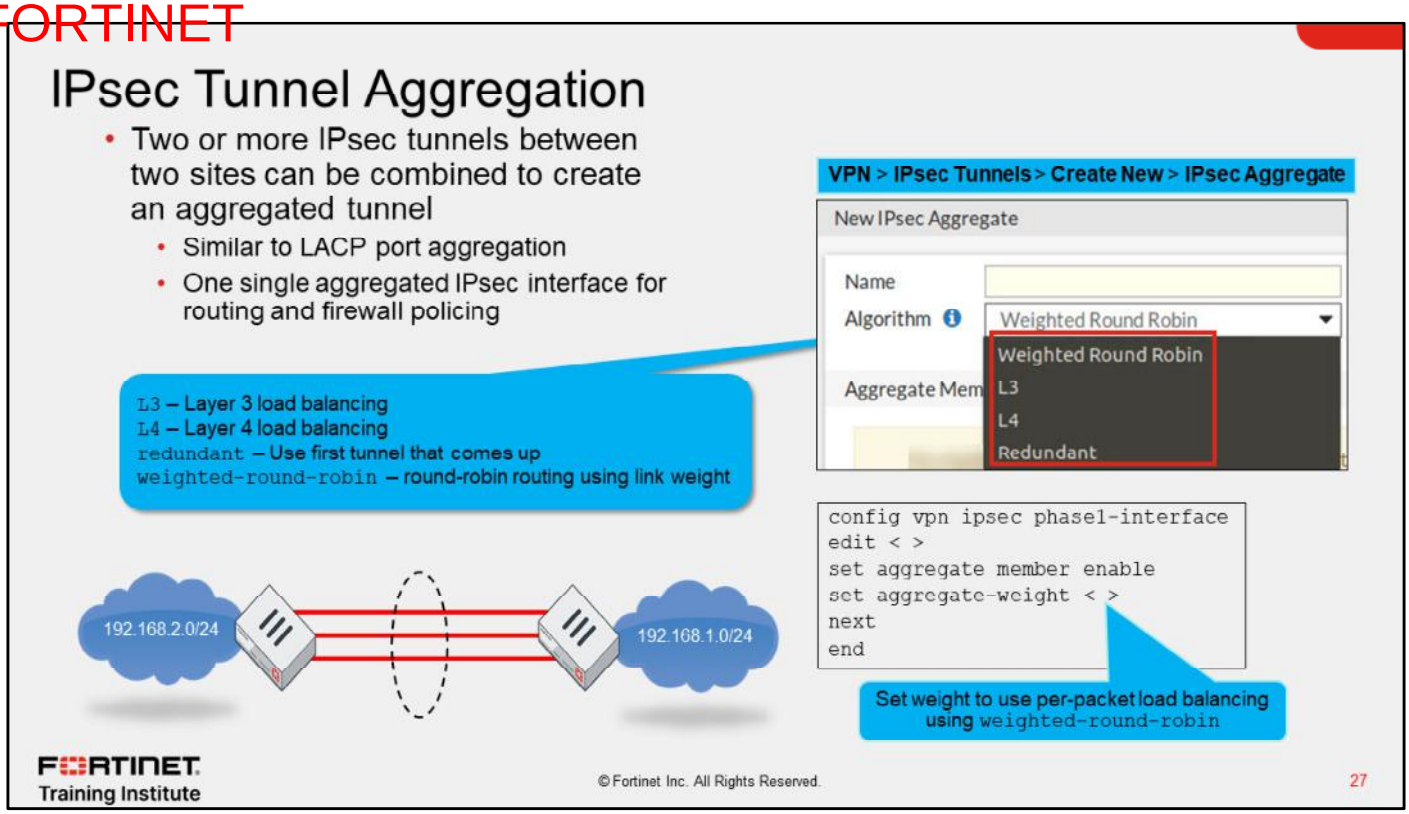


If two remote sites have the same subnets, they might create overlapping static routes in the central FortiGate. The setting route-overlap, found in phase 2, defines what action FortiGate will take when a new remote site is connecting and there is a remote site already connected with an overlapping subnet. The possible actions include:

- `use-new` (default): Disconnect the existing dialup VPN and accept the new VPN.
- `use-old`: Keep the existing dialup VPN up and reject the new one.
- `allow`: Keep the existing dialup VPN up and accept the new one. Traffic for sessions that start from the central FortiGate will be load balanced (ECMP) between both VPNs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



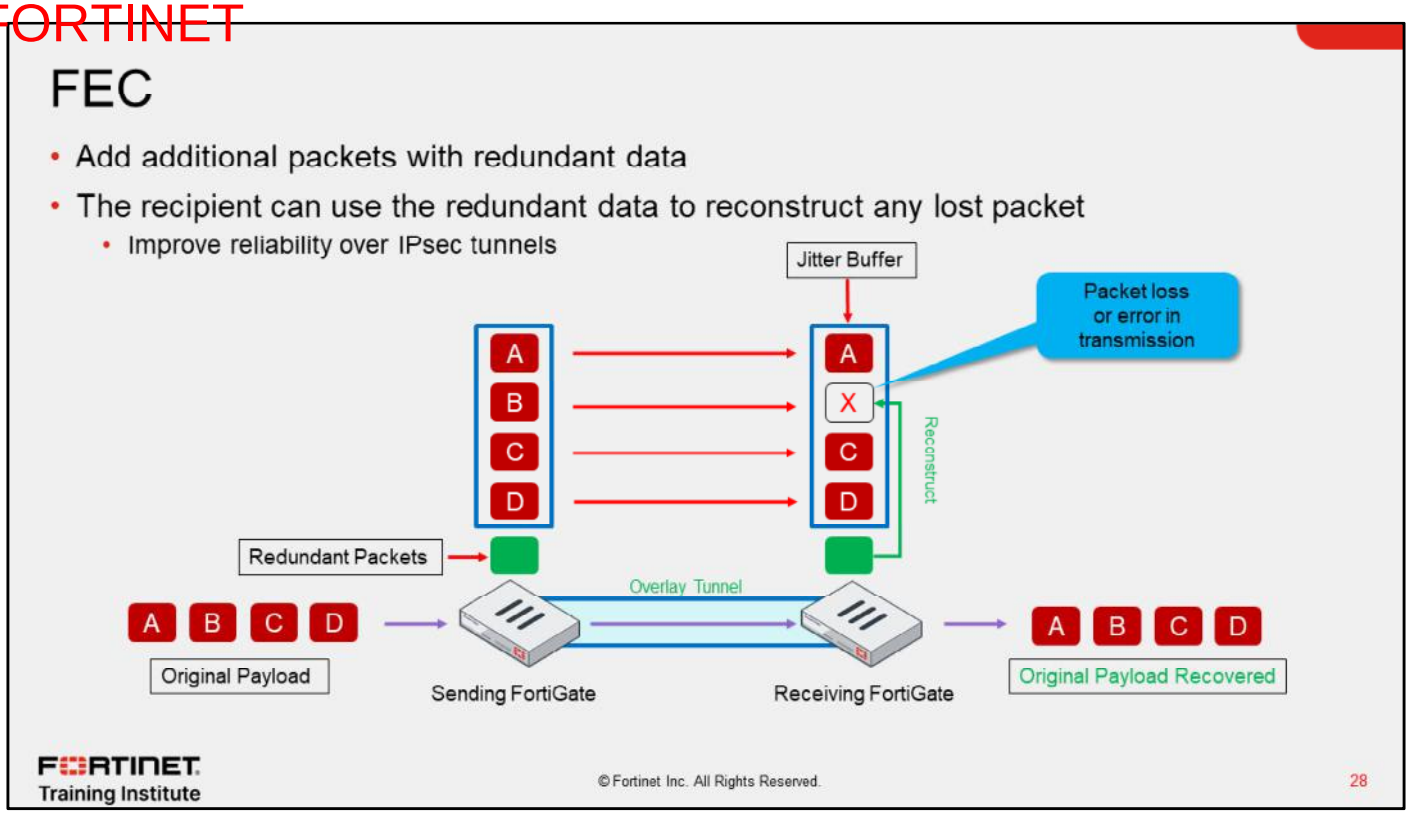
Two or more IPsec tunnels between two sites can be combined to create an aggregated tunnel. This is similar to LACP port aggregation. One single aggregated IPsec interface is created and used for routing and firewall policing.

Aggregated IPsec tunnels support five load-balancing methods:

- round-robin: Traffic is balanced per packet.
- L3: Traffic is balanced based on the Layer 3 header information.
- L4: Traffic is balanced based on the Layer 4 header information.
- redundant: All traffic is sent though the tunnel that came up first. The other tunnels are used for backup.
- weighted-round-robin: Traffic is load balanced in a round-robin manner based on link weights configured for each tunnel.

Vouchers & Dumps are Available | WhatsApp +201224560923

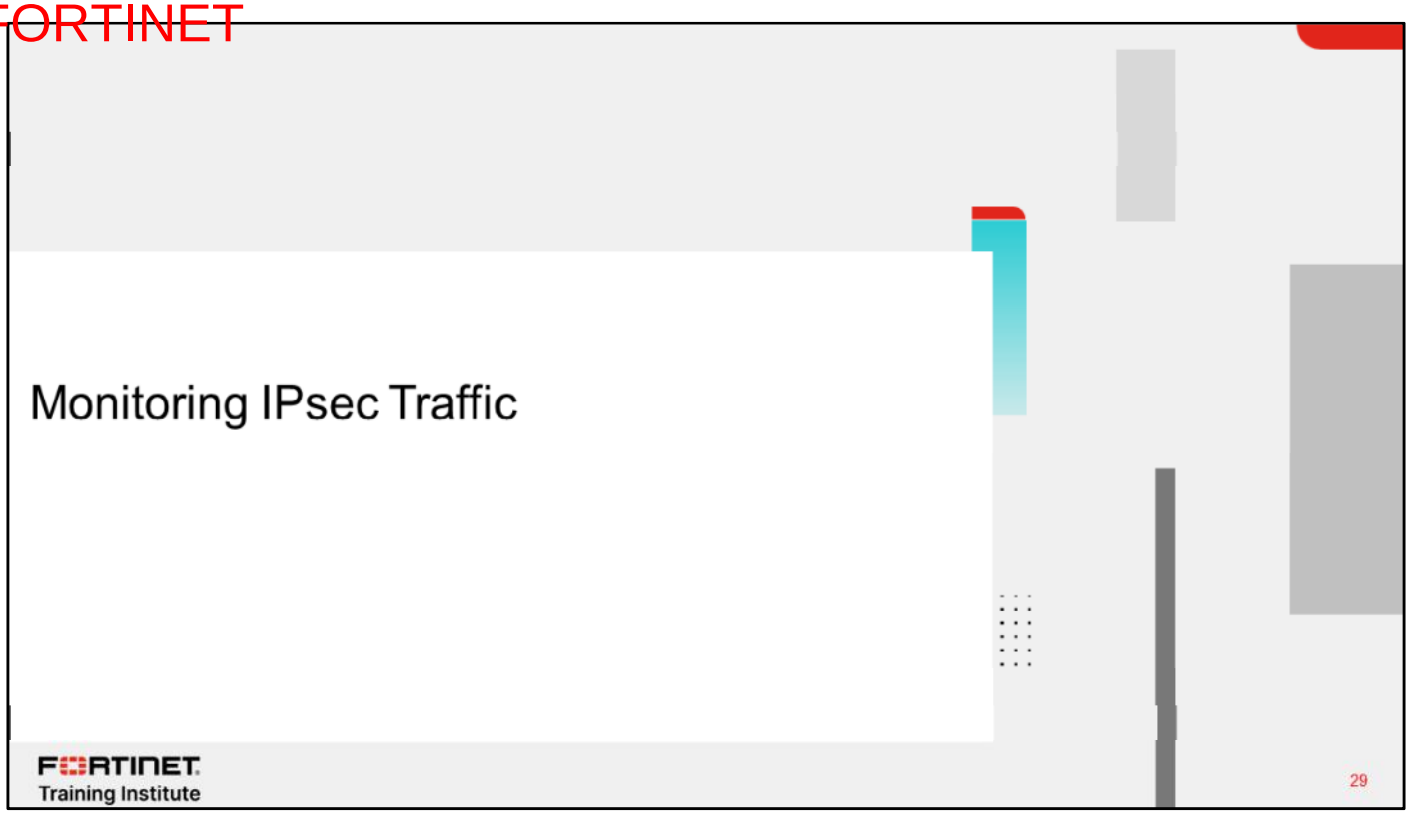
DO NOT REPRINT Brave-dumps.com
© FORTINET



Forward error correction (FEC) is a phase 1 setting that, when enabled, adds additional packets with redundant data. The recipient can use this redundant information to reconstruct any lost packet, or any packet that arrived with errors. Although this feature increases the bandwidth usage, it improves reliability that can overcome adverse WAN conditions such as lossy or noisy links. FEC can be critical for delivering a better user experience for business-critical applications like voice and video services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn how to monitor the status of an IPsec VPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IPsec Monitor on the CLI

```
Spoke-1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=H2S_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1 dst_mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc run_state=0 role=primary accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=465 olast=43122777 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=H2S_0_0 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA: ref=3 options=30202 type=00 soft=0 mtu=1438 expire=1234/0B replaywin=2048
      seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1772/1800
  dec: spi=db09f361 esp=aes key=16 7dfd3ea877bb0d85f3eae0059dc9f64d
      ah=sha256 key=32 37b1255e2db93574e77097c9a7dbe21746156a979297fbac2ae06c0fbc67093e
  enc: spi=ffaba7ea esp=aes key=16 74891598fd6f575a039767f1e59ef85a
      ah=sha256 key=32 ec2ca86b8336eb9c9c11f1dce4d43f714e1e2807450c414024cdc4f4b2f4679a
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

You can use the `diagnose vpn tunnel list` command to view and monitor the IPsec tunnels.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hardware Offloading Requirements

- You can offload IPsec encryption and decryption to hardware on some FortiGate models
- Hardware offloading capabilities and supported algorithms vary by processor type and model
- By default, offloading is enabled for supported algorithms
  - You can manually disable offloading:

```
config vpn ipsec phase1-interface
        edit <tunnel_name>
                set npu-offload enable | disable
        next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

On some FortiGate models, you can offload the encryption and decryption of IPsec traffic to hardware. The supported algorithms depend on the model and type of processor on the unit that is offloading the encryption and decryption.

By default, hardware offloading is enabled for the supported algorithms. This slide shows the commands you can use to disable hardware offloading per tunnel, if necessary.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Session NPU-Flag Field

- IPsec SAs have an NPU-flag field

```
# diagnose vpn tunnel list name Hub2Spoke1
list ipsec tunnel by names in vd 0
...
npu_flag=03 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1
npu_selid=1
```

NPU-flag Value	Description
npu_flag=00	Both IPsec SAs loaded to the kernel
npu_flag=01	Outbound IPsec SA copied to NPU
npu_flag=02	Inbound IPsec SA copied to NPU
npu_flag=03	Both outbound and inbound IPsec SA copied to NPU
npu_flag=20	Unsupported cipher or HMAC, IPsec SA cannot be offloaded

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

All IPsec SAs have an `npu_flag` field indicating offloading status. In the case of IPsec traffic, the FortiGate session table also includes that field.

First, when phase 2 goes up, the IPsec SAs are created and loaded to the kernel. As long as there is no traffic crossing the tunnel, the SAs are not copied to the NPU, and the `npu_flag` shows `00`. The value of that field also remains `00` when IPsec offloading is disabled.

Second, if the first IPsec packet that arrives is an outbound packet that can be offloaded, the outbound SA is copied to the NPU and the `npu_flag` changes to `01`. However, if the first IPsec packet is inbound and can be offloaded, the inbound SA is copied to the NPU and the `npu_flag` changes to `02`.

After both SAs are copied to the NPU, the `npu_flag` changes to `03`.

The value `20` in the `npu_flag` field indicates that hardware offloading is unavailable because of an unsupported cipher or HMAC algorithm.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Review IPsec
- ✓ Review IKE
- ✓ Route IPsec traffic
- ✓ Configure remote IPsec sites with overlapping IP subnets
- ✓ Verify that IPsec encryption and decryption is offloaded to hardware
- ✓ Monitor the status of an IPsec VPN

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

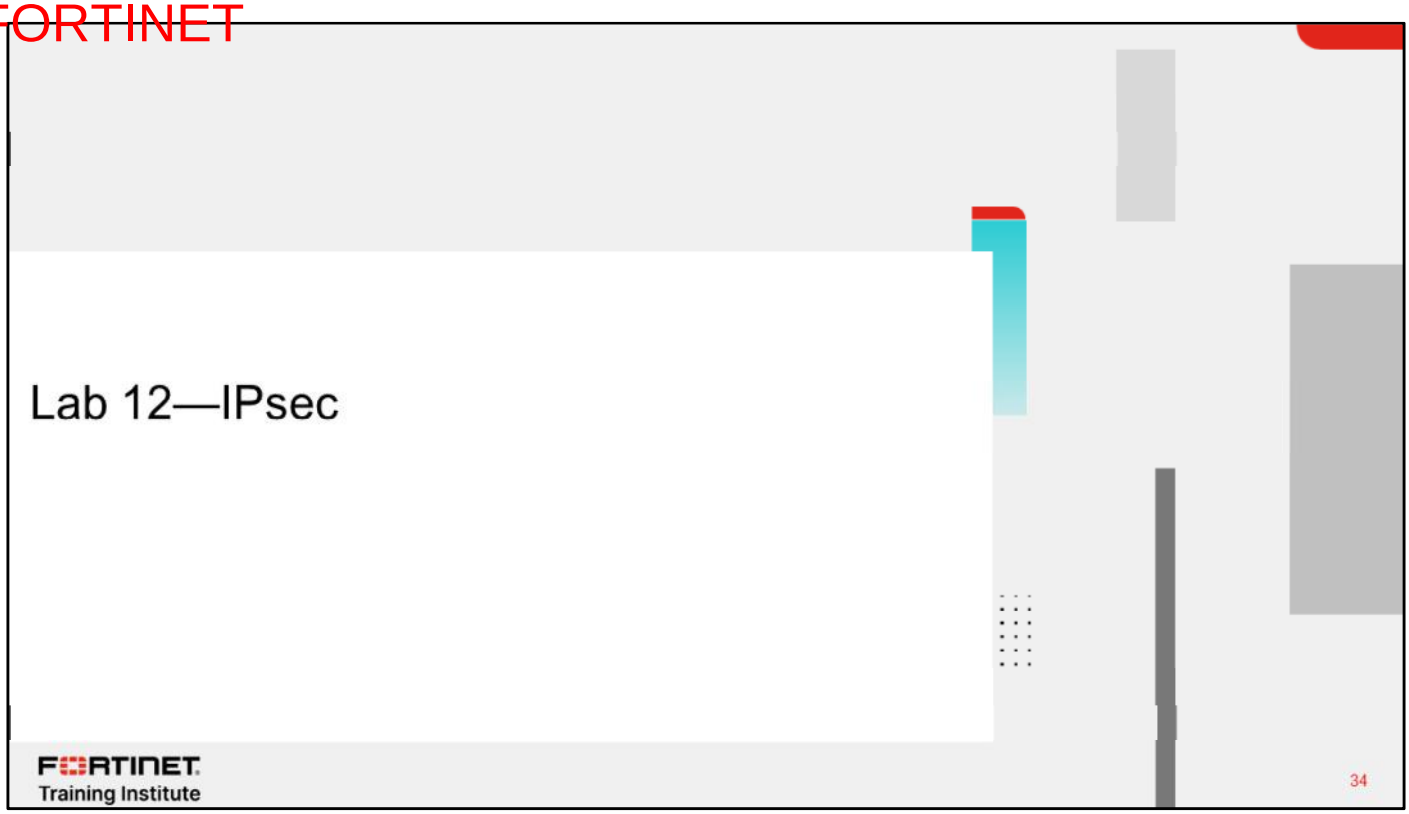
33

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

By mastering the objectives covered in this lesson, you learned how to use IPsec.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



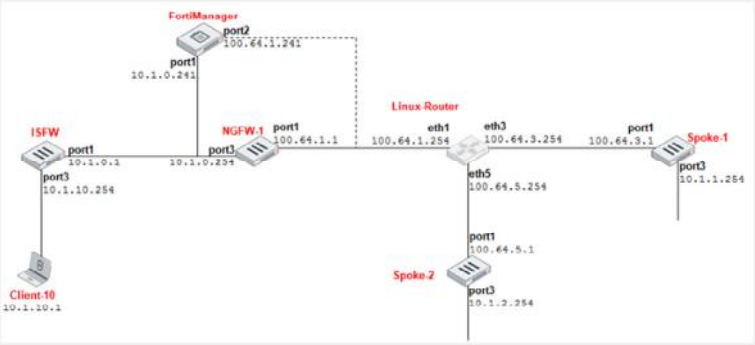
Now, you will work on *Lab 12–IPsec*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 12—IPsec

- VPN Manager:
  - Create a VPN community
  - NGFW-1 is the hub
  - Spoke-1 and Spoke-2 are spokes
  - Install the VPN configuration
  - Add IPsec firewall policies
  - Install the policies



- Do not send traffic; routing is not ready yet

FORTINET Training Institute

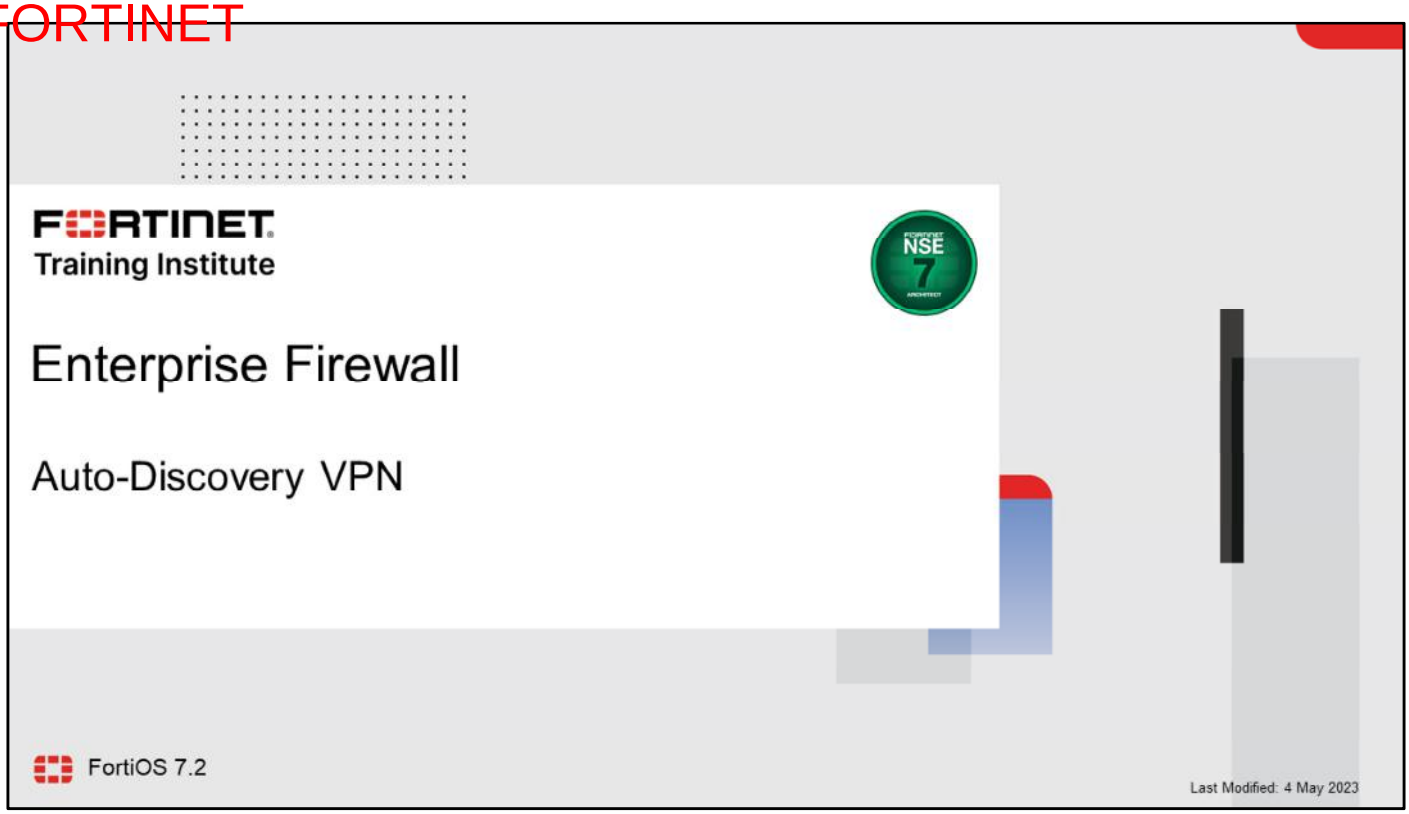
© Fortinet Inc. All Rights Reserved.

35

Then, you will configure a hub-and-spoke VPN network using the FortiManager VPN manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn about auto-discovery VPN (ADVPN) with IKE version 2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Objectives

- Configure and test ADVPN with IKE version 2
- Implement Internal Border Gateway Protocol (IBGP) with ADVPN

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

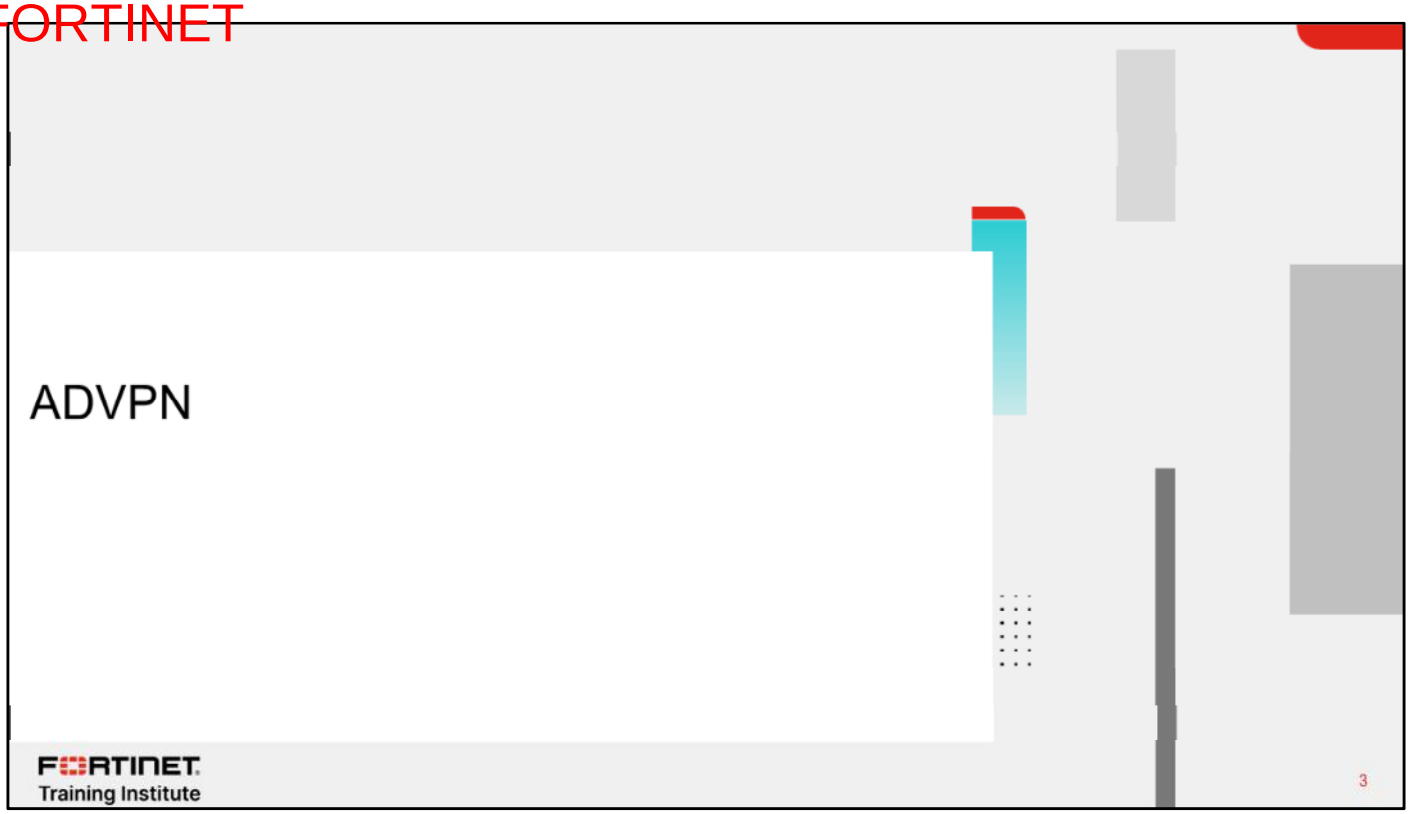
2

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

By demonstrating competence in Fortinet ADVPN, you will be able to configure and test ADVPN with IBGP.

Vouchers & Dumps are Available | WhatsApp +201224560923

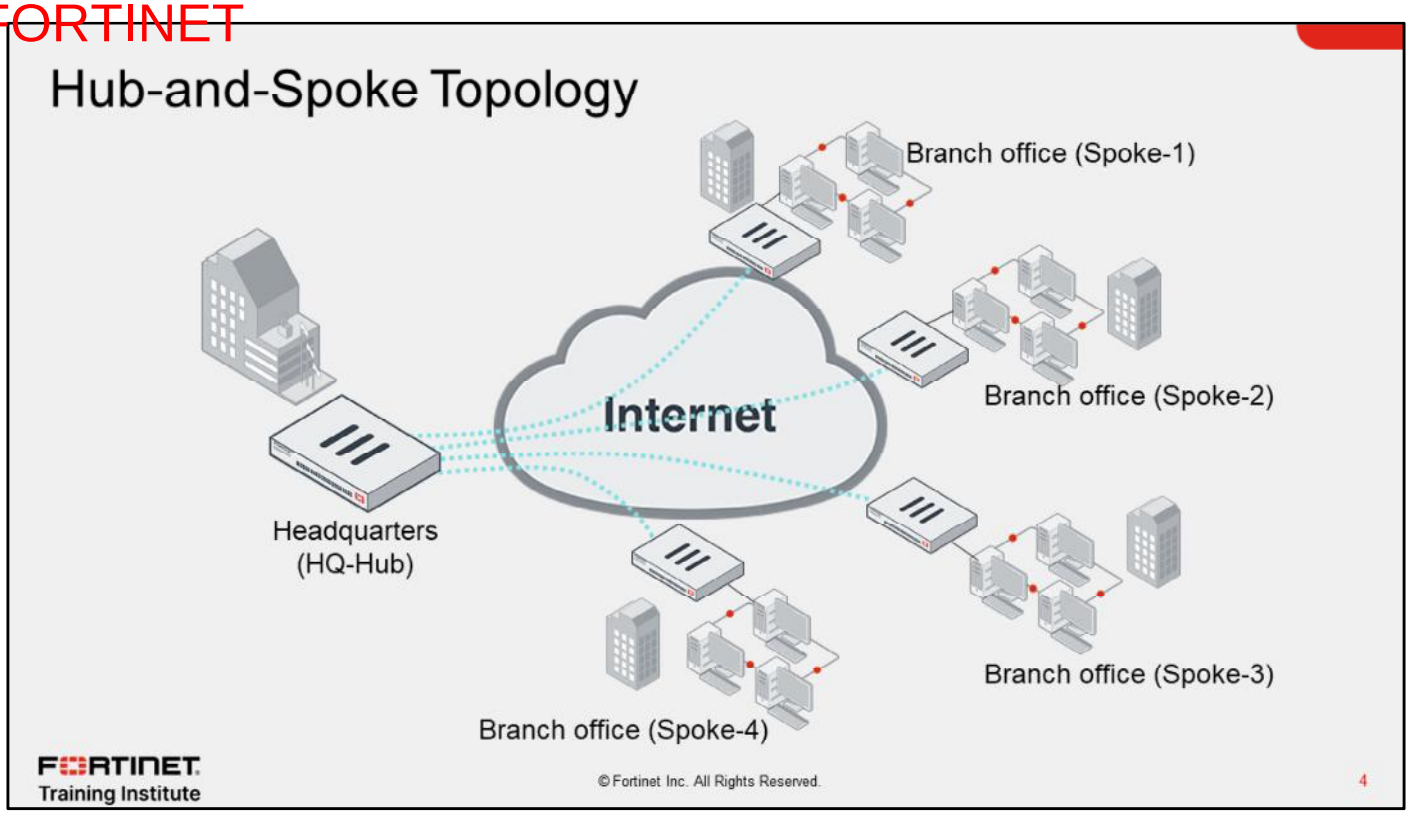
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will learn how to deploy and manage ADVPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Why should you use ADVPN? To find the answer, you will review the most common VPN topologies.

One point-to-multipoint topology variation is called *hub-and-spoke*. As its name describes, all clients connect through a central *hub*, similar to the way spokes connect to hubs on wheels.

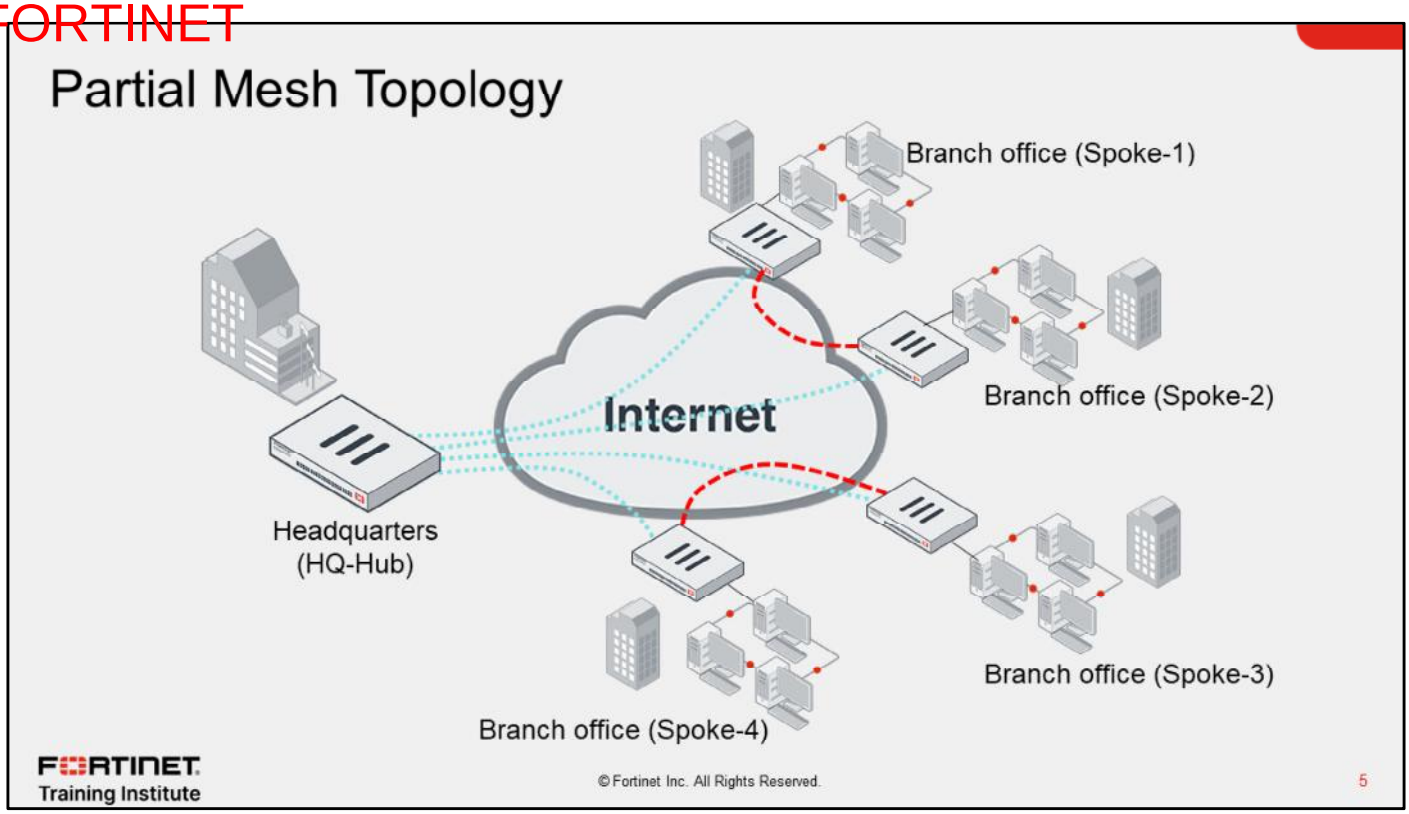
In the example shown on this slide, each client—*spoke*—is a branch-office FortiGate. For any branch office to reach another branch office, its traffic must pass through the hub.

One advantage of using this topology is that you can easily manage the VPN configuration and firewall policies. Also, system requirements are minimal for the FortiGate devices that function as branch offices, because each FortiGate must maintain only one tunnel, or two SAs. In this example, four tunnels, or eight security associations (SAs), are necessary in the hub.

A disadvantage of using this topology is that communication between branch offices through headquarters (HQ) is slower than it would be using a direct connection, especially if HQ is physically distant, as it can be for global companies. For example, if your company's HQ is in Brazil, and your company also has offices in Japan and Germany, latency can be significant. Another disadvantage is lack of redundancy. For example, if FortiGate at HQ fails, the VPN fails company wide. Also, FortiGate at HQ must be more powerful, because it handles four tunnels simultaneously, or eight SAs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

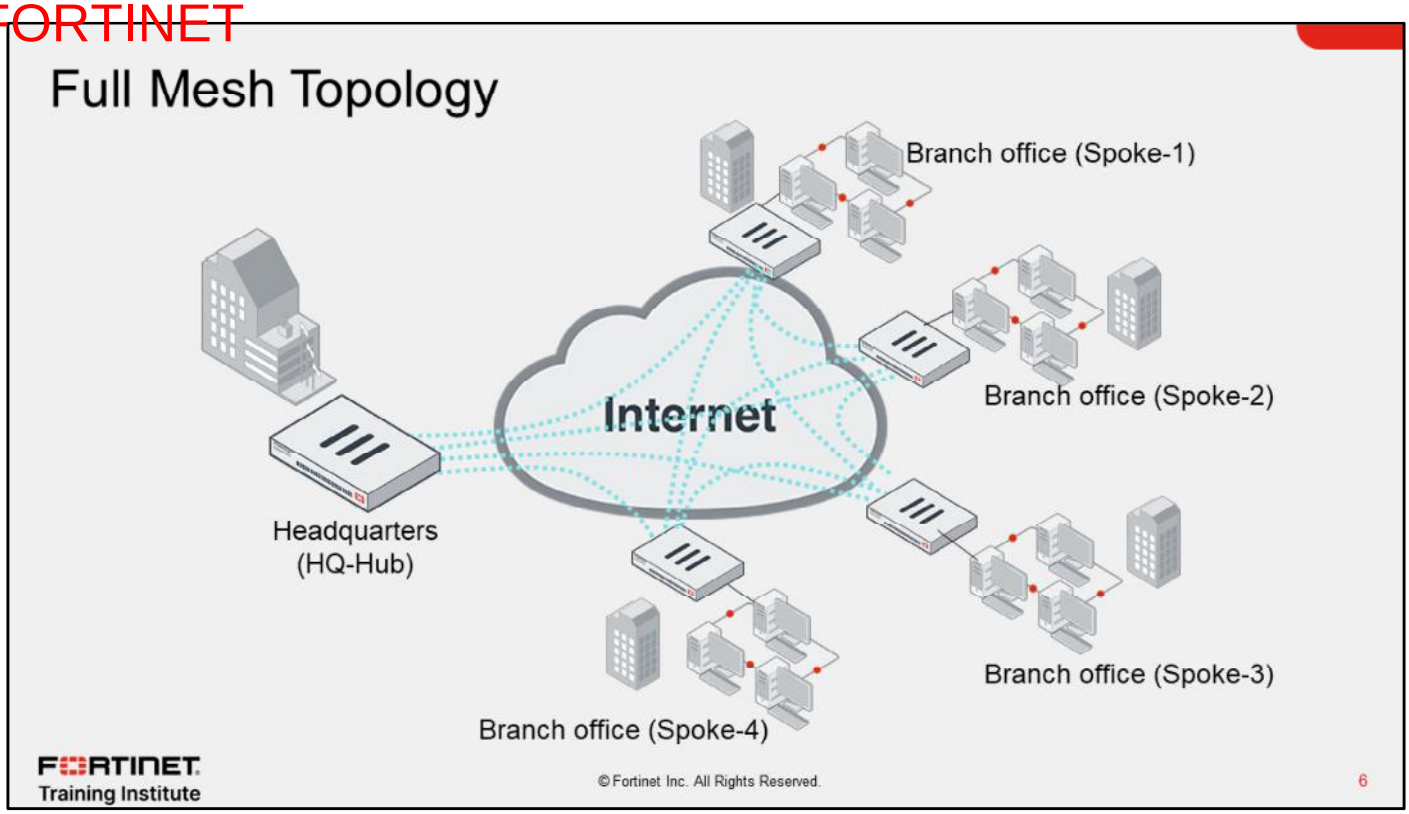


This slide shows a VPN that has a partial mesh topology. There are two types of mesh topologies, partial mesh and full mesh.

Partial mesh attempts to compromise, minimizing required resources as well as latency. Partial mesh can be appropriate if communication is not required between every location. This slide shows additional connections between Spoke-1 and Spoke-2 and, Spoke-3 and Spoke-4 connections. However, each FortiGate device configuration is still more complex than hub-and-spoke. Routing, especially, may require extensive planning.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows a VPN that has a full mesh topology.

Full mesh connects every location to every other location. Like the previous hub-and-spoke example, the example on this slide shows only five locations. In order to fully interconnect, each FortiGate needs four VPN tunnels, or eight SAs, to the other FortiGate devices. This equals three more tunnels for each spoke FortiGate. In total, 10 tunnels are needed. If your company were to expand to six locations, it would require 15 tunnels. Seven locations would need 21 tunnels, and so on. You can use the formula `N sites = N (N-1) / 2` to calculate the number of tunnels. This topology causes less latency and requires much less HQ bandwidth than hub-and-spoke. Its disadvantages? Every spoke FortiGate must be more powerful. Additionally, both administration and troubleshooting get more complicated.

So, in general, if your company has many locations, hub-and-spoke will be cheaper, but slower, than a mesh topology. Mesh topologies place less strain on the central location and can be more fault-tolerant, but are also more expensive.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Fortinet ADVPN

- ADVPN is a proprietary solution based on IKE and IPsec
- Provides direct connectivity between all sites by creating on-demand tunnels between spokes
  - Benefit of full-mesh topology while providing scalability with minimum configuration
- Supports multiple hub-and-spoke architecture
- Spoke-to-spoke traffic no longer needs to flow through the hub
- Supports NAT for on-demand tunnels
- Requires use of dynamic routing
  - BGP, OSPF, and RIPv2/RIPng are supported
- Supports both IPv4 and IPv6

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

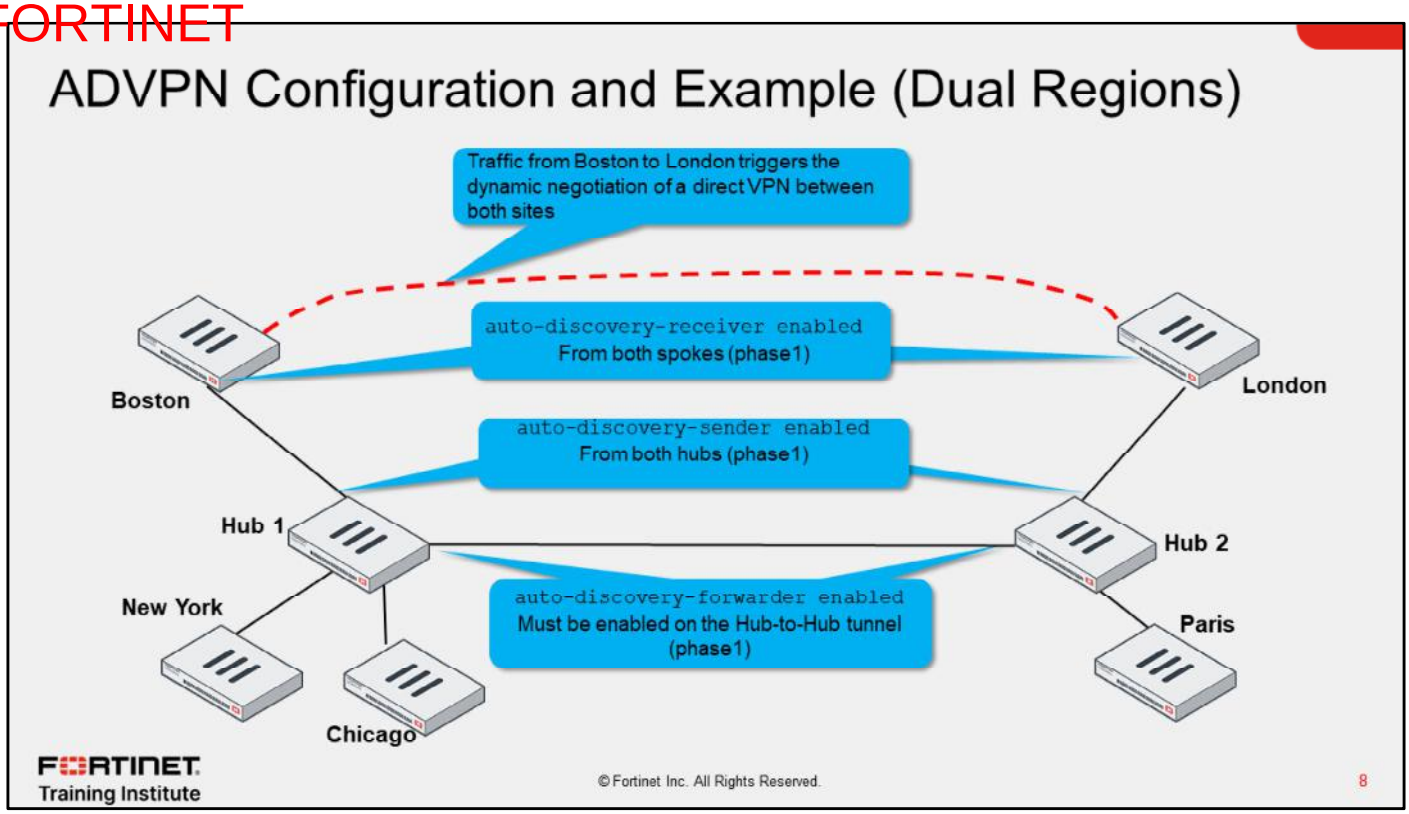
7

ADVPN was introduced in FortiOS 5.4. It combines the benefits of hub-and-spoke and full-mesh topologies because all the spoke-to-spoke tunnels are dynamically created on demand. After a shortcut tunnel is established between two spokes and routing has converged, spoke-to-spoke traffic no longer needs to flow through the hub. ADVPN provides direct connectivity.

ADVPN supports:
- Single or multiple hub architectures
- NAT for on-demand tunnels
- Both IPv4 and IPv6
- BGP, OSPF, and RIPv2/RIPng; as ADVPN requires the use of a routing protocol

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



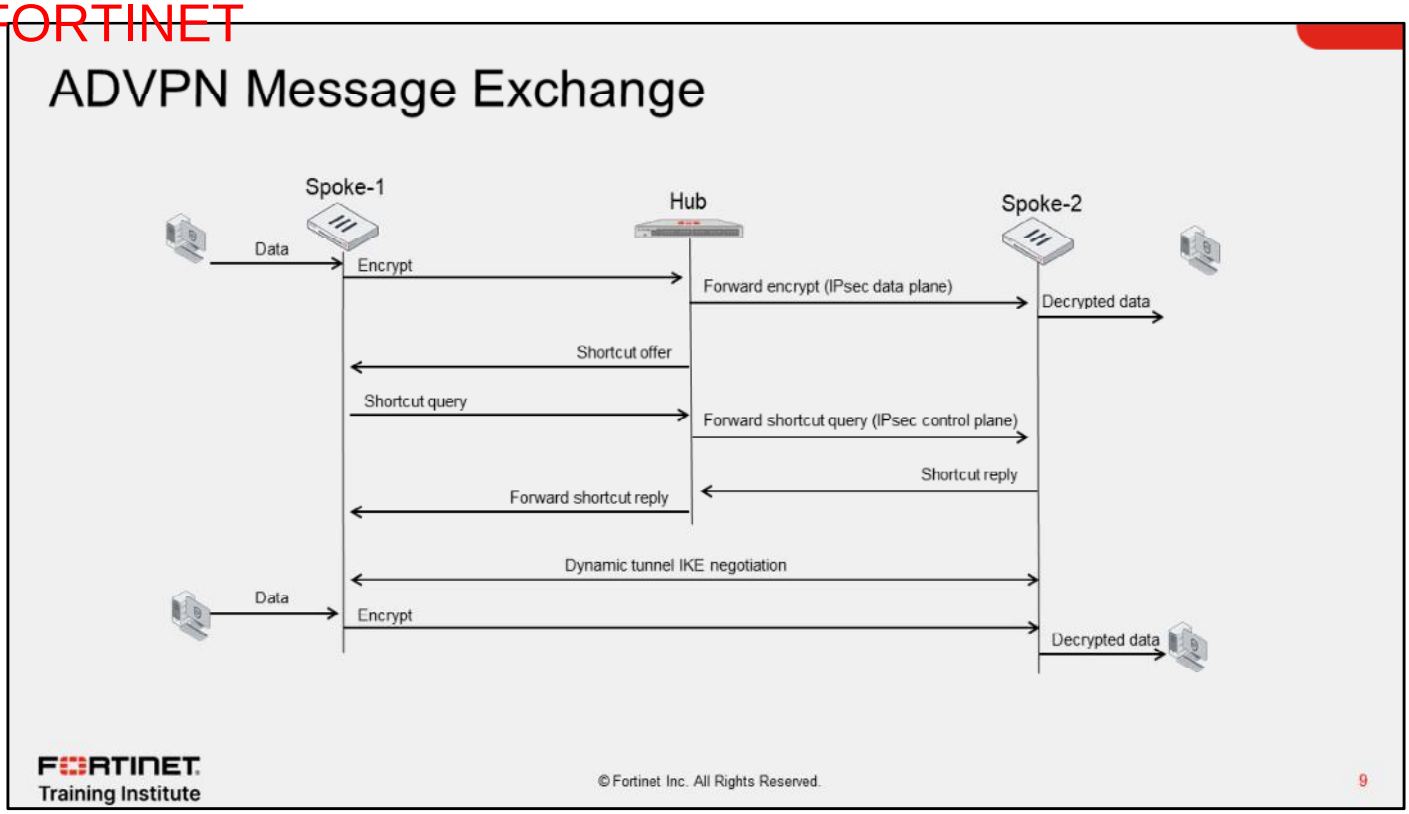
This slide shows an example of how ADVPN works.

An administrator configures IPsec VPNs in multiple FortiGate devices to form VPN hub-and-spoke topologies. In this example, there are two hubs. Hub 1 has three spokes. Hub 2 has two spokes. There is also a VPN connecting both hubs.

The dynamic tunnels between spokes are created on demand. Say that a user in Boston sends traffic to London. Initially, the direct tunnel 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 because of `auto-discovery-sender enable` settings. So, Hub 1 sends an IKE message to Boston informing it 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 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 dynamic tunnel 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 Brave-dumps.com
© FORTINET

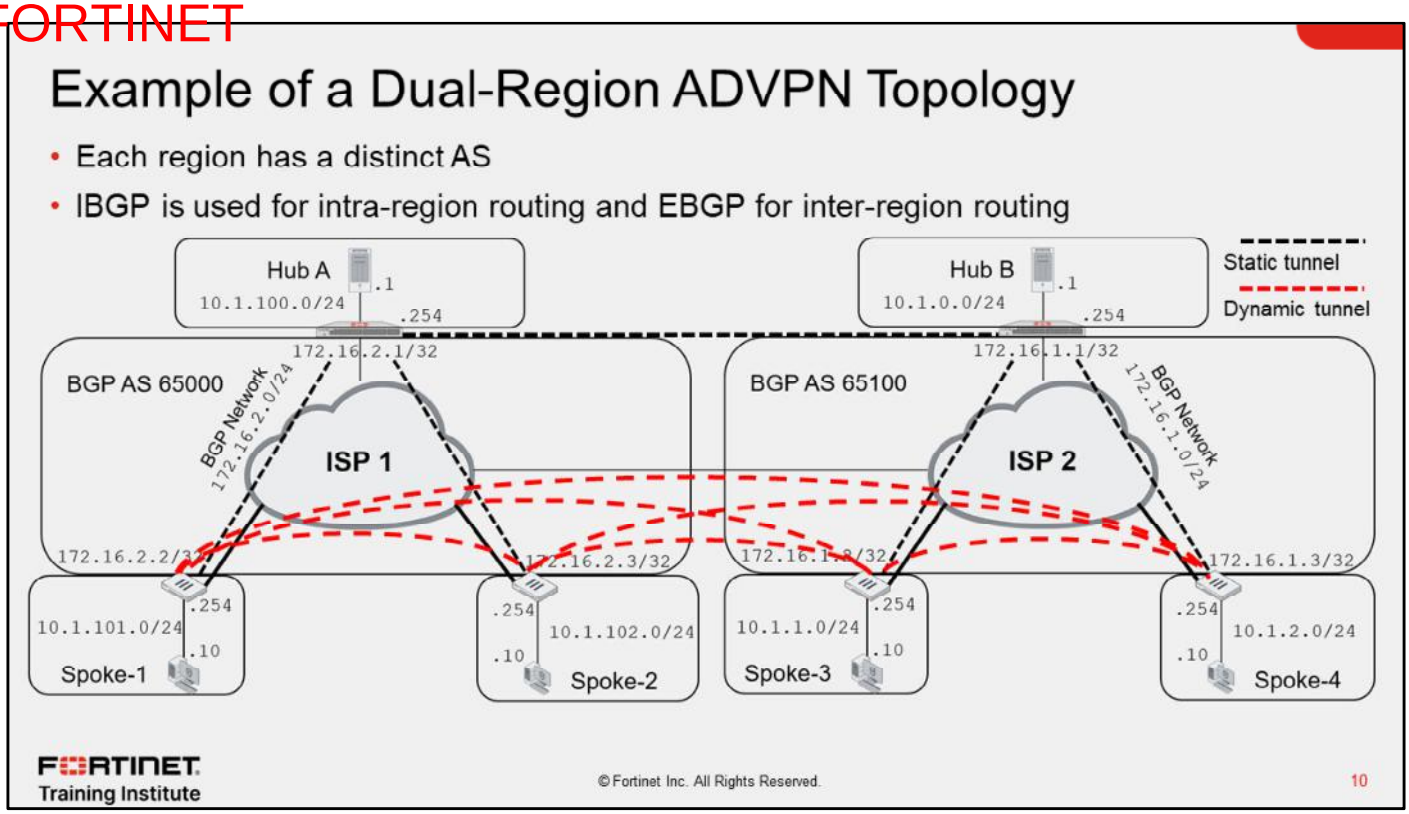


Now, you will examine how IKE messages that are exchanged when an on-demand tunnel is being negotiated:

1. The client behind Spoke-1 generates traffic for devices located behind Spoke-2.
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 Brave-dumps.com
© FORTINET

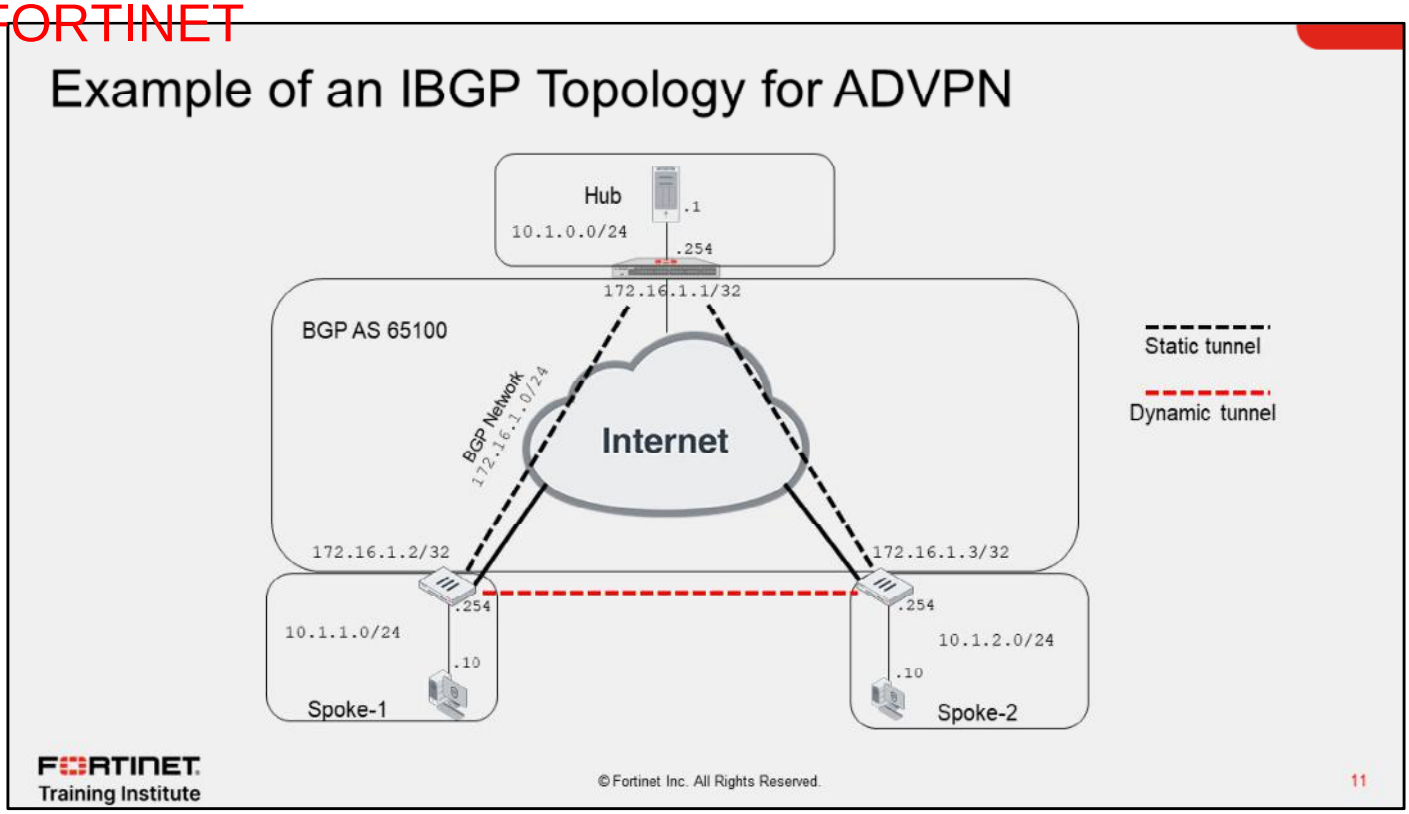


ADVPN requires the use of a dynamic routing protocol and can be implemented over multiple regions.

As an example, the dual-region ADVPN topology shown in this slide is handled through IBGP for inter-region routing and EBGP for inter-region routing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to configure one part of the dual region topology, meaning ADVPN with IBGP.

This IBGP topology includes one hub with two spokes and all the devices are in the AS 65100.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hub ADVPN Configuration

```
Hub # config vpn ipsec phase1-interface
    edit "H2S_0"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set net-device disable
        set add-route disable
        ...
        set auto-discovery-sender enable
        ...
 next
end
config vpn ipsec phase2-interface
    edit "H2S_0"
        set phase1name "H2S_0"
        ...
    next
end
```

Sets IKE to version 2

Dynamic routing is used for learning the protected subnets of the spokes

Enables ADVPN

```
Hub # show sys interface | grep -f H2S_0
config system interface
    edit "H2S_0" <---
        set vdom "root"
        set ip 172.16.1.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 172.16.1.254/24
        set snmp-index 34
        set interface "port1"
    next
end
```

The mask for the local IP can only be /32 so, the mask for the overlay subnet must be specified in remote-ip

Assign a remote dummy IP (overlay IP and subnet)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

This slide shows the following ADVPN configuration in the hub:

- Set `ike-version` to version 2.
- Disable `set add-route` to ensure that dynamic routing is used for learning the protected subnets of the spokes.
- Disable `set net-device` to ensure FortiGate does not create a dynamic interface.
- You must enable `set auto-discovery-sender` if you want ADVPN. This setting indicates that when IPsec traffic transits the hub, it should send a shortcut offer to the initiator of the traffic to indicate that it could perhaps establish a more direct connection (shortcut).
- Assign an overlay IP address to the IPsec virtual interface. This is a requirement for having a dynamic routing protocol over IPsec.
- The overlay IPs of all hub-and-spoke participants are in the same subnet.
- For the `remote-ip`, you can use an unused IP from the overlay subnet. You will need to add the appropriate subnet based on the number of hub and spoke topologies.
- For the phase 2 configuration, ensure that quick modes are set to all `(0.0.0.0/0.0.0.0)`.
- Set a firewall policy to allow traffic from the spokes to the hub, from the hub to the spokes, and between spokes through the hub.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Spoke ADVPN Configuration

```
Spoke-1 # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "H2S_0"
        set interface "port1"
        set ike-version 2
        set auto-discovery-receiver enable
        set net-device enable
        ...
    next
end

config vpn ipsec phase2-interface
    edit "H2S_0"
        set phase1name "H2S_0"
        set proposal aes128-sha1
    next
end
```

Sets IKE to version 2

Enables ADVPN

```
Spoke-1 # show sys interface
config system interface
...
 edit "H2S_0"
        set vdom "root"
        set ip 172.16.1.2 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 172.16.1.1/24
        set snmp-index 33
        set interface "port1"
    next
end
```

Local IP with /32

Hub overlay IP with /24

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

This slide shows the following ADVPN configuration in a spoke:

- Enable ADVPN with the command `auto-discovery-receiver`. Use this command to indicate that this IPsec tunnel wants to participate in an autodiscovery VPN (that is, receive a SHORTCUT-OFFER).
- Assign an interface IP, remote IP, and subnet to the IPsec virtual interface.

In a spoke ADVPN configuration, the command `net-device` can be disabled. In a spoke SD-WAN configuration, it must be enabled.

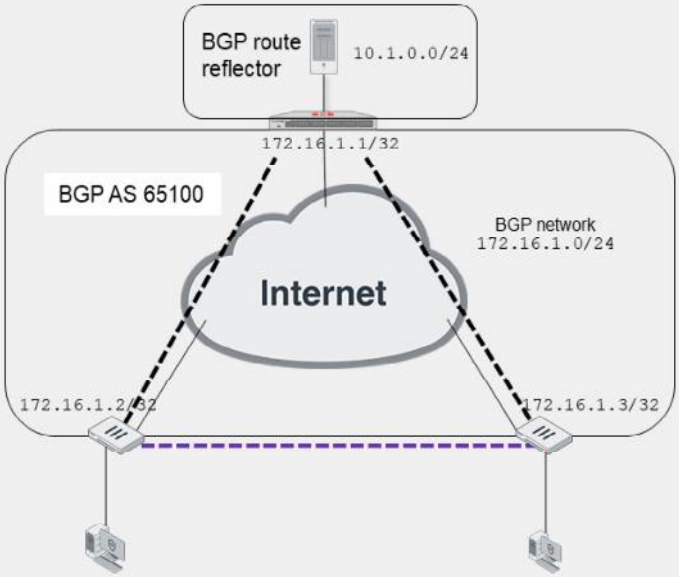
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hub IBGP Configuration

```
Hub # show router bgp
config router bgp
    set as 65100
    set router-id 172.16.1.1
    config neighbor-group
        edit "advpn"
            set remote-as 65100

            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 172.16.1.0 255.255.255.0
            set neighbor-group "advpn"
        next
    end
    config network
        edit 1
            set prefix 10.1.0.0 255.255.255.0
        next
    end
....
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

This slide shows the following IBGP configuration in the hub:

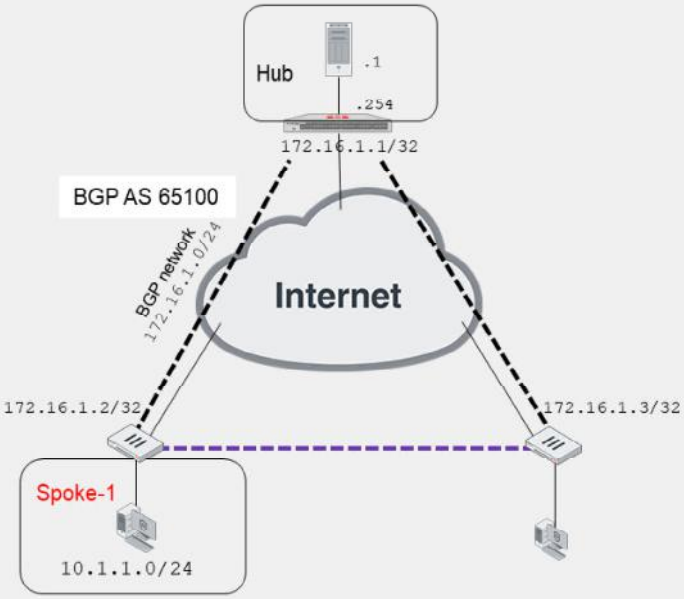
- Configure a BGP neighbor group. All the spokes are part of it.
- Create a neighbor range with a prefix that includes all the spokes. When configured this way, you don't need to define each spoke individually as a neighbor.
- If you are using IBGP for ADVPN, you must configure the hub as a route reflector. So, routes learned from one spoke are forwarded to the other spokes.
- Add the local network(s) behind the hub to be advertised over BGP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Spoke IBGP Configuration

```
Spoke-1 # show router bgp
config router bgp
    set as 65100
    set router-id 172.16.1.2
    config neighbor
        edit "172.16.1.1"
            set remote-as 65100
        next
    end
    config network
        edit 1
            set prefix 10.1.1.0 255.255.255.0
        next
    end
...
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

This slide shows the following IBGP configuration in one of the spokes:

- Configure the hub as a BGP neighbor.
- Define the internal network that will be advertised over the BGP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ADVPN and FortiManager VPN Manager

- Some settings need to be changed from their default values:
  - Set protected networks to **all**
  - Enable ADVPN in the IPsec phase 1
    - Use a script
  - Ensure that the **Add Route** option is disabled on the hub
  - Enable `net-device` on spokes
    - Use a script
  - Configure IP addresses on the IPsec virtual interfaces
  - Configure dynamic routing
    - Use a script to enable route reflector if using IBGP
  - Phase1 name_0
    - FortiManager creates phase1 name_0 interface when using VPN console

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

If you are configuring ADVPN on FortiManager using the VPN manager, remember the following:

- Set the protected networks to **all**.
- Use scripts to enable ADVPN in phase 1.
- Disable the option **Add Route** on the hub .
- Use scripts to enable `net-device` on spokes.
- Configure IP addresses on the IPsec virtual interfaces.
- Configure dynamic routing. If you are using IBGP, use a script to enable route reflector on the hub.
- It is important to know that when creating phase-1 using a FortiManager VPN console, the phase-1 name is created with an underscore and a zero (phase1name_0). For example, a phase-1 named VPN will be created as VPN_0.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

VPN Manager—ADVPN

- Change the address object for **Protected Subnet** to **all**:

	Name		Role	Default VPN Interface	Protected Subnet
☐	NGFW-1 (root)	View Details >	Hub	external	all
☐	Spoke-1 (root)	View Details >	Spoke	external	all
☐	Spoke-2 (root)	View Details >	Spoke	external	all

FORTINET Training Institute

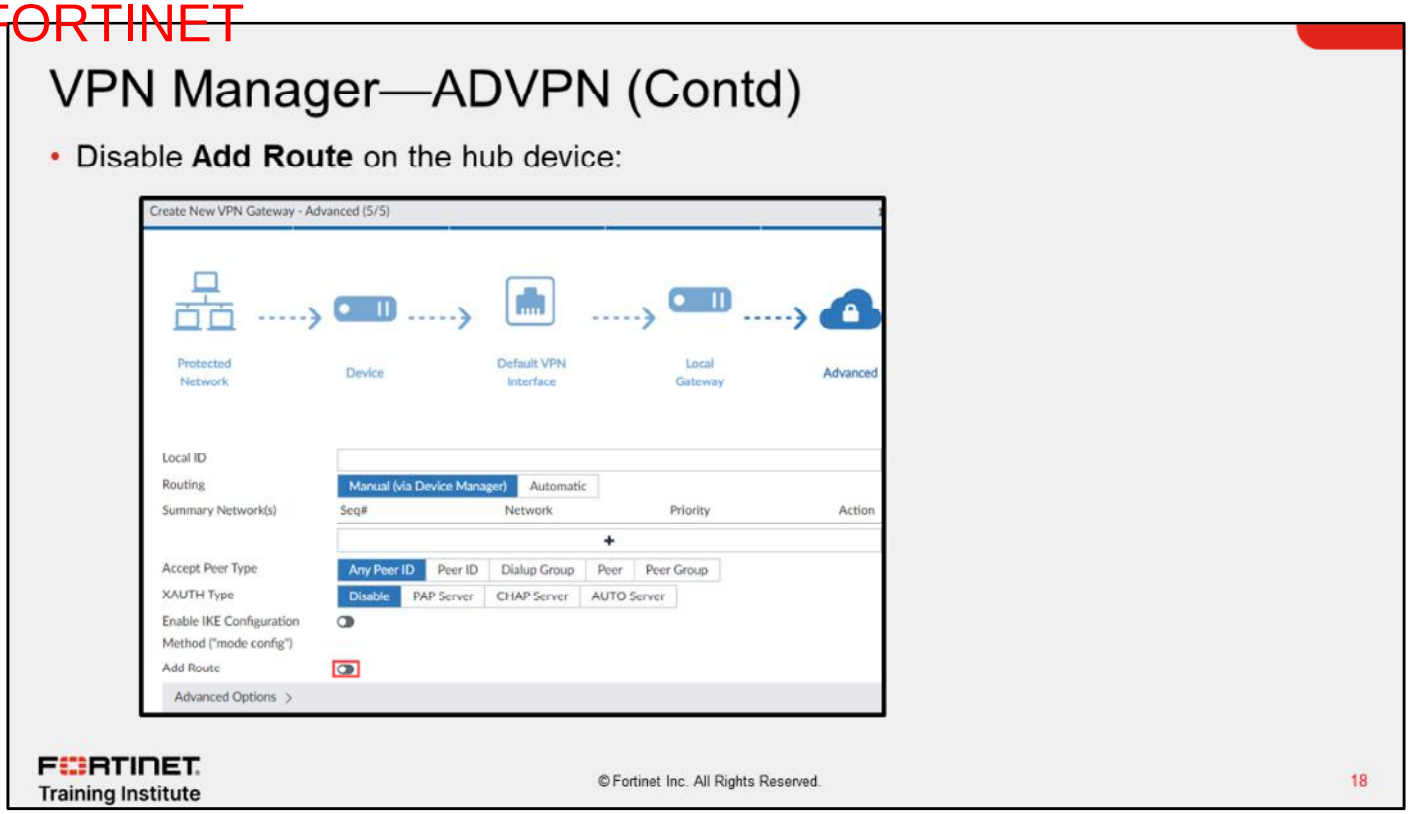
© Fortinet Inc. All Rights Reserved.

17

The configuration of the **Protected Subnet** is shown when editing the gateways in **VPN Manager** > **Ipsec VPN** > **VPN Communities**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



For ADVPN, disable **Add Route** under the VPN gateway configuration of the hub.

This prevents the hub from adding routes based on IKE negotiations. For that purpose, ADVPN uses a dynamic routing protocol instead.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Spoke Routing Table Before On-Demand Tunnel

```
Spoke-1 # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 172.16.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i0.0.0.0/0        172.16.1.1      0              100      0        0 100 i <-/1>
*>i10.1.0.0/24      172.16.1.1      0              100      0        0 i <-/1>
*> 10.1.1.0/24      0.0.0.0                        100  32768        0 i <-/1>
*>i10.1.2.0/24      172.16.1.3      0              100      0        0 i <-/1>
```

BGP next-hop must be accessible through tunnel

```
Spoke-1 # get router info routing-table all
S*      0.0.0.0/0 [10/0] via 100.64.3.254, port1, [1/0]
B       10.1.0.0/24 [200/0] via 172.16.1.1 (recursive via H2S_0 tunnel 100.64.1.1), 4d01h21m, [1/0]
C       10.1.1.0/24 is directly connected, port3
B       10.1.2.0/24 [200/0] via 172.16.1.3 (recursive via H2S_0 tunnel 100.64.1.1), 4d01h02m, [1/0]
C       100.64.3.0/24 is directly connected, port1
C       100.64.4.0/24 is directly connected, port2
S       172.16.1.0/24 [5/0] via H2S_0 tunnel 100.64.1.1, [1/0]
S       172.16.1.1/32 [15/0] via H2S_0 tunnel 100.64.1.1, [1/0]
C       172.16.1.2/32 is directly connected, H2S_0
```

Spoke-to-spoke traffic flows through the hub

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

After the tunnels between the hub and the spokes come up, you can run the commands shown on this slide on the spokes, to verify that routing updates are taking place.

This slide shows that Spoke-1 learned the routes to the hubs and to the networks of Spoke-2, through BGP. Spoke-2 is currently accessible through the hub.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ADVPN Tunnels

- IPsec tunnel list on Spoke-1 before on-demand tunnel

```
Spoke-1 # get ipsec tunnel list
NAME=H2S_0 REMOTE-GW=100.64.1.1:0
        P2NAME=H2S_0_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
TIMEOUT=518
```

Tunnel to the hub

- IPsec tunnel list on Spoke-1 after on-demand tunnel

```
Spoke-1 # get ipsec tunnel list
NAME=H2S_0 REMOTE-GW=100.64.1.1:0
        P2NAME=H2S_0_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
TIMEOUT=336
NAME=H2S_0_0 REMOTE-GW=100.64.5.1:0
        P2NAME=H2S_0_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
TIMEOUT=1772
```

On-demand tunnel

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

Using the `get ipsec tunnel list` command, you can verify which on-demand tunnels are up. It is important to note that on-demand tunnels remain active until their SAs are manually flushed, or until they time out.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Spoke Routing Table After On-Demand Tunnel

```
Spoke-1 # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 172.16.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i0.0.0.0/0        172.16.1.1      0             100      0        0 100 i <-/1>
*>i10.1.0.0/24      172.16.1.1      0             100      0        0 i <-/1>
*> 10.1.1.0/24      0.0.0.0                       100  32768        0 i <-/1>
*>i10.1.2.0/24      172.16.1.3      0             100      0        0 i <-/1>

Spoke-1 # get router info routing-table all

S*      0.0.0.0/0 [10/0] via 100.64.3.254, port1, [1/0]
B       10.1.0.0/24 [200/0] via 172.16.1.1 (recursive via H2S_0 tunnel 100.64.1.1), 4d01h32m, [1/0]
C       10.1.1.0/24 is directly connected, port3
B       10.1.2.0/24 [200/0] via 172.16.1.3 (recursive is directly connected, H2S_0_0), 00:01:48, [1/0]
C       100.64.3.0/24 is directly connected, port1
C       100.64.4.0/24 is directly connected, port2
S       172.16.1.0/24 [5/0] via H2S_0 tunnel 100.64.1.1, [1/0]
S       172.16.1.1/32 [15/0] via H2S_0 tunnel 100.64.1.1, [1/0]
C       172.16.1.2/32 is directly connected, H2S_0
                      is directly connected, H2S_0_0
C       172.16.1.3/32 is directly connected, H2S_0_0
```

BGP next hop does not change, while it is now accessible through on-demand tunnel

Spoke-2 network is now available through an on-demand tunnel

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

This slide shows the routing table after the on-demand tunnel is up.

It confirms that the network of Spoke-2 is directly accessible using the on-demand tunnel: `H2S_0_0`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Configure ADVPN
- ✓ Implement IBGP with ADVPN

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

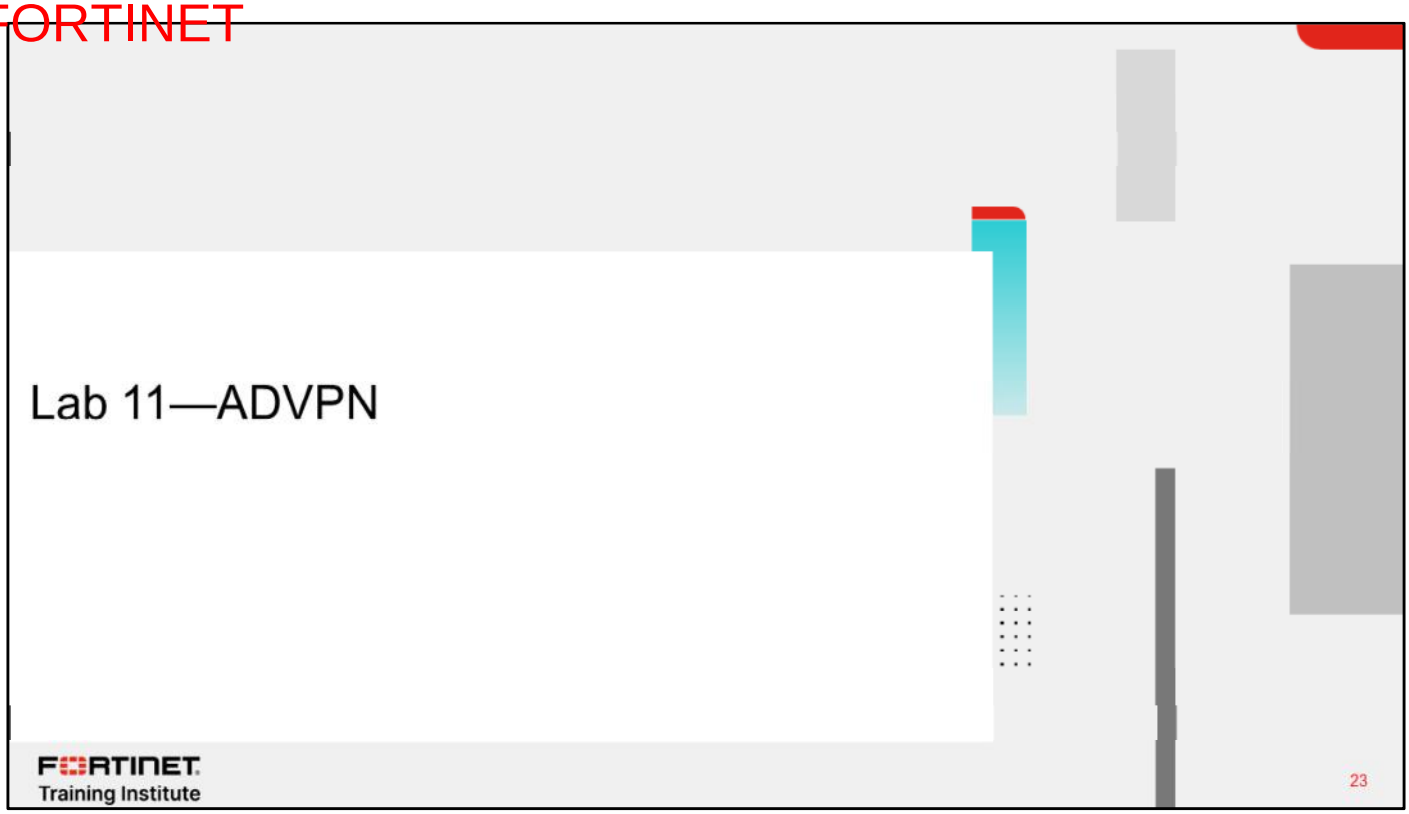
22

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

By mastering the objectives covered in this lesson, you learned about ADVPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



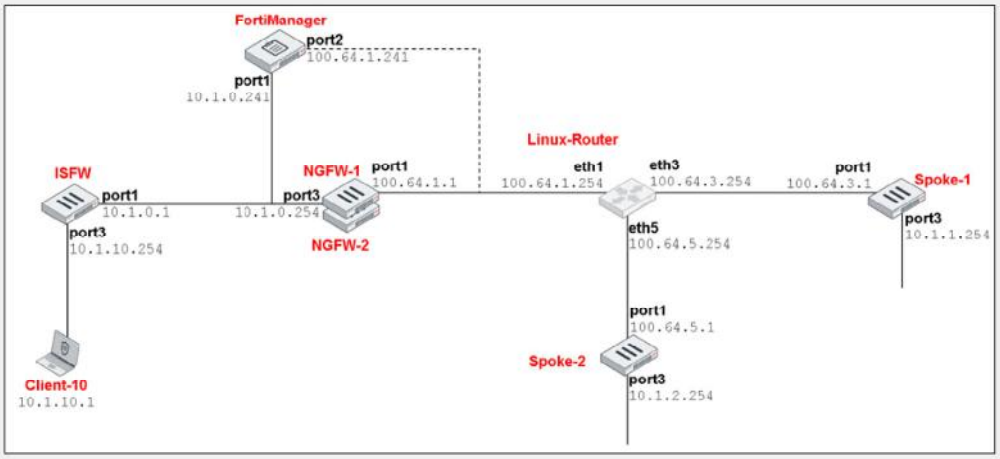
Now, you will work on *Lab 11–ADVPN*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lab 13—ADVPN

- On each FortiGate:
  - Enable ADVPN
  - Assign an IP address to the IPsec interface
  - Configure IBGP with route reflector



FORTINET Training Institute

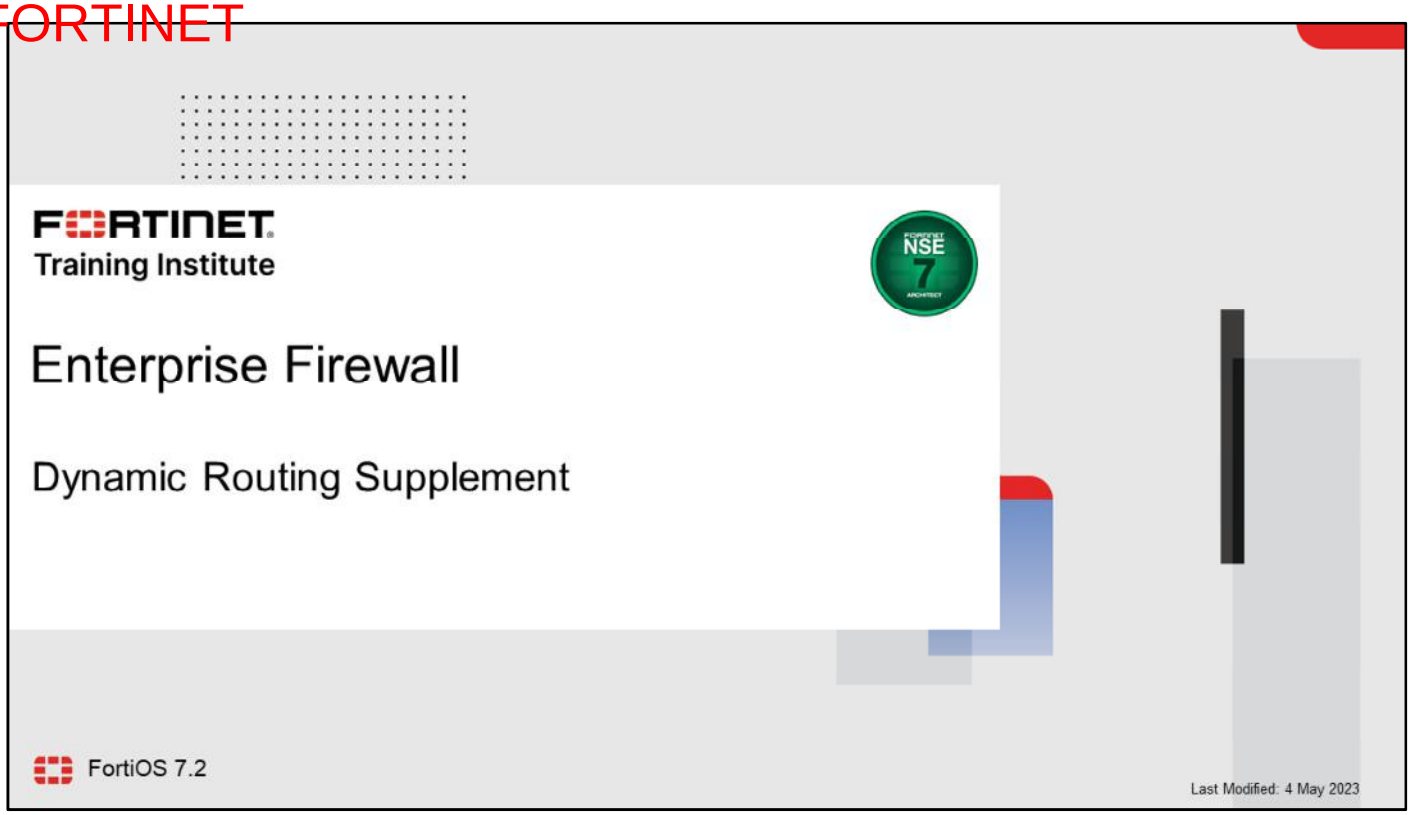
© Fortinet Inc. All Rights Reserved.

24

In this lab, you will run CLI and TCL scripts to configure ADVPN and IBGP on three FortiGate devices (NGFW1, Spoke-1 and Spoke-2).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will review Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) concepts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

In this section, you will review OSPF concepts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Overview

- Link state protocol
- Advantages:
  - Scalable to large networks
  - Faster convergence than distance-vector routing protocols
  - Relatively quiet during steady-state conditions
    - Periodic refresh every 30 minutes
    - Otherwise, updates only sent when there are changes
- Disadvantages:
  - May require planning and tuning to optimize performance
  - May be difficult to troubleshoot in large networks

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

3

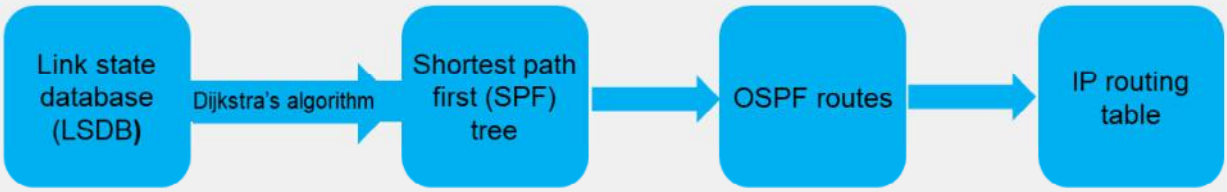
With a link state protocol like OSPF, every router has a complete view of the network topology. Advantages of OSPF include scalability and fast convergence. Every 30 minutes, routers advertise their OSPF information again. Between these 30-minute intervals, routers send updates only if they detect topology changes.. So, it is a relatively quiet protocol, as long as the network topology is stable. In large networks, using OSPF requires good planning and may be difficult to troubleshoot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Components

- Link state database (LSDB): Each router maintains identical databases describing the network topology
- From the LSDB, and using Dijkstra's algorithm, each router builds a tree with the shortest paths
- The tree gives an OSPF route to each destination
- OSPF can inject routes into the IP routing table



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

Each router in the same area has identical and synchronized databases. You will learn about OSPF areas later in this lesson. An OSPF router uses the information in the LSDB and Dijkstra's algorithm to generate an OSPF tree, which contains the shortest path from the local router to each other router and network. This tree gives the best route to each destination, which is the information that OSPF can inject into the device routing table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Link State Advertisement

- Routers exchange link state advertisements (LSAs) to maintain consistent databases
  - Network changes generate LSAs
  - LSDBs are composed of all received LSAs
- A link state update consists of an OSPF header and a string of LSAs
  - Each LSA has its own header
  - Routers acknowledge the receipt of LSAs

IP header	OSPF header	Number of LSAs	LSA 1	LSA 2	…	LSA *n*

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

The topology information exchanged by OSPF peers is contained in LSAs. The LSDB of a router is populated with information from the local LSAs and all the LSAs received from other routers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Cost

- Metric in OSPF is cost:
  - 16-bit positive number (1 to 65,535)
- Routes with lowest cost are most preferred
- Routing decisions made on total cost of a path to the final destination

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

If there are multiple OSPF routes to the same destination subnet, OSPF selects the route with the lowest cost. Each router interface is associated with an interface cost, which is usually related to how fast or preferable that interface is. An OSPF route cost is the sum of the costs of all interfaces to the final destination.

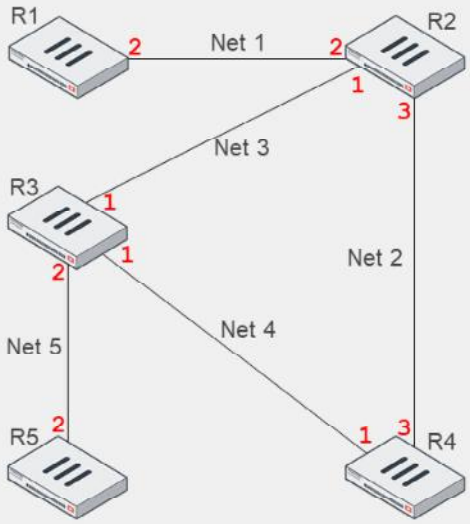
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LSDB

- Each router advertises its locally connected subnets
- LSDBs in all routers contain information about the network topology

```
Link State Database (network/cost)
R2    Net 1/2, Net 2/3, Net 3/1
R1    Net 1/2
R3    Net 3/1, Net 4/1, Net 5/2
R4    Net 2/3, Net 4/1
R5    Net 5/2
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

This slide and the next slide explain how an OSPF router builds its OSPF tree. The initial information for each router is the locally connected networks, together with the OSPF cost for each interface. In the example shown on this slide, the router `R2` has three locally connected subnets: subnet `Net 1` with a cost of `2`, subnet `Net 2` with a cost of `3`, and subnet `Net 3` with a cost of `1`. Router `R1` has only one subnet connected: `Net 1` with a cost of `2`, and so on.

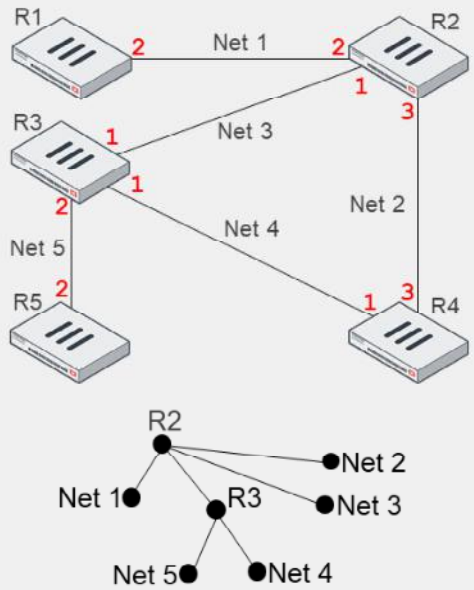
Each router starts advertising its locally connected subnets by sending LSAs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Tree

- Routers use Dijkstra's algorithm to determine the best path to each destination
  - The best path has the lowest overall cost
  - The destination is either a network or a router
- Routers build an OSPF tree
  - During each iteration, the router maps all known paths to a destination and chooses the lowest path
  - The router repeats the process until it discovers the best path to each destination



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

OSPF routers use Dijkstra's algorithm to determine the best route to each destination. The best routes can be represented as a tree with the local router at the root. Dijkstra's algorithm is a recursive process that the router repeats multiple times until it finds the best routes. For example, this slide shows the OSPF tree for router R2. It indicates that the best route to Net 5 and Net 4 is through R3, and that Net 1, Net 2, and Net 3 are locally connected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Areas

- A logical collection of OSPF networks and routers
- Defined with a 32-bit number
  - IP address format
    `0.0.0.10`
  - Single decimal format
    `10`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

You can segment an OSPF network into areas. Each area is identified by a unique number, which you can define in decimal or IP address formats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Areas (Contd)

- When a network is broken up into areas, routers maintain separate LSDBs for each area
- Advantages:
  - Smaller LSDB tables
  - Impact of a topology change is minimized outside the area
  - You can summarize routes on the area borders
- Disadvantages:
  - More complex to troubleshoot
  - Network design considerations

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

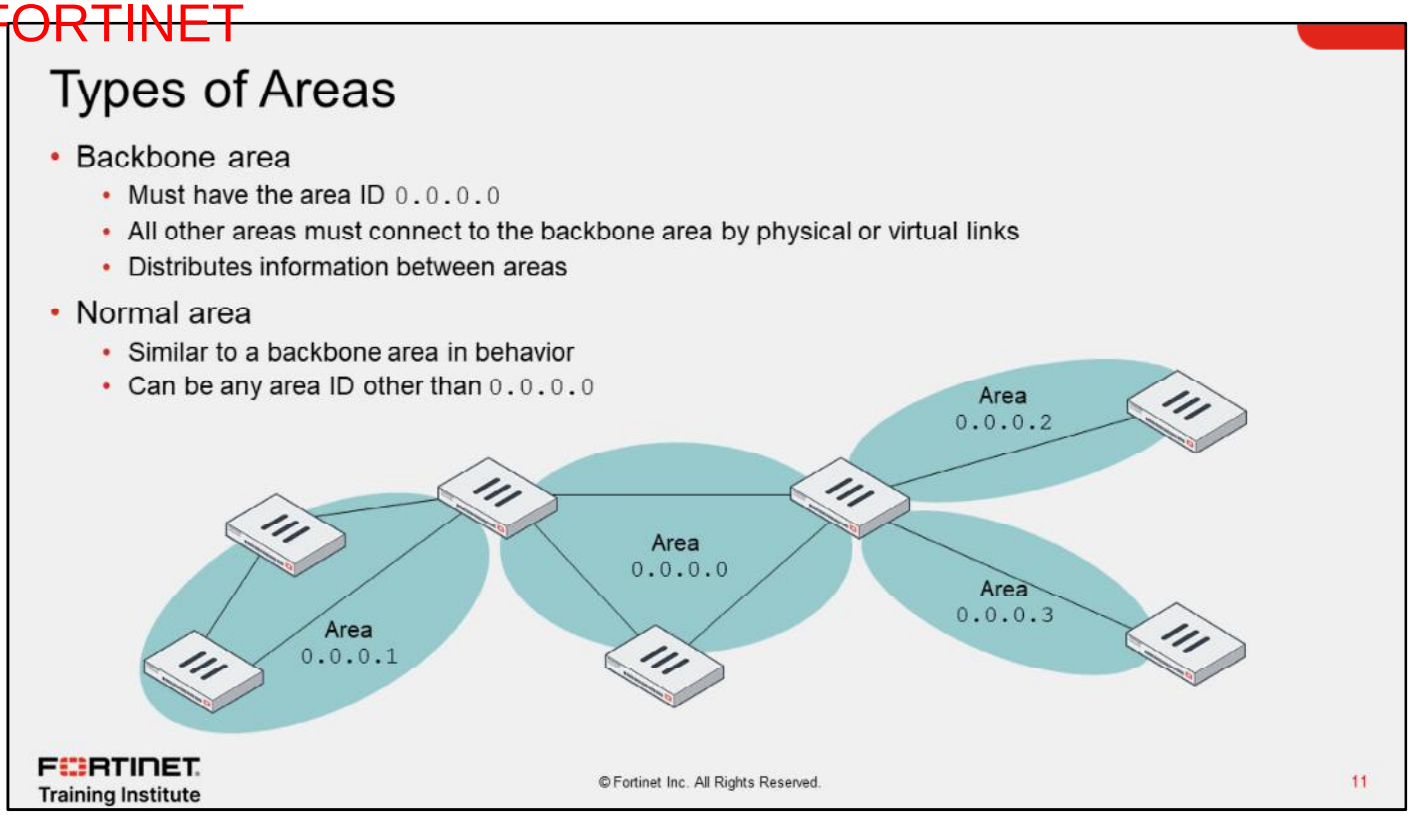
Each area has its own separate LSDB. All routers in the same area maintain an identical copy of the LSDB of an area. As you will learn in this lesson, a router can belong to more than one area. In those cases, the router maintains multiple LSDBs—one LSDB for each area connected to it.

Segmenting big OSPF networks into areas reduces the sizes of the LSDB tables. Additionally, a topology change does not impact the whole network, but only the area where the change happens.

Using OSPF areas requires good planning and may complicate the troubleshooting process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



All OSPF networks must have at least one area—the backbone area. The backbone area is the core of the network, and all the other areas connect to it in a hub-and-spoke topology.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Router Types

- Internal router
  - All connected interfaces belong to the same area
  - Maintains one LSDB and one OSPF tree
- Area border router (ABR)
  - A router with interfaces in multiple areas
  - One LSDB and one OSPF tree for each connected area
  - Always connected to the backbone
- Backbone router
  - Has at least one interface in the backbone area
- Autonomous system boundary router (ASBR)
  - Imports external (non-OSPF) routes into OSPF
  - Has at least one source of routing information that is not of OSPF origin

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

An internal OSPF router has all its interfaces connected to the same area. So, it maintains only one LSDB.

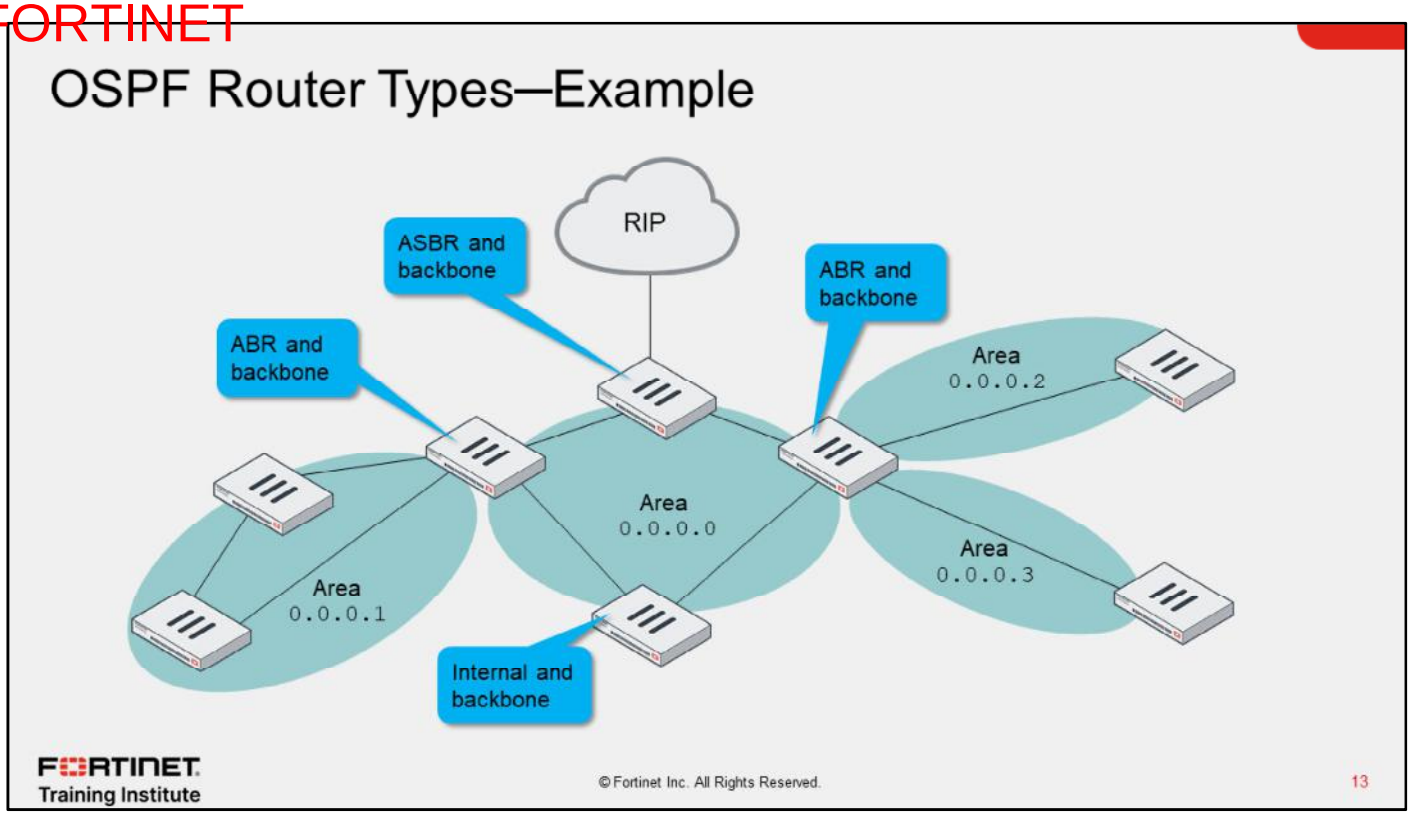
On the other hand, an ABR is connected to multiple areas, so it keeps multiple LSDBs.

A backbone router has at least one interface connected to the backbone area.

An ASBR redistributes non-OSPF routes into the OSPF network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows an example of each router type.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Network Types

- Point-to-point
  - A pair of routers connected through a point-to-point link
- Broadcast (multi-access)
  - Supports more than two attached routers
  - Supports the sending of a single message to all routers (multicast)
  - Example: Ethernet networks
- Point-to-multipoint
  - Supports more than two attached routers
  - Does not support multicast

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

There are three types of OSPF networks:

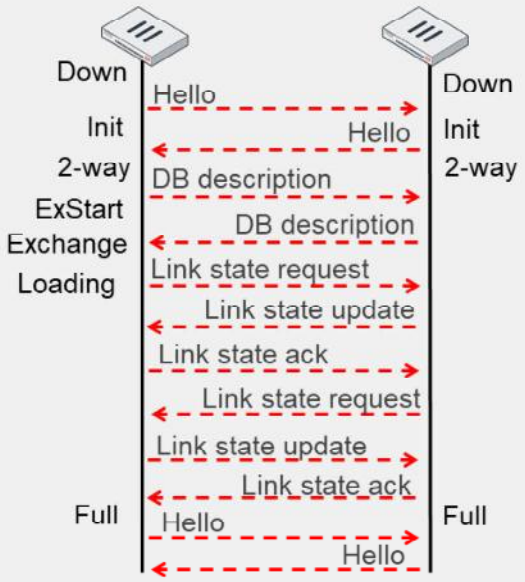
- Point-to-point networks contain only two peers, one at each end of a point-to-point link.
- Broadcast networks support more than two attached routers. They also support sending messages to multiple recipients (broadcasting).
- Point-to-multipoint networks support more than two attached routers. However, they do not support broadcasting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Forming an Adjacency

- **Down**: Initial state
- **Init**: A hello packet was seen from a non-adjacent neighbor
- **2-way**: Communication is bidirectional between the two routers
- **ExStart**: A primary and secondary relationship is negotiated
- **Exchange**: Database description packets are exchanged
- **Loading**: LSA information is exchanged
- **Full**: LSDBs are identical



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

An OSPF session between two OSPF peers is called an adjacency. This slide shows the initial interchange between two peers that are forming an adjacency. Any new adjacency goes through different states: Init, 2-way, ExStart, Exchange, Loading, and Full. The Full state indicates that the adjacency has successfully formed, and both routers have identical copies of the LSDB.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Adjacency Requirements

- Requirements for forming an adjacency:
  - Primary IP addresses of peers are in the same subnet with the same mask
  - Interfaces of peers are the same type and in the same OSPF area
  - Hello and dead intervals of peers match
  - Each peer has an unique router ID
  - OSPF IP MTUs match
  - OSPF authentication, if enabled, is successful

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

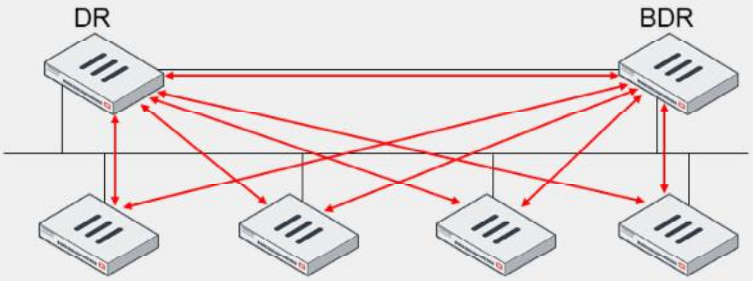
This slide lists the requirements for two peers to form an OSPF adjacency. If any of the requirements are not met, the adjacency fails and will not reach the Full state.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Designated Router

- In multi-access networks, one designated router (DR) and one backup DR (BDR) are elected
  - Router priority: highest priority wins, 0 = never become a DR
  - Router ID: highest ID wins
- If the DR fails, the BDR takes the DR role
- Full adjacencies are only formed to the DR and BDR to reduce resource utilization



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

In any multi-access network there is one DR and one BDR. The OSPF network elects the router with the highest priority as the DR. If two or more routers are tied with the highest priority, the network elects the router with the highest OSPF ID.

The BDR monitors the DR status. If the DR fails, the BDR takes the DR role.

Other routers form adjacencies only with the DR and BDR. The DR forwards the link state information from one router to another. This simplifies the number of adjacencies required in multi-access networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

OSPF Destination Addresses

- On broadcast networks, OSPF uses two multicast destination addresses
  - 224.0.0.5 AllSPFRouters
    - Hello packets
    - Either the DR or BDR sends LSA updates and acknowledgements
  - 224.0.0.6 AllDRouters
    - All other routers send LSA updates and acknowledgements
- On point-to-point networks
  - 224.0.0.5 AllSPFRouters
    - Routers send all packets to this address
- Some OSPF packets may be unicast
  - Database description (DD) packets exchanged
  - LSA retransmissions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

This slide shows the multicast addresses that OSPF uses in broadcast multi-access, and point-to-point networks. Keep in mind that OSPF also uses unicast addresses for LSA retransmissions and database description packets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LSA Types

- There are 11 LSA types. These are the five most common types:
  - Type 1: Router link advertisement
    - Describes the links of a router. Confined within an area.
  - Type 2: Network link advertisement
    - Describes all the routers (if more than one) in a multi-access network. Confined within an area.
  - Type 3: Summary link advertisement
    - Describes summarized networks within an area. Generated by an ABR.
  - Type 4: AS summary link advertisement
    - Describes the path to an ASBR router
  - Type 5: AS external link advertisement
    - Describes external destinations originated on an ASBR. Generated by the ASBR.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

There are 11 LSA types. This lesson covers the following five most commonly used types:

- Type 1 describes all the links connected to a router.
- Type 2 describes all the routers (if more than one) in a multi-access network.
- Type 3 describes the networks within an area (only generated by an ABR).
- Type 4 describes the path to reach an ASBR.
- Type 5 describes the external destinations originated by an ASBR.

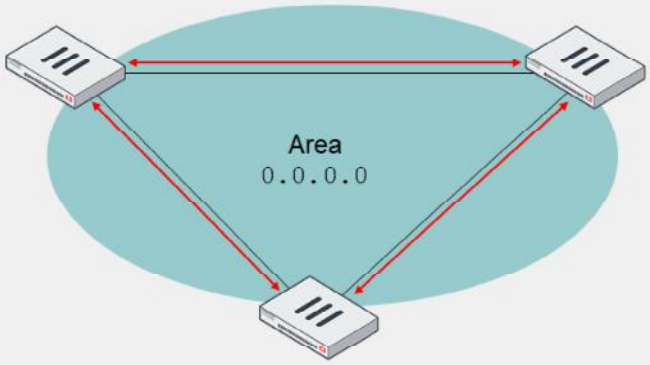
You will see examples of each of these five types in the next slides.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Router Link Advertisements (Type 1)

- Advertised by every OSPF router in an area
- Describe router network connections within that area



FORTINET Training Institute

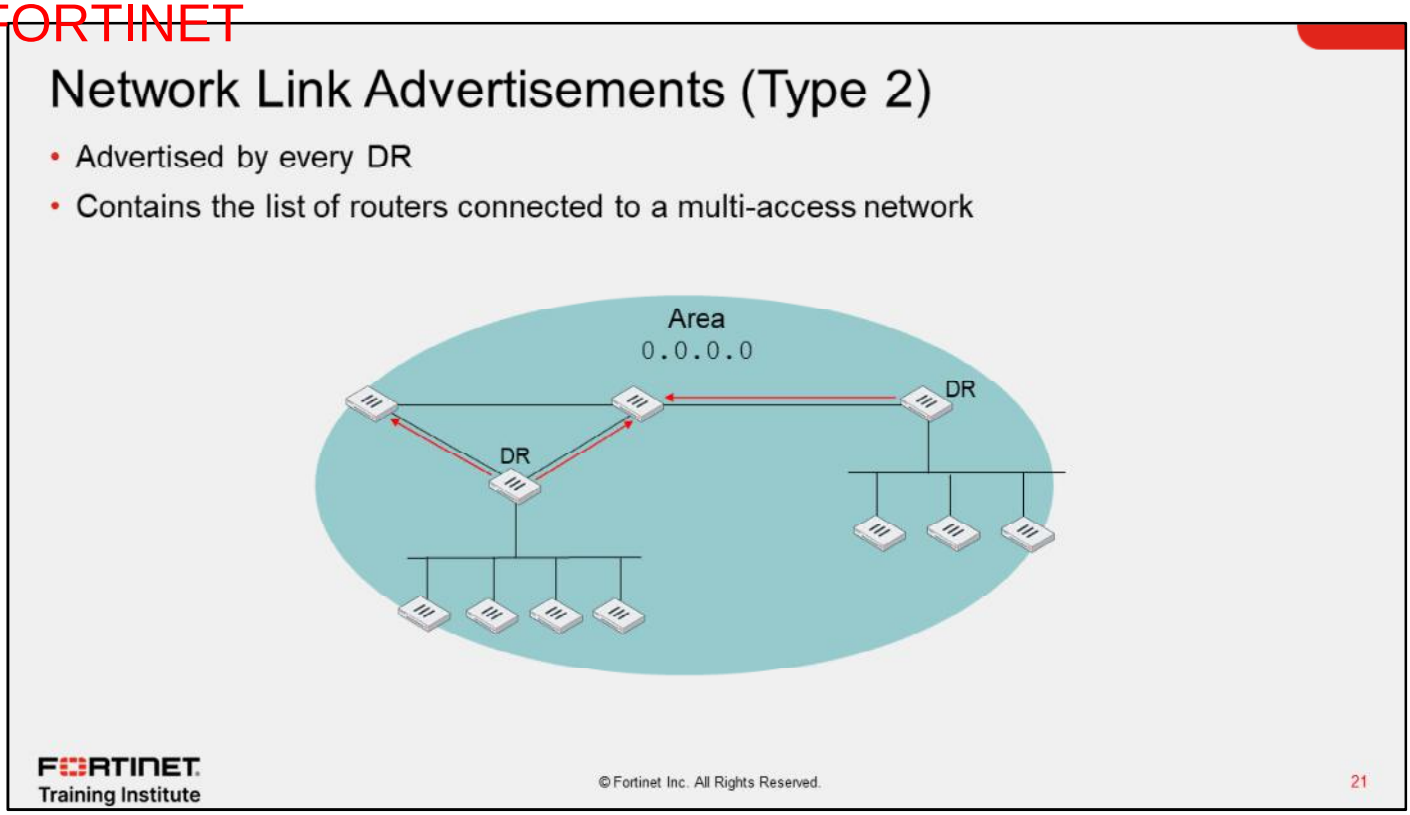
© Fortinet Inc. All Rights Reserved.

20

Type 1 describes the networks connected to a router. They are advertised by all the routers in an area. Type 1 LSAs are not advertised outside the area where they originate.

Vouchers & Dumps are Available | WhatsApp +201224560923

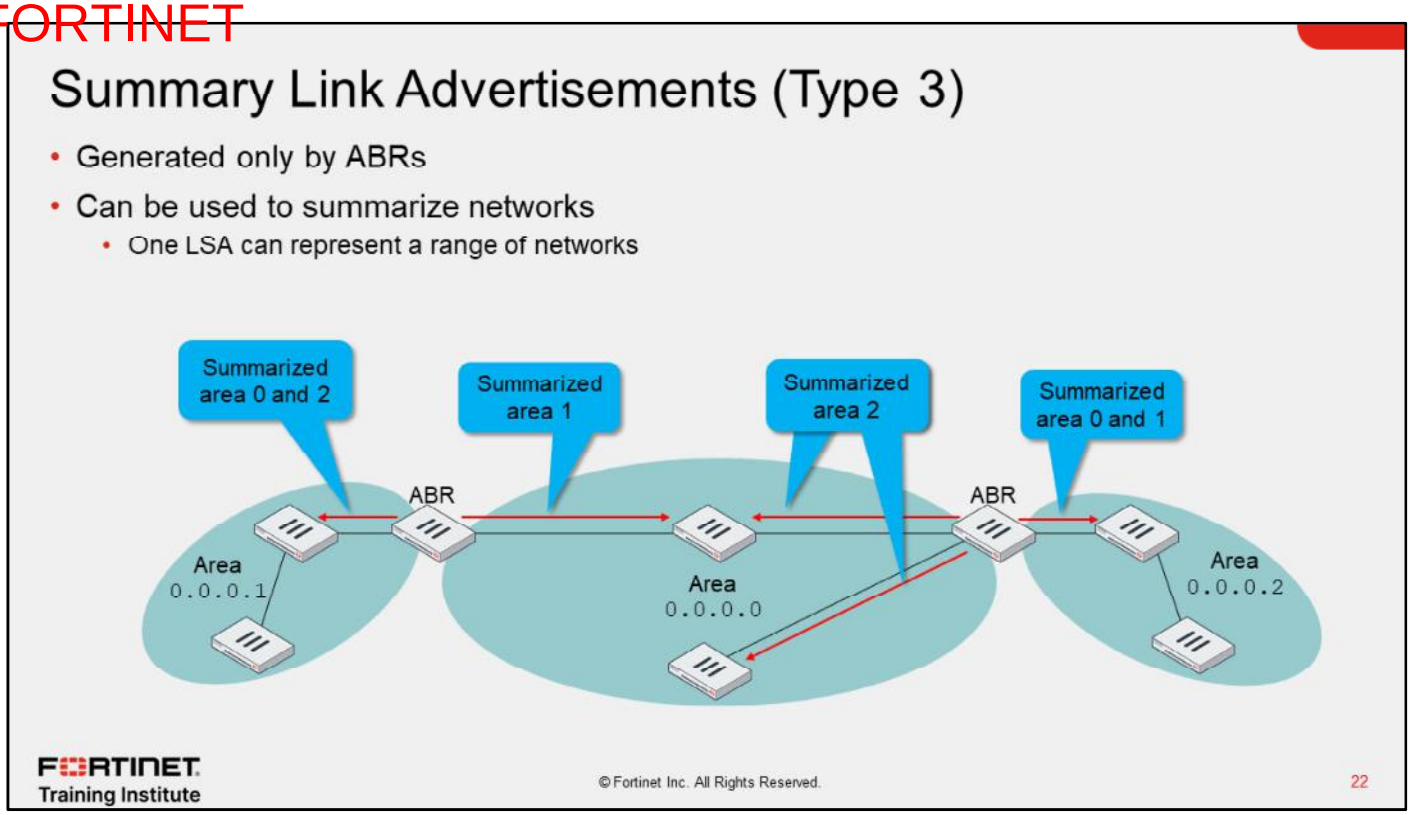
DO NOT REPRINT Brave-dumps.com
© FORTINET



Only DRs advertise Type 2 LSAs. In the example shown on this slide, the area has two multi-access networks, each of them with one DR. The two DRs advertise type 2 LSAs, which contain information about the other routers connected to their multi-access networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Type 3 LSAs contain summarized link state information. They are advertised only by ABRs. In the example shown on this slide, the ABR on the left sends type 3 LSAs to area 1. They contain link state information for the summarized subnets in areas 0 and 2. This same ABR also sends type 3 LSAs to the backbone area, with a summary of the subnets in area 1.

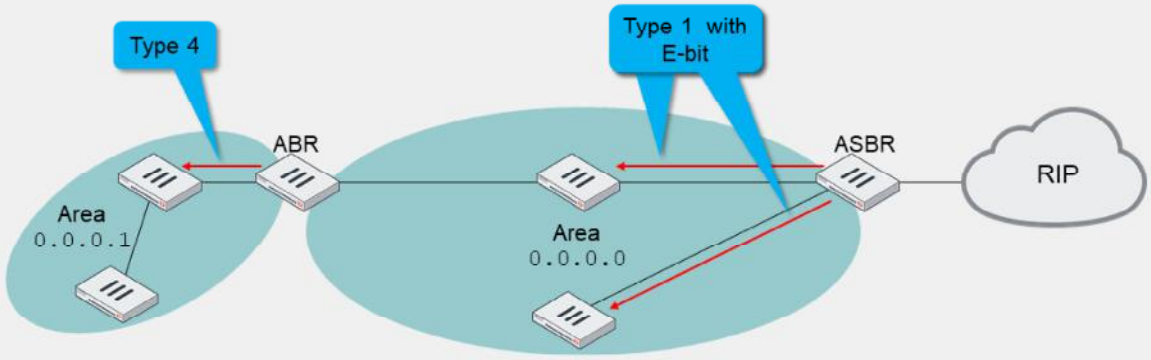
Something similar happens with the ABR shown on the right side of the diagram. It sends type 3 LSAs to area 2. They contain link state information for the summarized subnets in areas 0 and 1. This same ABR also sends type 3 LSAs to the backbone area, with a summary of the subnets in area 2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

AS Summary Link Advertisements (Type 4)

- An ASBR announces itself by setting the E-bit in its router link advertisements
- The ABRs in the same area generate a type 4 advertisement to the other areas



FORTINET Training Institute

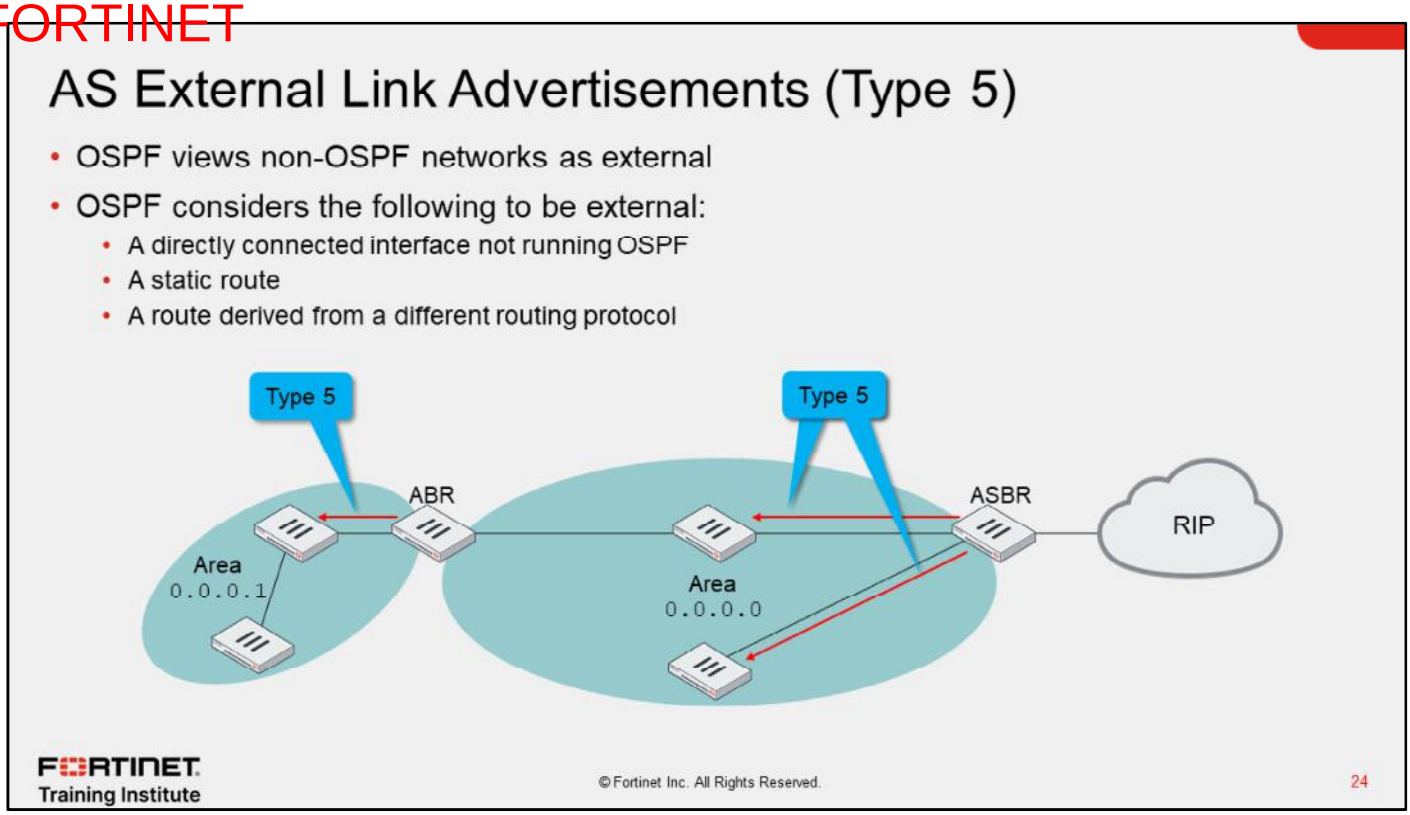
© Fortinet Inc. All Rights Reserved.

23

An ASBR advertises itself by sending type 1 LSAs. These LSAs have the E-bit on in the OSPF header. Like any other type 1, the LSAs with the E-bit are confined to the area where they originate. However, ABRs in the same area send a type 4 LSA to the other areas with information about how to reach the ASBR. In the example shown on this slide, an ASBR that is redistributing RIP routes into OSPF announces itself by sending type 1 LSAs to the backbone area. The ABR receives that LSA and sends a type 4 LSA to area 1.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The last type of LSA covered in this lesson is type 5. Type 5 LSAs are sent only by the ASBRs and are not confined to one area. They reach all the standard areas. They contain link state information for routes redistributed to OSPF (also called external routes).

Note that all the area examples in this lesson are standard areas. There are also stub and not-so-stubby areas (NSSA), which are not covered in this lesson. Type 5 LSAs are not advertised to stub or NSSAs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

External Route Metrics Types

- Type 1
  - Considered *close* to the AS
  - Metric is based on the sum of the internal and external costs
- Type 2
  - Considered *far away* from the AS
  - Metric is based on the external cost only
- OSPF router prefers a type 1 external router over a type 2

FORTINET Training Institute

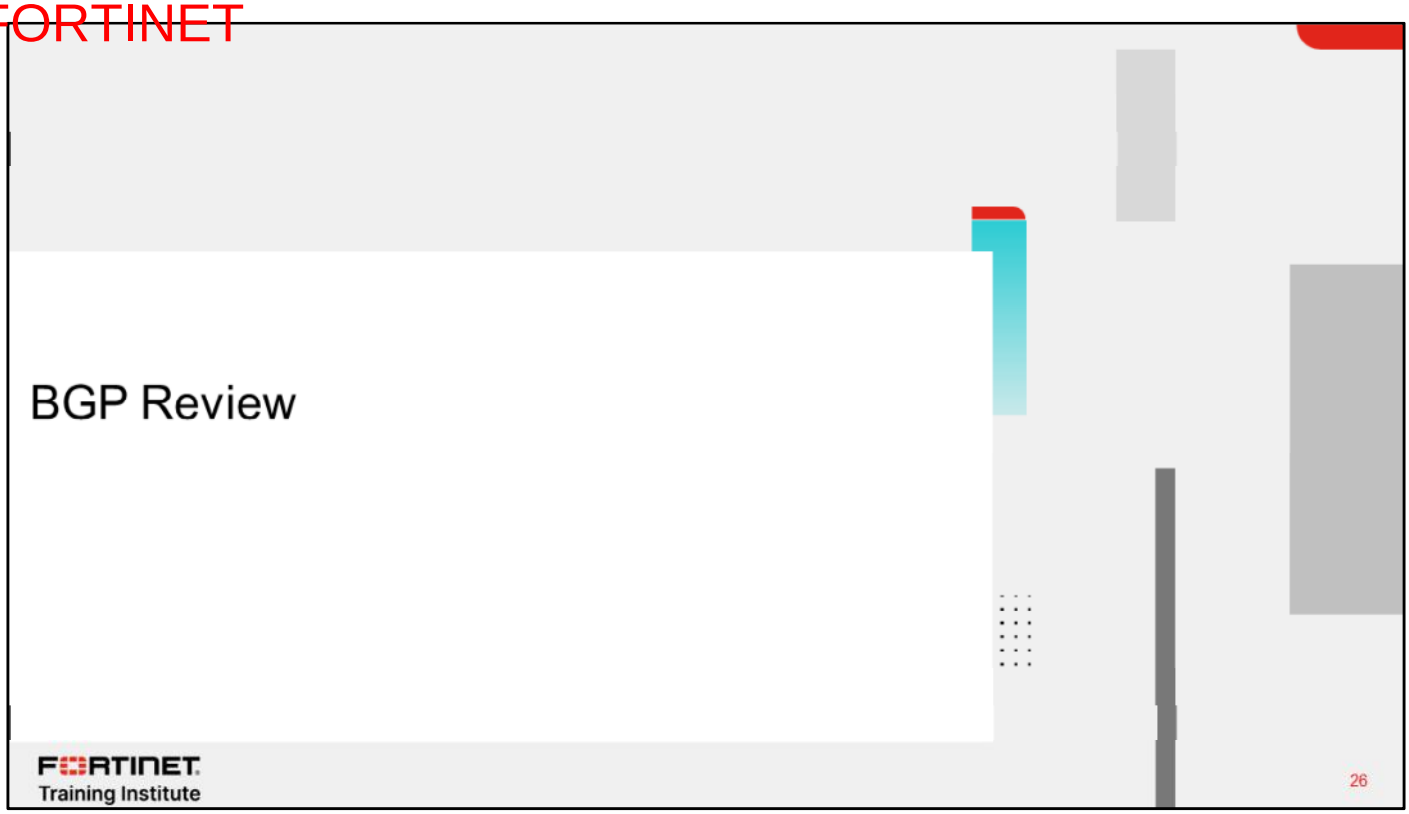
© Fortinet Inc. All Rights Reserved.

25

Each external route is assigned a metric. There are two types of external-route metrics. A type 1 metric is the sum of the external cost plus the internal cost to reach the ASBR. A type 2 metric is only the external cost (the internal cost is not considered). If there are two external routes to the same destination, one type 1 and one type 2, an OSPF router selects the type 1 route over the type 2 route.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this section, you will review BGP concepts and how to configure BGP on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

AS

- Set of routers and networks under the same, consistent administration
- An AS administrator is free to choose any internal routing architecture:
  - OSPF, RIP, and so on
- Each AS is identified by a unique number

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

An autonomous system (AS) is a set of routers and networks under the same administration. Each AS is identified by a unique number, and usually runs an interior gateway protocol, such as OSPF or RIP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BGP

- You can configure BGP to operate as EBGP or IBGP:
  - EBGP advertises routing updates across multiple ASs
  - IBGP advertises routing updates within the same AS
- BGP is typically used when the network requires:
  - Large numbers of routes
  - Strict control over which routes are announced or accepted
- BGP4 is the dominant EGP today
  - Example: the internet

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

BGP can serve one of two purposes: external BGP (EBGP) or internal BGP (IBGP).

An exterior gateway protocol (EGP) exchanges routing information between ASs. BGP4, which runs in the internet, is the dominant EGP protocol today. EBGP is typically used when strict control is required over a large number of routes.

Two EBGP routers exchange AS path information for destination prefixes or subnets. When two routers start an EBGP communication, the whole BGP routing table is exchanged. After that, only network updates are sent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BGP Components

- Speaker or peer:
  - Router that transmits and receives BGP messages, and acts on those messages
- Session
  - Connectivity between two peers

FORTINET Training Institute

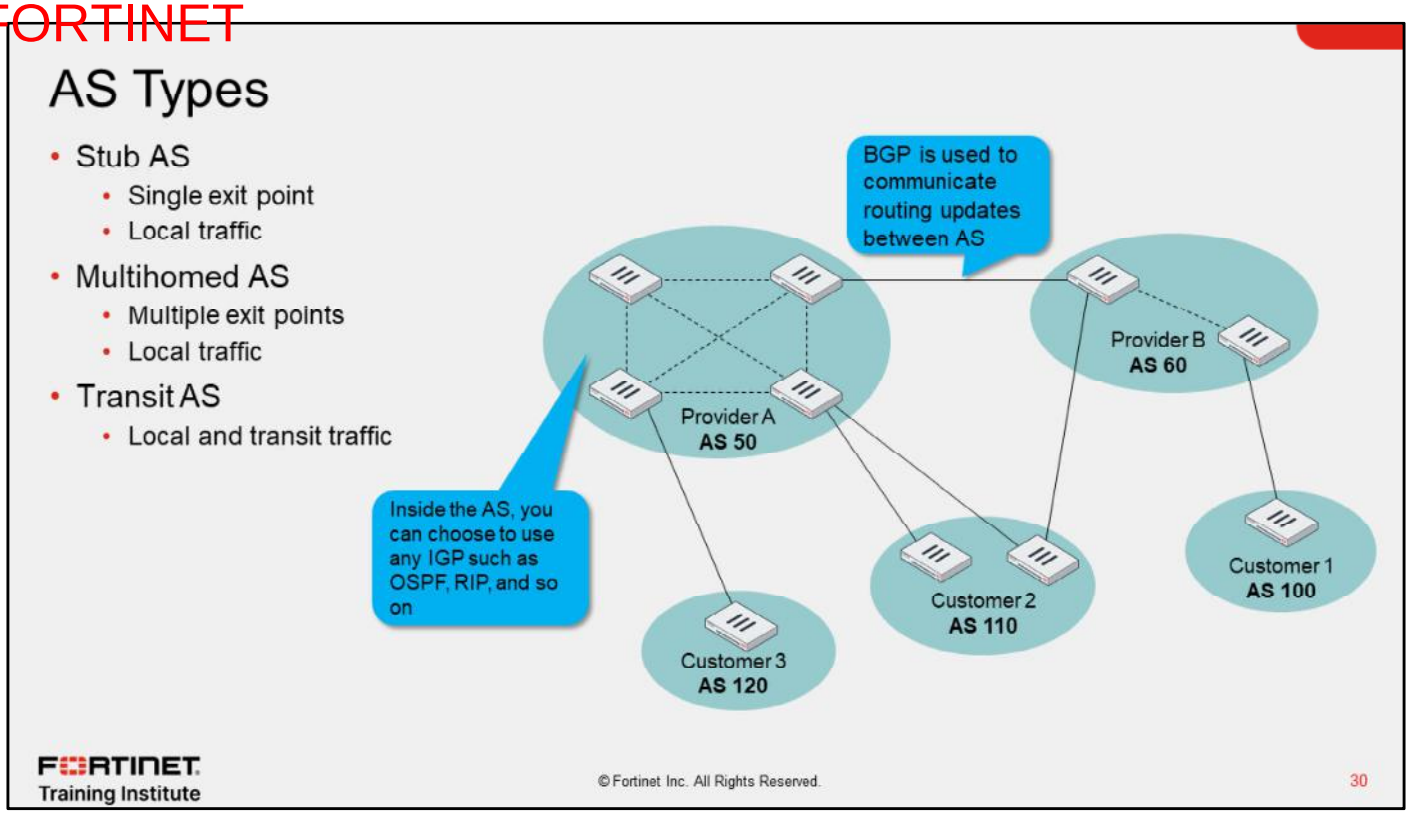
© Fortinet Inc. All Rights Reserved.

29

A BGP speaker or peer is a router that sends and receives BGP routing information. The connection between two BGP peers is called a BGP session.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

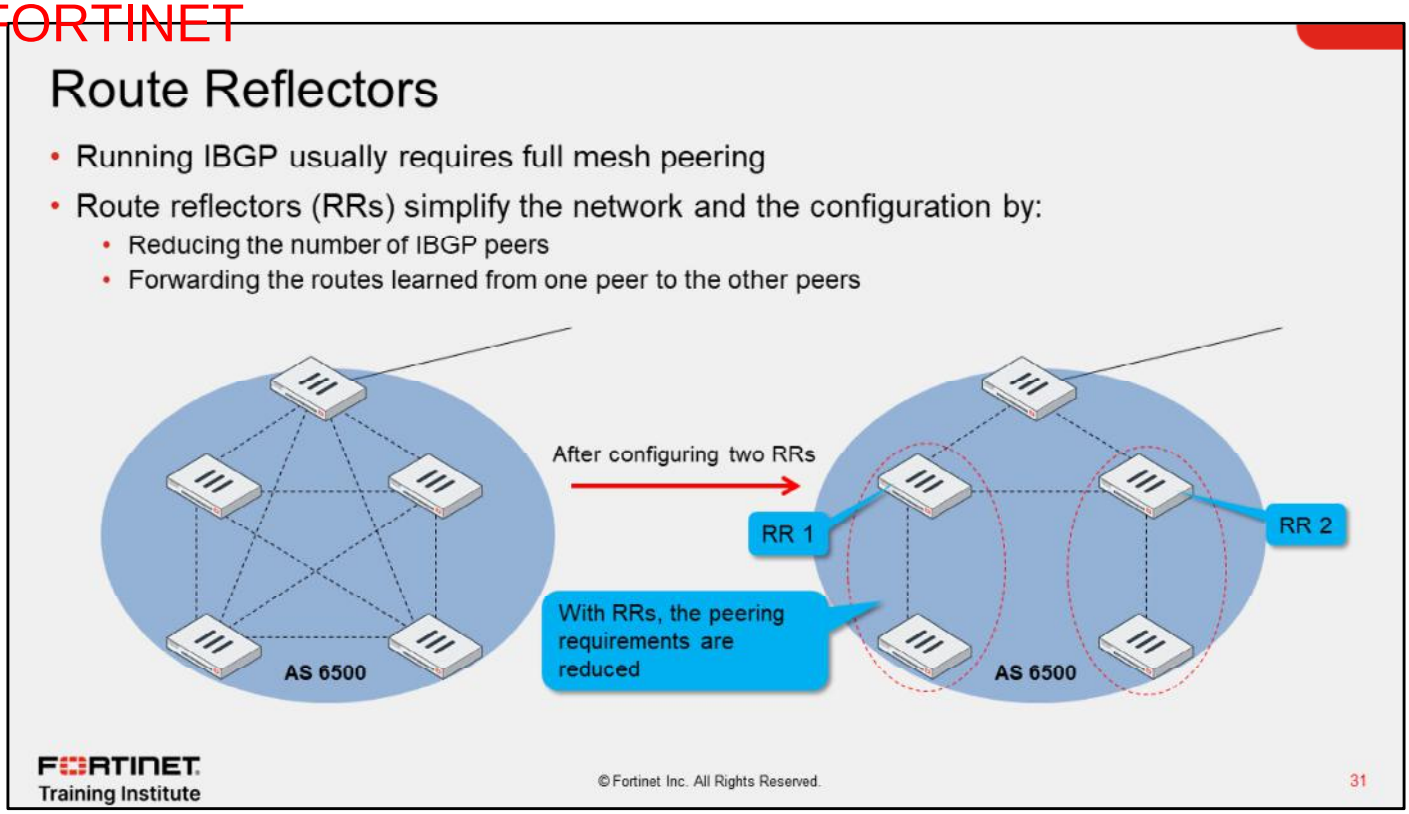


There are three types of ASs:

- A stub AS handles and routes local traffic only and has only one connection to another AS. One example is a company that is running BGP, and has its own AS number and one ISP connection.
- Multihomed AS also handles and routes local traffic only, but it has multiple connections to different ASs. One example is a company that is running BGP, and has its own AS number and multiple ISP connections.
- Transit AS handles and routes local traffic as well as traffic that originates and terminates in different ASs (transit traffic). An ISP is an example of a transit AS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When running IBGP, you usually need to configure full mesh peering between all the routers. In large networks, full mesh peering between routers can be difficult to administer and is not scalable.

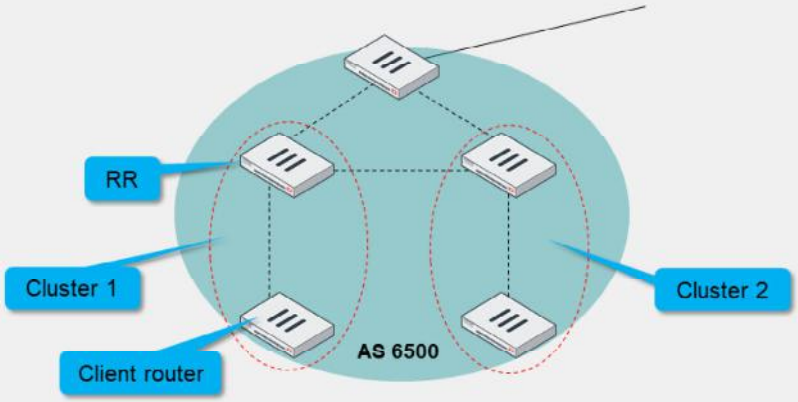
RRs help to reduce the number of IBGP sessions inside an AS. An RR forwards the routes learned from one peer to the other peers. If you configure RRs, you don't need to create a full mesh IBGP network. RRs pass the routing updates to other RRs and border routers within the AS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Route Reflectors (Contd)

- An RR and its clients form a cluster
- All clients in a cluster communicate with the RR only for routing updates
- The RR communicates all routing updates to peers external to the cluster



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

In a BGP RR configuration, the AS is divided into different clusters that each include an RR and clients. The client routers communicate route updates only to the RR in the cluster. The RR communicates with other RRs and border routers. FortiGate can be configured as either an RR or a client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

RIBs

- Routes are stored in routing information bases (RIBs)
  - RIB-in
    - Routing information learned from inbound update messages
    - Contains unprocessed routing information advertised to the local BGP speaker by its peers
  - Local RIB
    - Routing information that the BGP speaker selects after applying its local policies to the RIB-in
  - RIB-out
    - Routing information that the local BGP speaker selects to advertise to its peers

FORTINET Training Institute

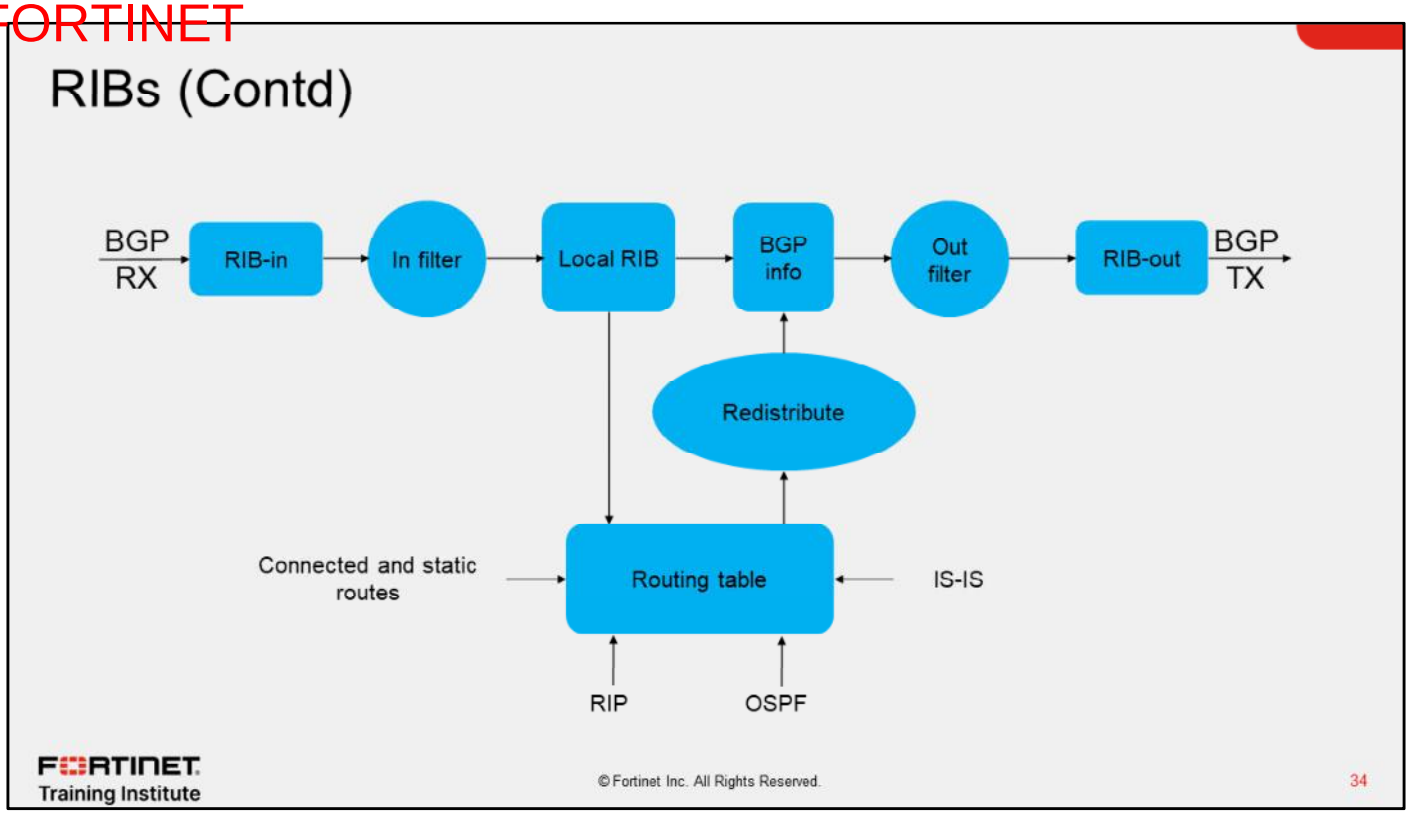
© Fortinet Inc. All Rights Reserved.

33

A BGP router stores routing information in three logical tables. The RIB-in table contains all routing information received from other BGP routers before any filtering. The local RIB table contains that same information after the filtering. The RIB-out table contains the BGP routing information selected to advertise to other BGP routers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows a flowchart that summarizes the BGP process. The BGP router stores the BGP routes it receives from other routers in the RIB-in table. The BGP router applies a filter, and the resulting routes are stored in the local RIB table. Then, the BGP router adds routes that were redistributed from the routing table, and applies another filter (outbound). The BGP router advertises the resulting routes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BGP Attributes

- BGP processes routes based on path information
- A path is a route to a destination
  - Paths are described by a set of attributes, including an AS list
  - Attributes help routers select the route to each destination

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

35

BGP routes traffic based on AS paths. Each AS path includes attributes, which BGP uses to select the best route to each destination. One of the attributes is the AS list, which contains the ASs through which the traffic must pass to reach the destination.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BGP Attributes (Contd)

- BGP path attribute categories
  - Well-known mandatory
    - Attributes are mandatory
  - Well-known discretionary
    - Attributes may or may not be included
  - Optional transitive
    - Attributes may or may not be accepted and can be passed outside of the local autonomous system
  - Optional non-transitive
    - Attributes may or may not be accepted and can't be passed outside of the local autonomous system

Supported Attributes	
ORIGIN	Well-known mandatory
AS_PATH	Well-known mandatory
NEXT_HOP	Well-known mandatory
MULTI_EXIT_DISC	Optional non-transitive
LOCAL_PREF	Well-known discretionary
ATOMIC_AGGREGATE	Well-known discretionary
AGGREGATOR	Optional transitive
COMMUNITY	Optional transitive

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

There are four types of BGP attributes:
- Well-known mandatory
- Well-known discretionary
- Optional transitive, which can be passed from one AS to another
- Optional non-transitive, which can't be passed from one AS to another

This slide shows a list of the BGP attributes and their attribute types that FortiGate supports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Route Selection

- Route selection tie breakers:
  1. Highest weight
  2. Highest local preference
  3. Prefer the path that originated locally
  4. Shortest AS path
  5. Lowest origin type
  6. Lowest multi-exit discriminator (MED)
  7. Lowest IGP metric to the BGP next-hop
  8. Prefer external paths (EBGP) over internal paths (IBGP)
  9. If ECMP is enabled, insert up to 10 routes in the routing table
  10. Lowest router ID

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

FortiGate uses some of the BGP attributes during the routing selection process. If all the attributes for multiple routes to the same destination match, and if ECMP is enabled, FortiGate shares the traffic among up to 10 BGP routes. If you don't enable ECMP, FortiGate uses the route that goes to the router with the lowest BGP router ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate BGP Implementation

- Scaling capabilities
  - No hard limits, system memory is the limitation
  - Number of neighbors, routes, and policies have an impact on the scaling capabilities
- By default, BGP doesn't originate any prefix
  - Redistribution or policies are required
- By default, all routes received are accepted

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

There are three important things to consider when you implement BGP on FortiGate.

First, there are no hardcoded limits. Limitations on the number of neighbors, routes, and policies depend exclusively on the available system memory.

Second, by default, FortiGate doesn't originate any prefix. You must enable redistribution, or manually indicate the prefixes that FortiGate originates.

Third, by default, FortiGate accepts all the prefixes it receives. Optionally, you can filter out or modify some prefixes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Protocol Redistribution

- A non-BGP route can be redistributed into BGP
- Optional route maps can filter out the redistribution of specific routes

```
# config router bgp
    config redistribute "static"
    set status enable
    end
  end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

By default, FortiGate BGP doesn't advertise prefixes. You can use the redistribution command to configure FortiGate to advertise prefixes. You can redistribute connected and static routes, and routes learned from other routing protocols, into BGP. Optionally, you can add route maps to filter the prefixes or modify some of their BGP attributes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Network Command

- An alternative to redistribution of protocols into BGP:

```
# config router bgp
    config network
      edit <id>
        set prefix <prefix>
  ...
```

- By default, the prefix is advertised only when it matches the destination subnet of an active route in the routing table
- To always advertise the prefix (regardless of the active routes):

```
# config router bgp
        set network-import-check disable
  end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

You can also use the `network` command to configure FortiGate BGP to advertise prefixes. However, an exact match of the prefix in the `network` command must be active in the routing table. If the routing table doesn't contain an active route with a destination subnet that matches the prefix, FortiGate doesn't advertise the prefix. You can change this behavior by disabling the `network-import-check` setting. After you disable the setting, FortiGate advertises all prefixes in the BGP network table, regardless of the active routes present in the routing table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Prefix Lists

- Prefix lists can be used to filter out the subnets being advertised to and being received from each neighbor

```
config router prefix-list
   edit filter-subnets
      config rule
         edit 1
           set prefix 10.1.0.0/16
           set action deny
         next
         edit 2
           set prefix 10.0.0.0/8
           set action permit
         next
      end
   end
end
```

```
config router bgp
  config neighbor
    edit 10.3.1.254
      set prefix-list-in filter-subnets
    next
  end
end
```

By default, traffic not matching the prefix list is denied

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

41

By default, the subnets under the `config network` command, and the subnets redistributed from other routing protocols, are advertised to all the neighbors.

With a prefix list, you can be more selective about which prefixes to advertise to each neighbor. Additionally, prefix lists allow you to select which prefixes you want to use from each neighbor. This example shows a prefix list that allows the prefix `10.0.0.0/8`, but blocks the prefix `10.1.0.0/16`. By default, all traffic that does not match a prefix list is denied. The prefix list is applied in the incoming direction from the neighbor `10.3.1.254`. The local FortiGate applies this filter for all prefix advertisements coming from `10.3.1.254`.

When applying a prefix list, all the prefixes that don't match an entry in the list are denied by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

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© 2023 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