DO NOT REPRINT
© FORTINET

Public Cloud Security Study Guide

for FortiGate 7.2

FORTINET®
Training Institute

DO NOT REPRINT
© 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

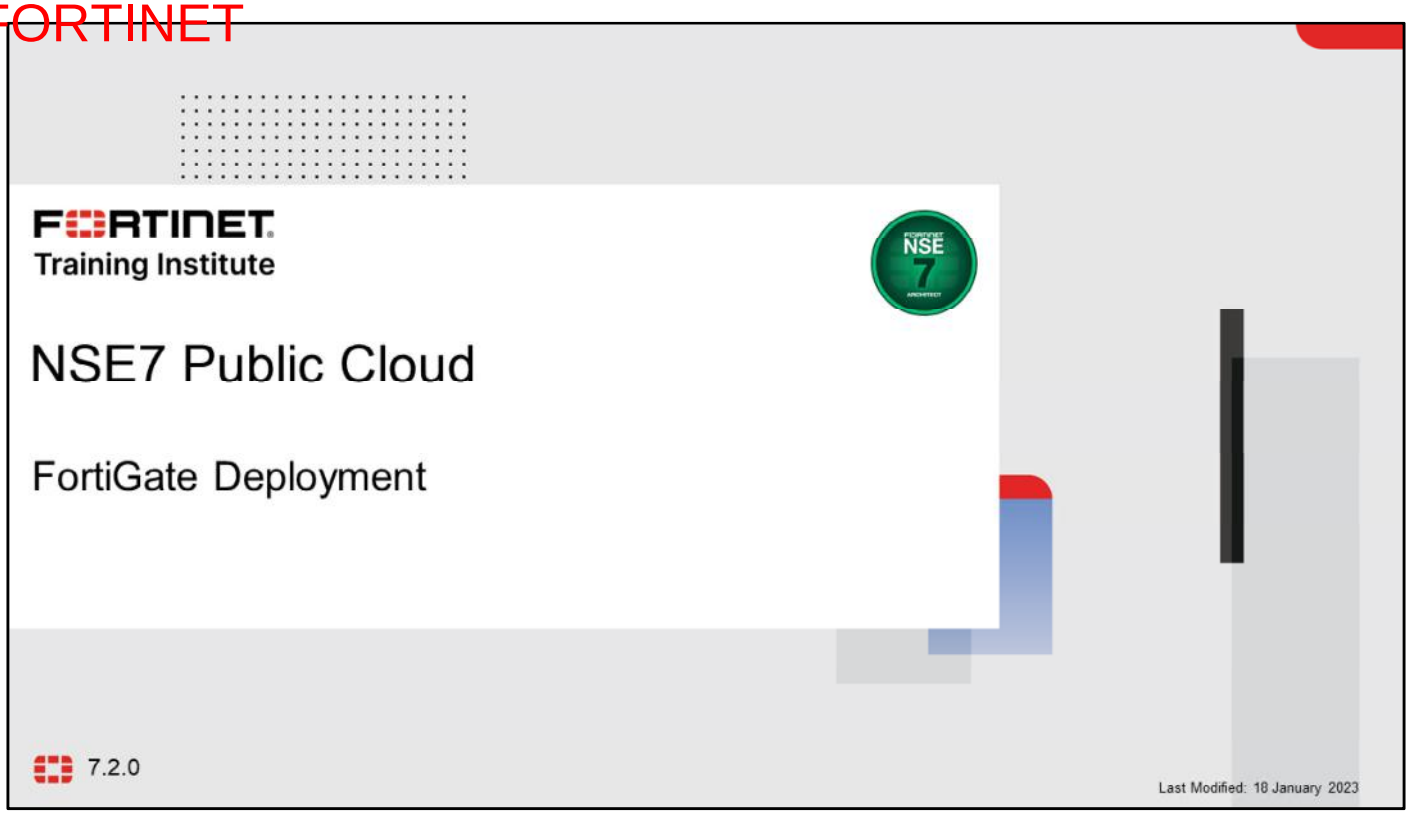
DO NOT REPRINT
© FORTINET

Brave-Dumps.com

TABLE OF CONTENTS

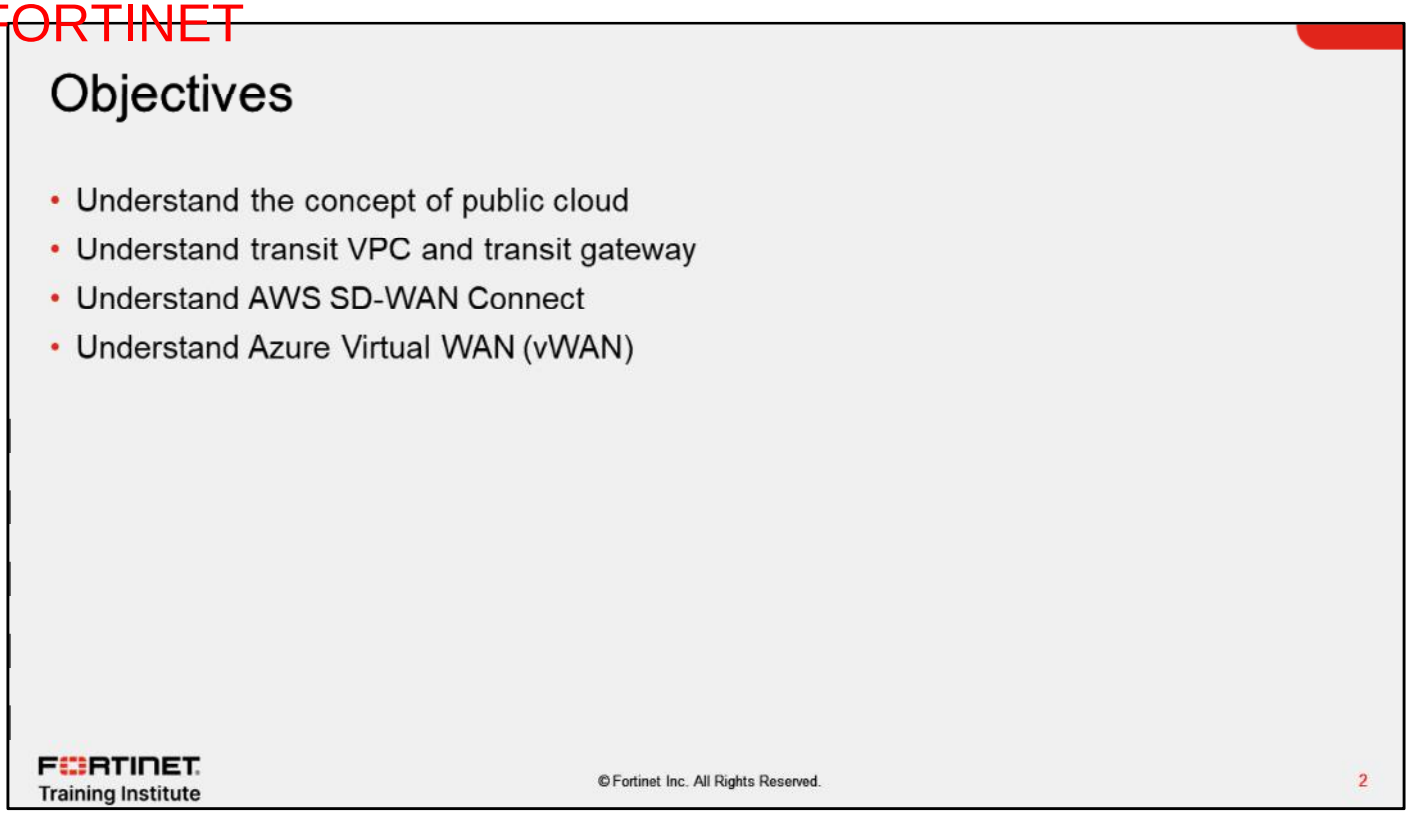
01 FortiGate Deployment **4**
02 Automation **47**
03 Deploying a FortiGate VM Using Terraform **90**
04 Troubleshooting **123**
05 FortiCNP **147**
Solution Slides **176**

DO NOT REPRINT
© FORTINET



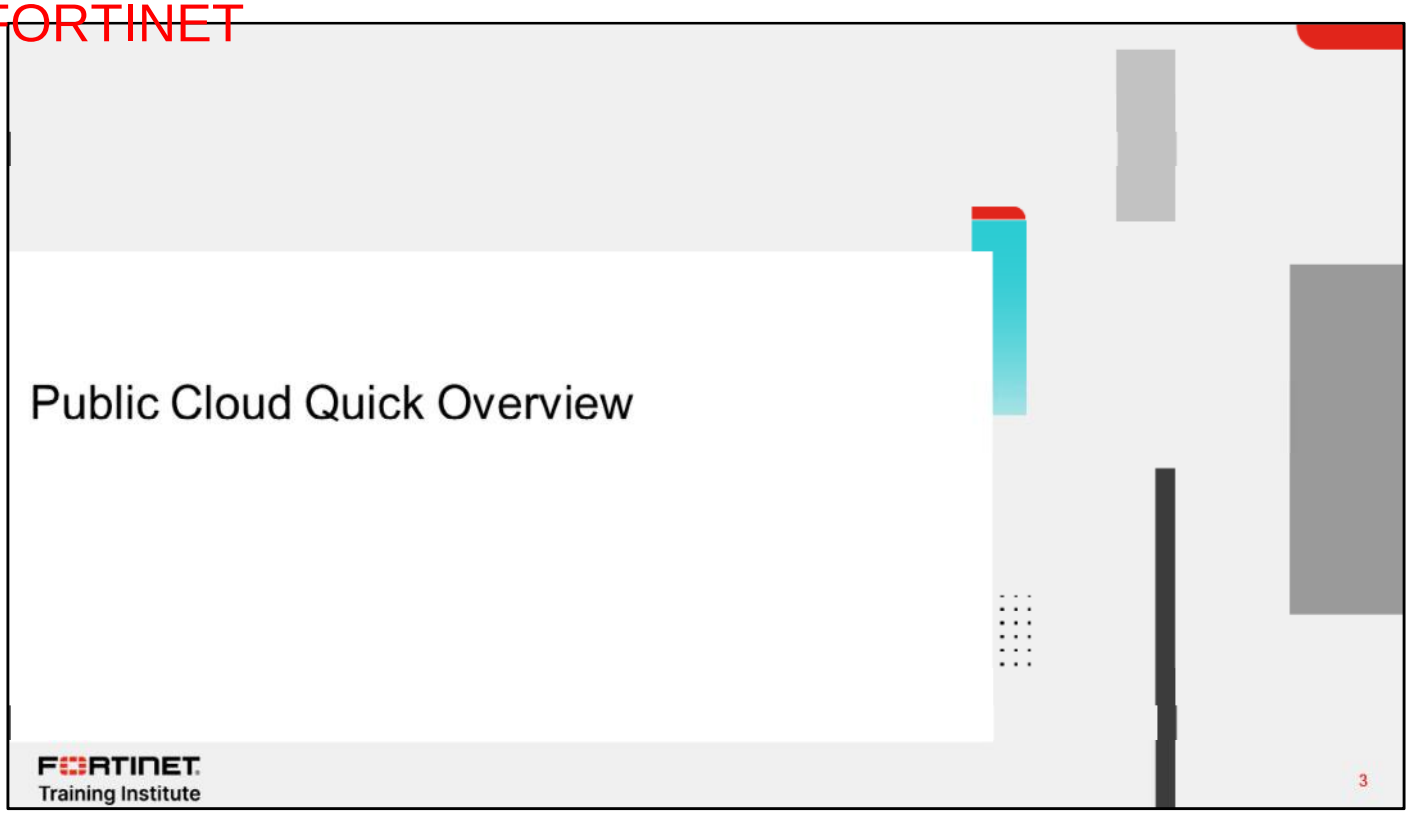
In this lesson, you will learn about public cloud FortiGate deployments in Amazon AWS and Microsoft Azure.

DO NOT REPRINT
© FORTINET



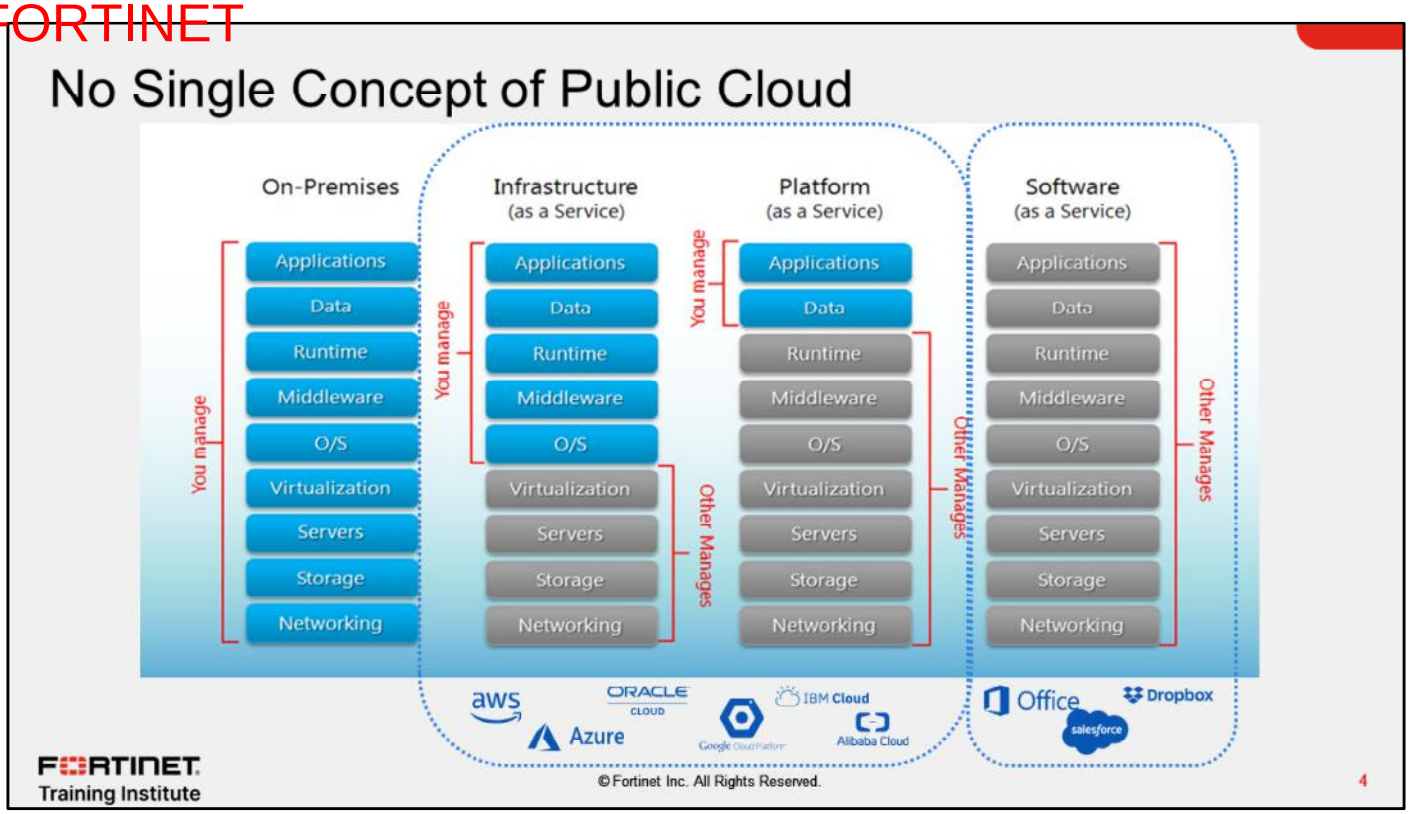
After completing this section, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



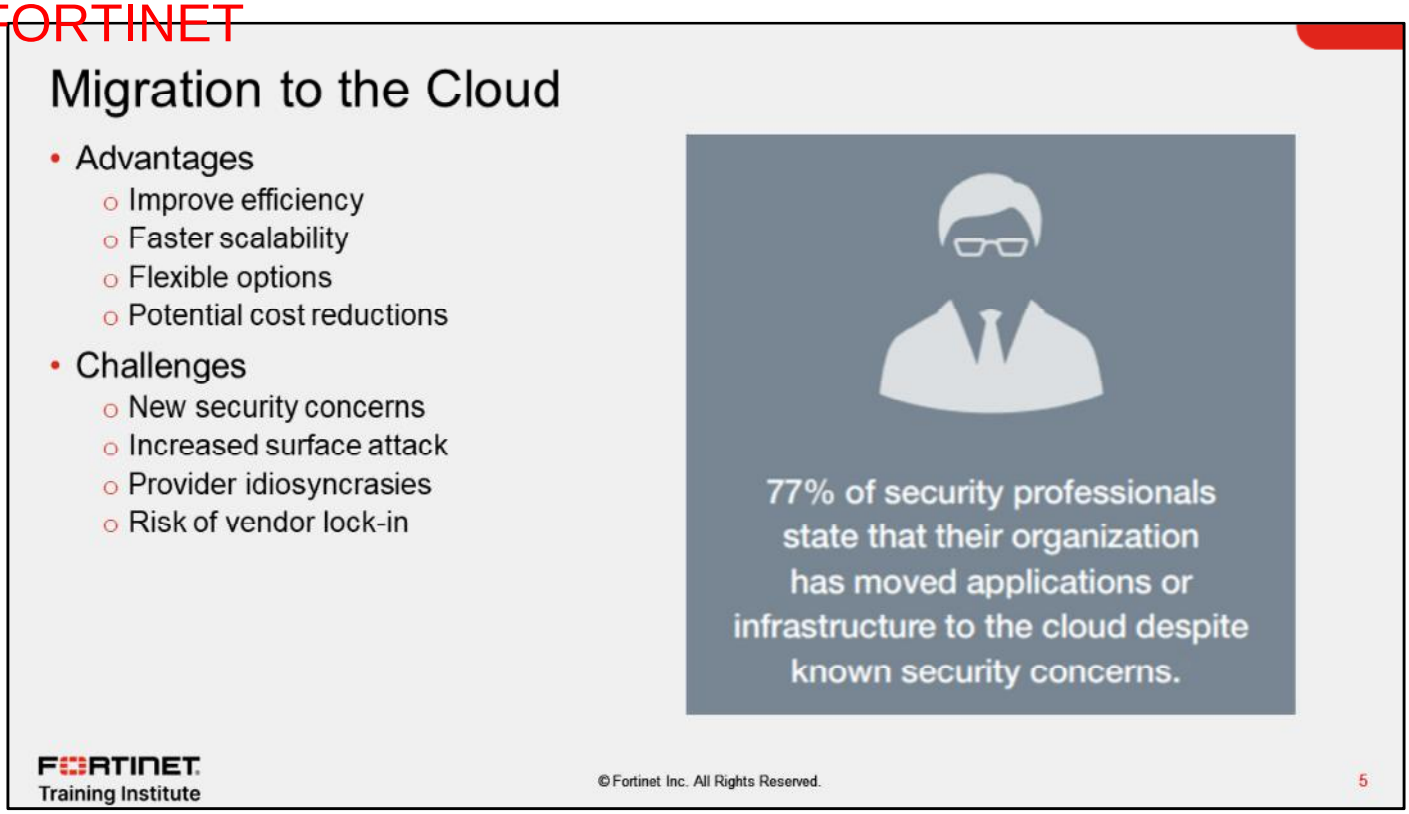
In this section, you will receive a quick overview of public cloud.

DO NOT REPRINT
© FORTINET



The term *public cloud* comes from the marketing world but, in the technology world, public cloud can mean one or more specific concepts. As shown on this slide, there are many different versions of a public cloud solution. In a traditional on-premises scenario, all the servers, switches, and databases run locally, on site. The VMs that you deploy during the labs are considered to be infrastructure-as-a-service (IaaS). In an IaaS solution, some parts of networking and services are managed by the vendor, and other parts are managed by the customer. There is also a solution called platform-as-a-service (PaaS), where the customer is responsible for programming applications and the rest of the services are managed by the vendor. Finally, in the software-as-a-service (SaaS) solution, the customer is using the services as a consumer for running applications. Some examples are Dropbox, Office365, and Salesforce. This course focuses on the IaaS solution.

DO NOT REPRINT
© FORTINET

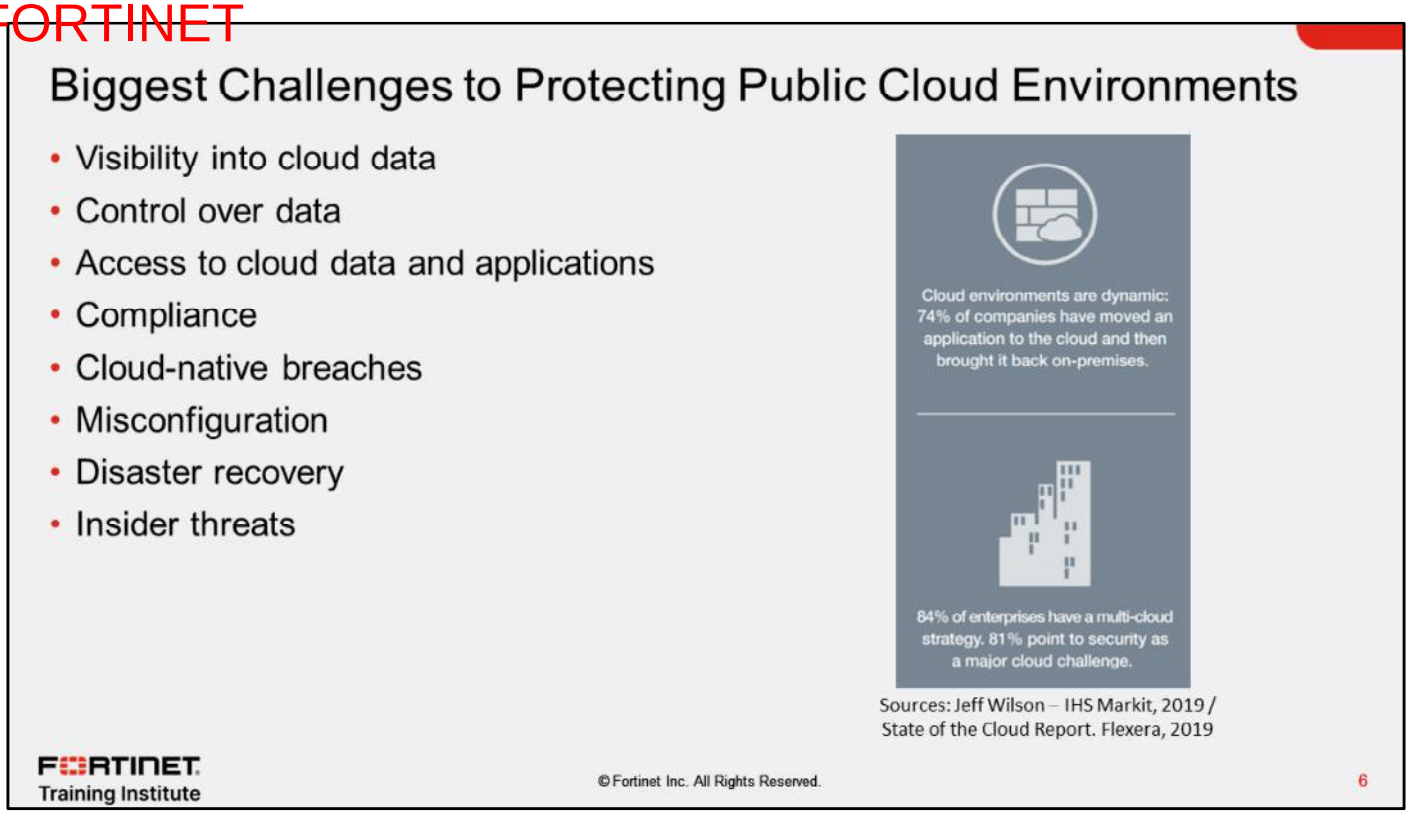


Almost every business has started to move some workloads and applications to the cloud—or at least plans to do so. These decisions are often driven by the desire to reduce costs and to improve operational efficiency and scalability by taking advantage of the flexibility that the cloud provides

Cloud service providers offer a wide range of possible deployment models. Businesses can take advantage of SaaS applications and services, such as Salesforce or Box. Alternatively, applications designed and deployed in on-premises environments can be lifted to IaaS or PaaS deployments, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure, and IBM Cloud.

Wary of cloud service provider lock-in and aiming to deploy each application and workload in the cloud for which it is best suited, many organizations have adopted a multi-cloud infrastructure. The downside of such freedom of choice is the need to learn the idiosyncrasies of each cloud environment. In addition, they must use different tools to manage the environment and its security provisions, which obscures visibility and necessitates the use of multiple management consoles for policy management, reporting, and more.

DO NOT REPRINT
© FORTINET



Since data in the public cloud is being stored by a third party and accessed over the internet, several challenges arise in the ability to maintain a secure cloud. These are:

Visibility into cloud data: In many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.

Control over cloud data: In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.

Access to cloud data and applications: Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.

Compliance: Use of cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may need to adhere to regulatory requirements such as HIPAA, PCI, and Sarbanes-Oxley, as well as requirements from internal teams, partners and customers. Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.

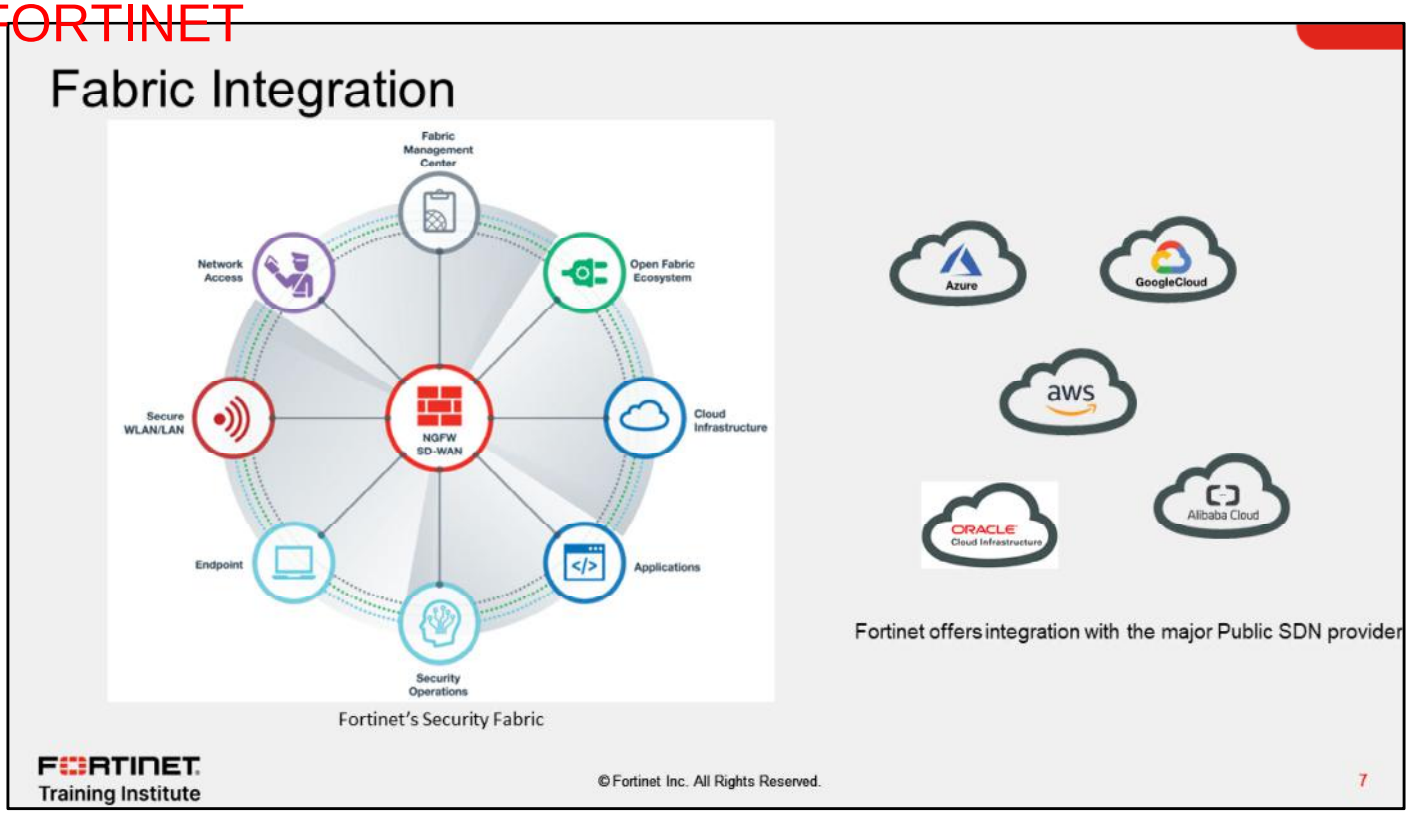
Cloud-native breaches: Data breaches in the cloud are unlike on-premises breaches in that data theft often occurs using native functions of the cloud. A cloud-native breach is a series of actions by an adversarial actor in which they land their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, expand their access through weakly configured or protected interfaces to locate valuable data, and exfiltrate that data to their own storage location.

Misconfiguration – Cloud-native breaches often fall to a cloud customer's responsibility for security, which includes the configuration of the cloud service. Research shows that just 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as the front door to a cloud-native breach, allowing the attacker to successfully land and then move on to expand and exfiltrate data. Research also shows 99% of misconfigurations go unnoticed in IaaS by cloud customers. Here's an excerpt from this study showing this level of misconfiguration disconnect:

Disaster recovery: Cybersecurity planning is needed to protect the effects of significant negative breaches. A disaster recovery plan includes policies, procedures, and tools designed to enable the recovery of data and allow an organization to continue operations and business.

Insider threats: A rogue employee is capable of using cloud services to expose an organization to a cybersecurity breach. A recent Cybersecurity Insiders study supported by Fortinet found that 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud.

DO NOT REPRINT
© FORTINET



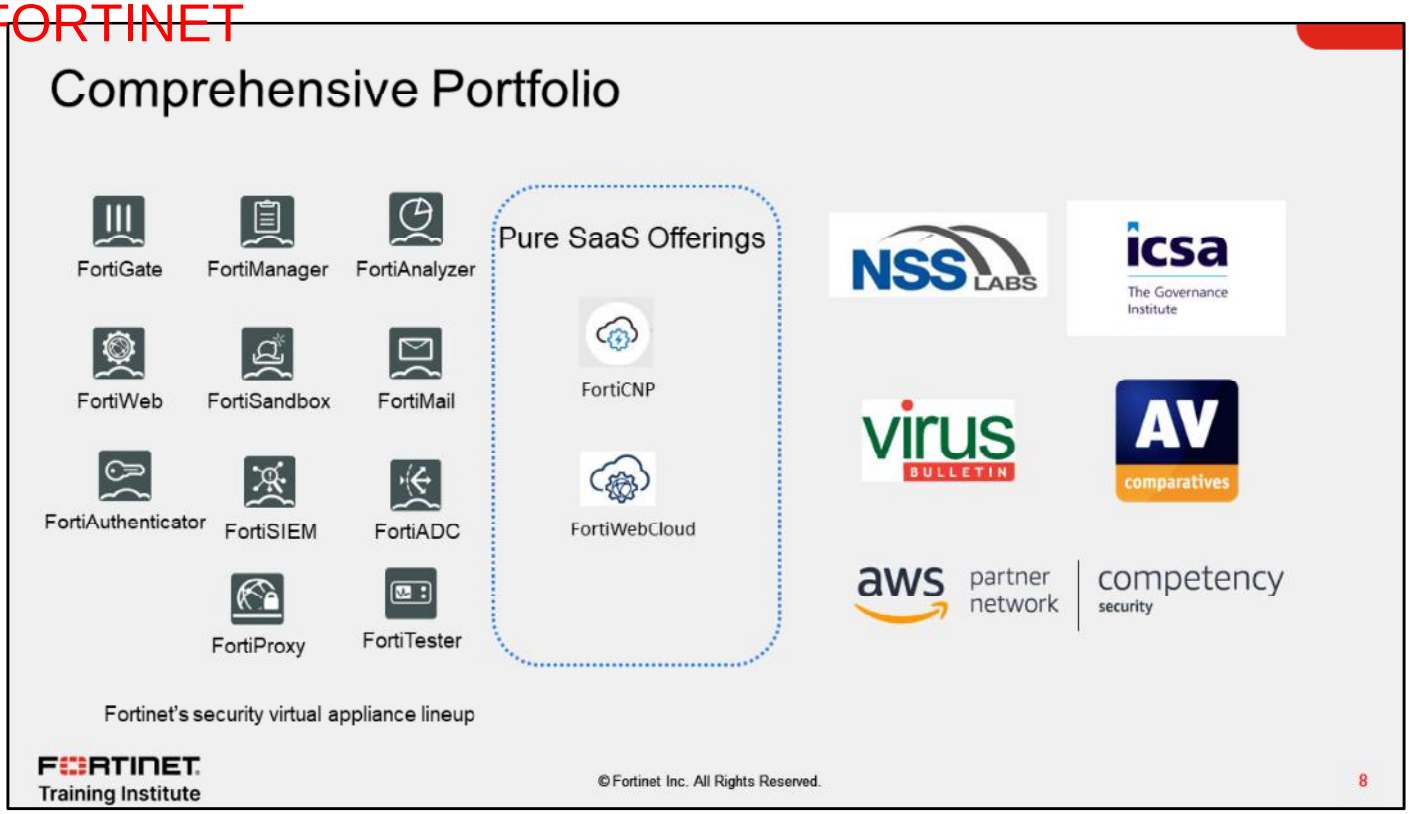
Some of you have probably seen this illustration of the Fortinet Security Fabric before. In a nutshell, the fabric is a holistic approach to security, with solutions that covers many aspects of cybersecurity, which is the same for cloud environments. It addresses the security challenges mentioned on the first slide by providing broad visibility and control of an organization's entire digital attack surface to minimize risk, an integrated solution that reduces the complexity of supporting multiple point products, and automated workflow to increase the speed of operation. The Fortinet security solutions offer network security, visibility, and control in both public and private cloud deployments.

FortiGate is situated at the core of the fabric, providing cloud-native security automation, VPN connectivity, network segmentation, intrusion prevention, and a secure web gateway.

Beyond protecting against malicious content, organizations also must ensure that their cloud deployments are correctly configured. FortiCNP (cloud-native protection), quickly resolves cloud security issues with actionable Resource Risk Insights (RRI). Maximize the value of your investments in cloud provider native security services and Fortinet cloud network and application security solutions by combining security findings from all your tools into actionable insights.

Organizations are also increasingly moving to cloud-based email solutions like Google G Suite and Microsoft Office 365. Since phishing attacks are a leading cause of security incidents and data breaches, securing cloud-based email is essential. Available as physical and virtual appliances or as a hosted service, FortiMail messaging security solutions protect both on-premises and cloud-based email deployments, including blocking traditional and advanced email threats and providing backup functionality to avoid the loss of sensitive information.

DO NOT REPRINT
© FORTINET



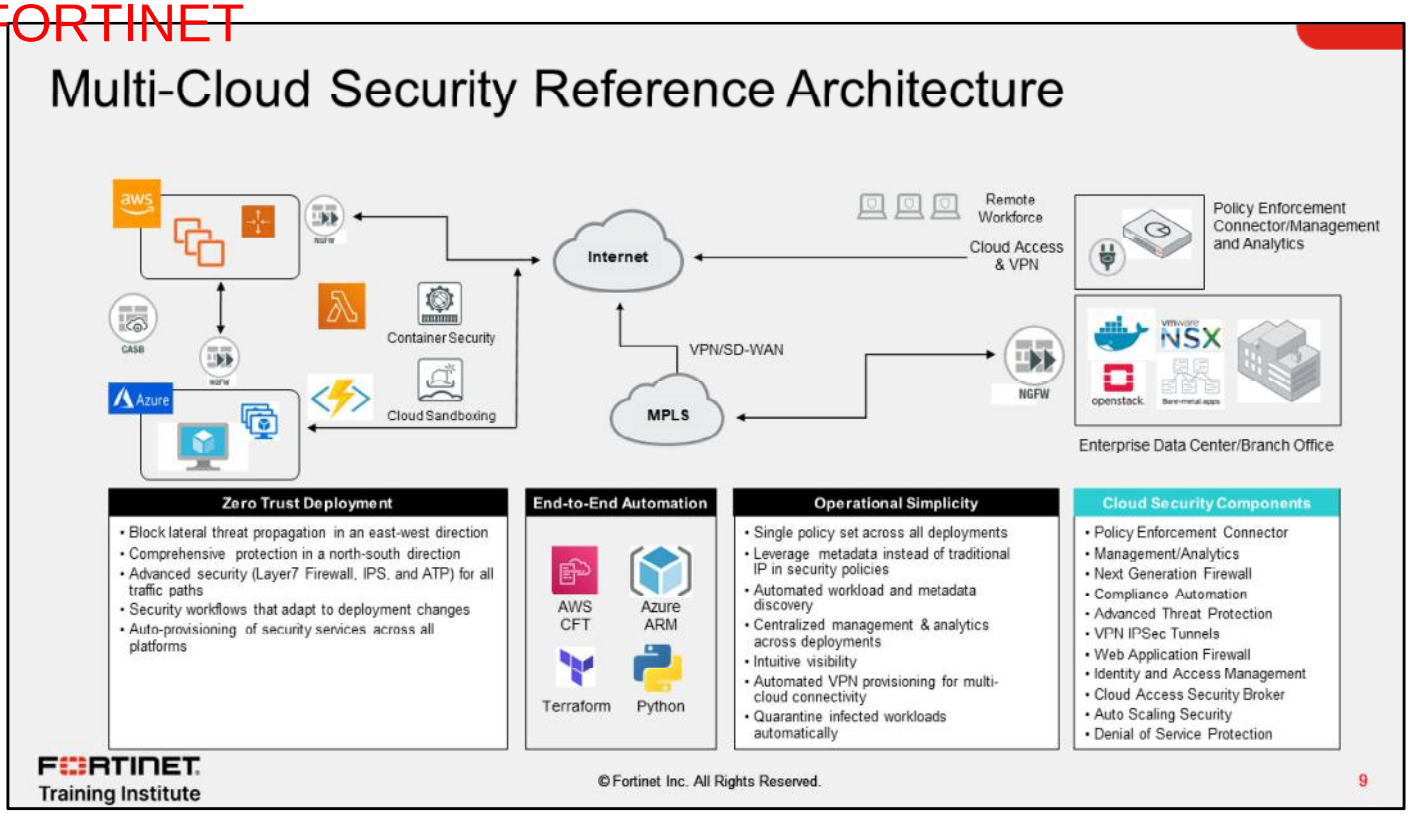
On this slide, you can see the Fortinet comprehensive virtual appliance lineup. You can start using the security fabric with just FortiGate and FortiAnalyzer. That gives you next-generation firewalling with content inspection, visibility into the network traffic and automated response to incidents based on the firewall logs. The latest FortiAnalyzer version includes a SoC component. For example, by using playbooks, you can have a single trigger start multiple actions, automating and accelerating incident response.

As you add more FortiGate devices to your environment, be it physical or virtual, you can leverage FortiManager to centralize the management and effectively have a single pane of glass to the fabric. Web applications and APIs have become the tools of choice for building business-critical applications. To protect those APIs and web applications, you can use FortiWeb, an advanced web application firewall (WAF) that can block known and zero-day threats to applications without blocking legitimate users, and, most importantly, without the excessive management overhead that traditional application learning requires.

It is worth mentioning that FortiCNP and FortiWebCloud are pure SaaS cloud-based offerings. FortiWeb Cloud is a SaaS cloud-based WAF that protects public cloud-hosted web applications from the OWASP Top 10, zero-day threats, and other application layer attacks. Requiring no hardware or software, the FortiWeb Cloud colony of WAF gateways runs in AWS, Azure, OCI, and Google Cloud regions allowing you to scrub your application traffic within the same region your applications reside, addressing performance, regulation concerns, and keeping traffic cost to minimum. FortiCNP is a cloud-native protection platform natively integrated with Cloud Service Provider (CSP) security services and the Fortinet Security Fabric to deliver a comprehensive, full-stack cloud security solution for securing cloud workloads.

Many of our solutions have been independently tested. For example, FortiGate has validated best security effectiveness and performance, receiving third-party certifications from different organizations, such as NSS Labs and ICSA. Fortinet is also a member of the AWS Security Competency partner network.

DO NOT REPRINT
© FORTINET



This slide shows a high-level overview of a multi-cloud security strategy using some Fortinet solutions. Multiple different environments are available, including Azure and AWS environments.

FortiGate provides advanced security with a Layer 7 firewall, IPS, and advanced threat protection for all traffic paths. It also provides connectivity to cloud applications, and VPN access for remote users. SDN connectors are used to integrate with cloud providers. For example, you can use the AWS connector to get VPC and instance information and use those directly in firewall policies. IPSec VPN provides a secure network integration between the different cloud providers, the enterprise data center, and branch offices. SD-WAN is being leveraged to guarantee that business-critical applications will always have the highest priority over regular network traffic.

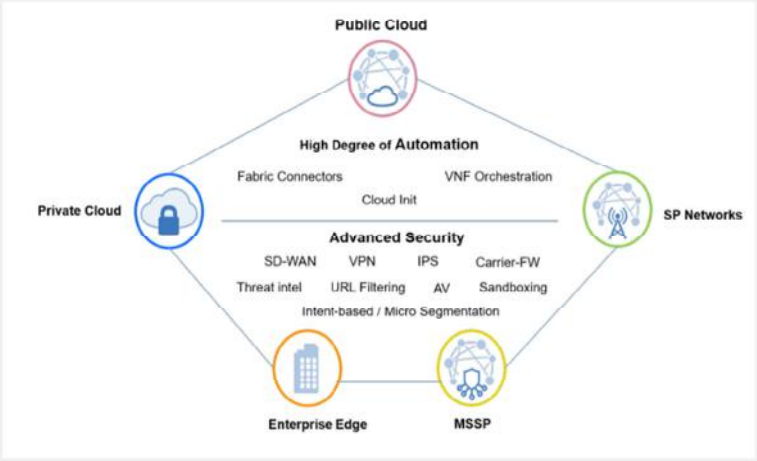
FortiCASB cloud access works to provide secure access to SaaS applications such as Office 365, giving you data-leak prevention and visibility into what your users are doing with corporate data.

Finally, end-to-end automation with tools, such as AWS CloudFormation, Azure Resource Manager, Python, and Terraform allows you to deploy complex infrastructure across the cloud and on-premises, in a consistent manner. For example, the VPN tunnels can be automatically provisioned after you add a new environment.

DO NOT REPRINT
© FORTINET

Public Cloud FortiGate Options (Use cases)

- Network security
- Protection against known exploits and malware
- Protection against unknown threats (sandboxing)
- Content inspection
- Data protection
- VPN gateway
- Security automation
- Container security



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

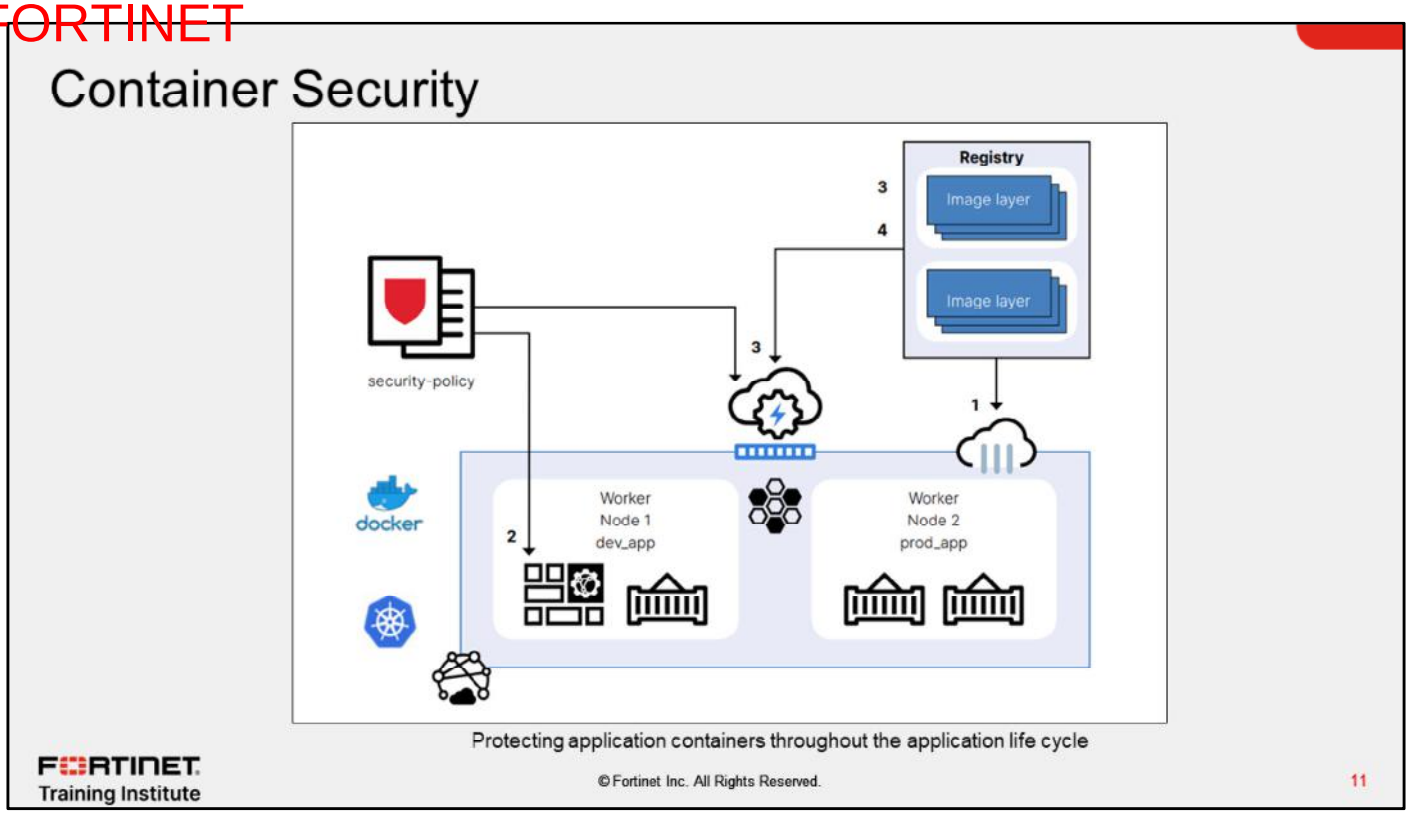
10

FortiGate VM for Public Cloud environments delivers complete content and network protection by combining stateful inspection with next-generation firewall features.

- Application control identifies thousands of applications including cloud applications, for deep inspection into network traffic.
- Protects against known exploits and malware using continuous threat intelligence provided by FortiGuard Labs security services.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- Sandboxing integration protects against unknown attacks using dynamic analysis, and provides automated mitigation to stop targeted attacks.

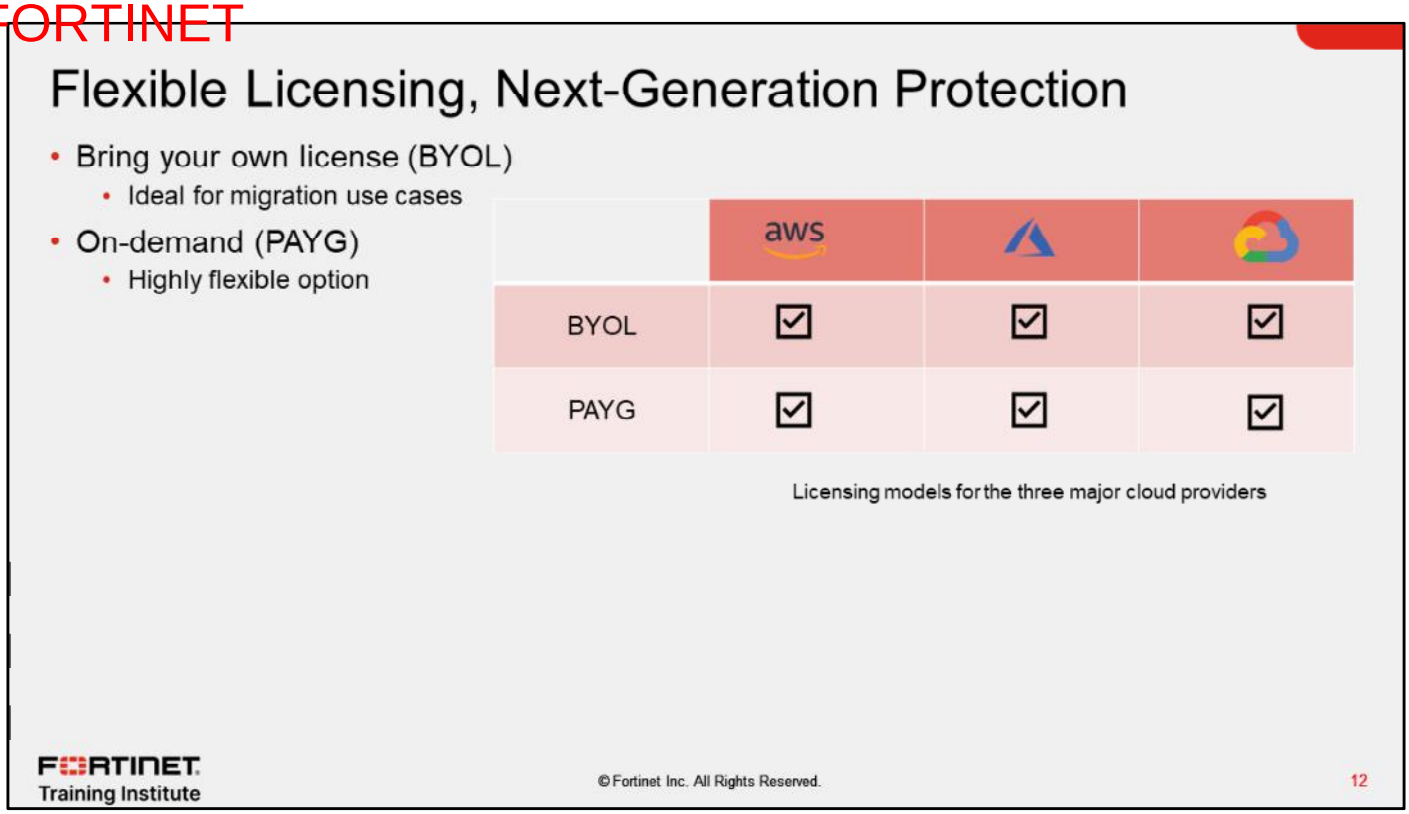
FortiGate VM has APIs for automation and orchestration with cloud and SDN extensions. For example, it can be integrated with AWS GuardDuty threat intelligence feeds for automated incident response. Additionally, new Docker application control signatures protect your container environments from newly emerged security threats.

DO NOT REPRINT
© FORTINET



Container security is one of the challenging components in the public cloud for network security administrators because of its dynamic nature. Developers are increasingly using containers, which have quickly grown in popularity. As shown on this slide, the Fortinet container security solutions can protect application containers throughout the application life cycle with FortiGate Next-Generation Firewall (NGFW), WAF, FortiCNP, and FortiSandbox. For example, FortiGate NGFW connects to the container management layer and learns the labels of different containers. The security policies are label-aware and can use these labels to describe objects in the security policies. This solution is primarily relevant to securing traffic in and out of the container infrastructure—namely, north-south security. FortiGate NGFWs offer fabric connectors that interface with major container orchestration systems to leverage metadata as security policy objects, including native Kubernetes, AWS EKS, GCP GKE, Azure AKS, and OCI OKE. When traffic leaves the boundaries of a containerized environment, it crosses a FortiGate NGFW that enforces the policy based on the container role. FortiGate also scans ingress and egress container traffic for vulnerabilities and file-based threats using an intrusion prevention system (IPS) and advanced malware protection through FortiSandbox integrations.

DO NOT REPRINT
© FORTINET

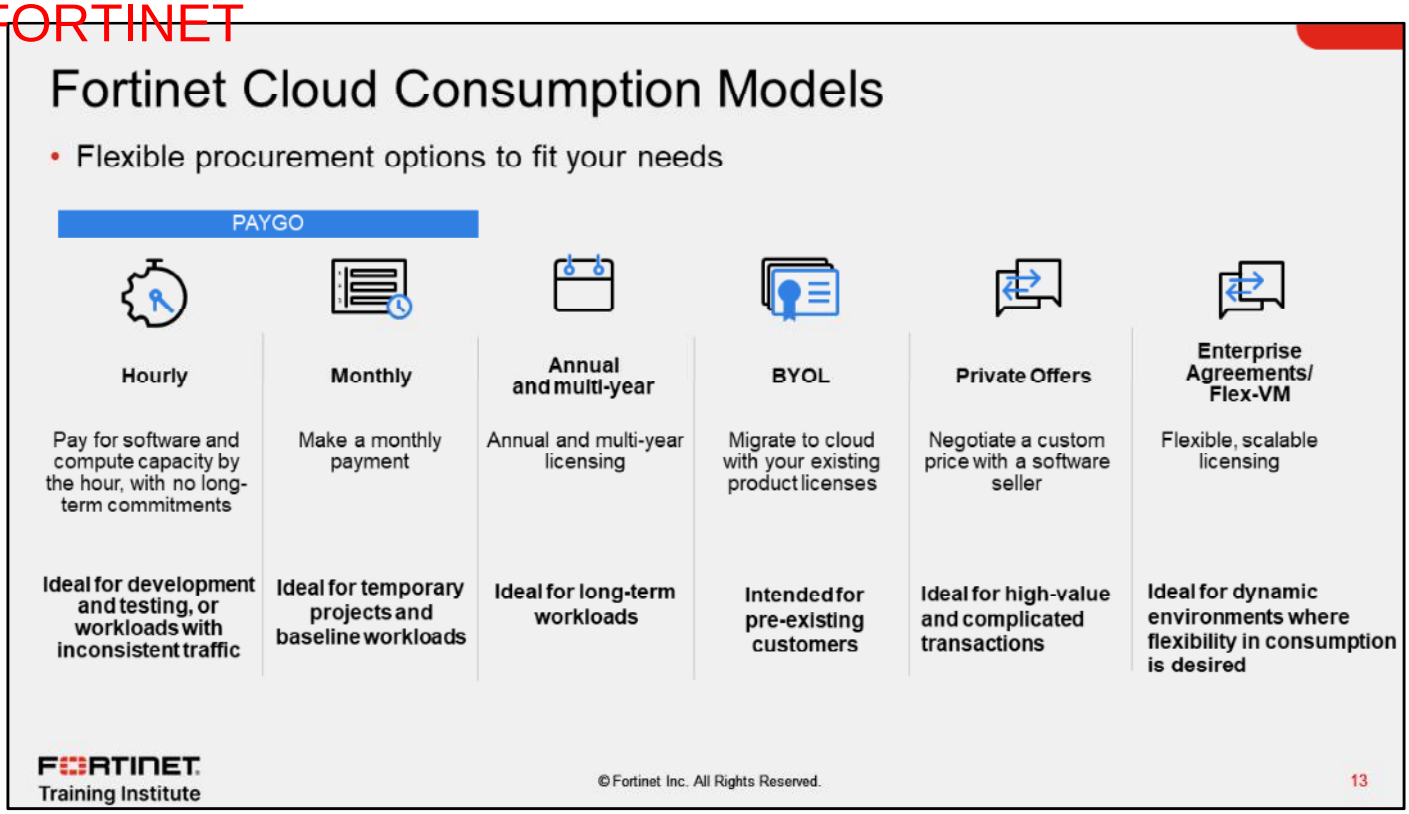


In terms of licensing, FortiGate VM for Public Cloud supports both on-demand (PAYG) and bring-your-own-license (BYOL) models.

BYOL is ideal for migration use cases, where an existing private cloud deployment is migrated to a public cloud deployment. When using an existing license, the only additional cost would be the price for the cloud instances.

On-demand licensing is a highly flexible option for both initial deployments and growing them as needed. With a wide selection of supported instance types, there is a solution for every use case. This license offers FortiOS with a UTM bundle.

DO NOT REPRINT
© FORTINET

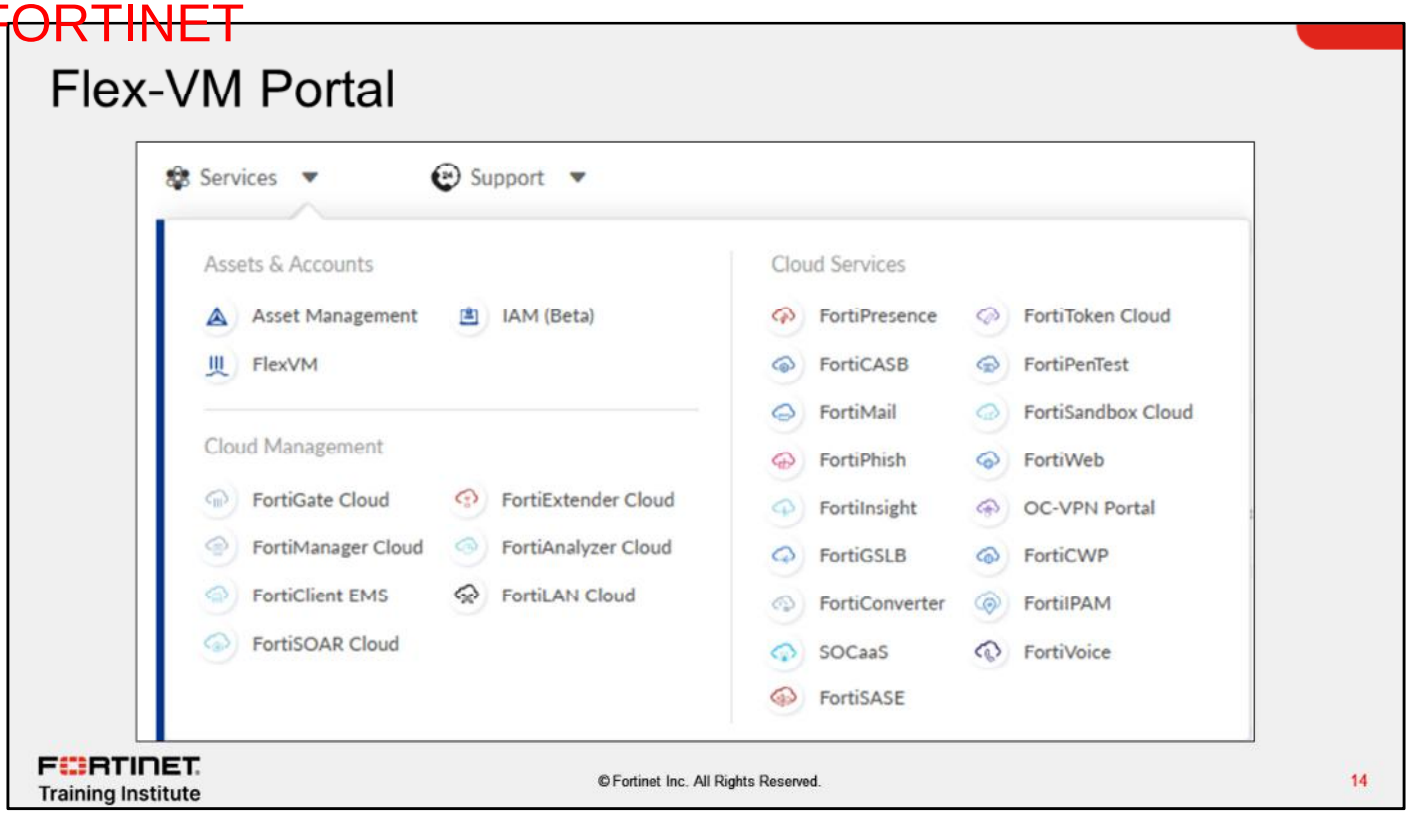


The Fortinet Flex-VM subscription program provides unmatched flexibility of VM usage in a consumption model. The program offers two types of subscriptions: one for enterprise customers and another for MSSP partners. The Flex-VM subscription program is a new consumption model for cloud security designed to address the elasticity and on-demand consumption requirements of cloud deployments.

The Flex-VM enterprise subscription is a prepaid program for large and medium-size enterprises, including service providers who want to leverage the program for their IT needs.

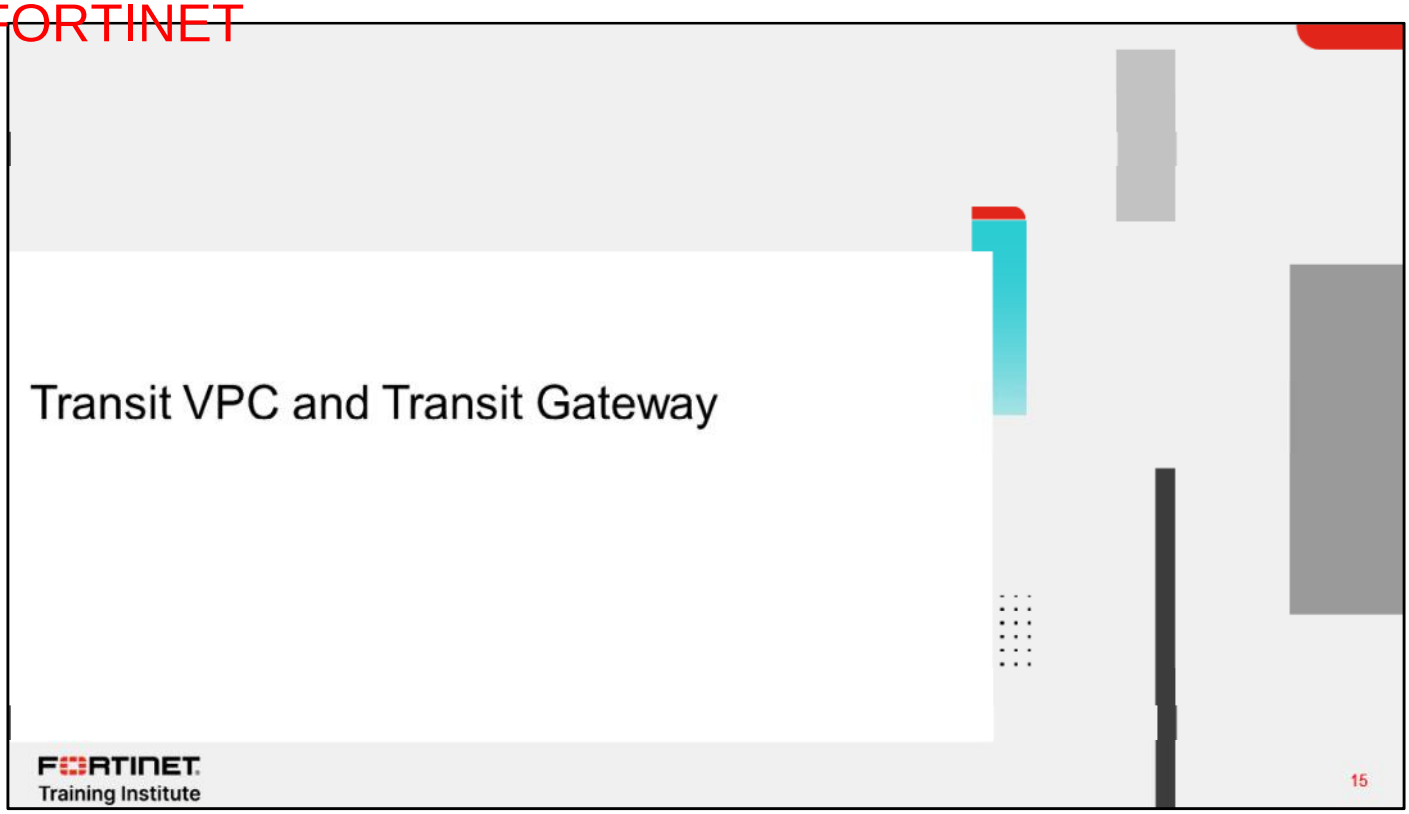
The Flex-VM MSSP subscription is a post-paid program that is available to qualified MSSPs that are advanced and expert-level partners. These partners could also include service providers who want to secure their infrastructure, including mobile and IP networks, and deliver security services.

DO NOT REPRINT
© FORTINET



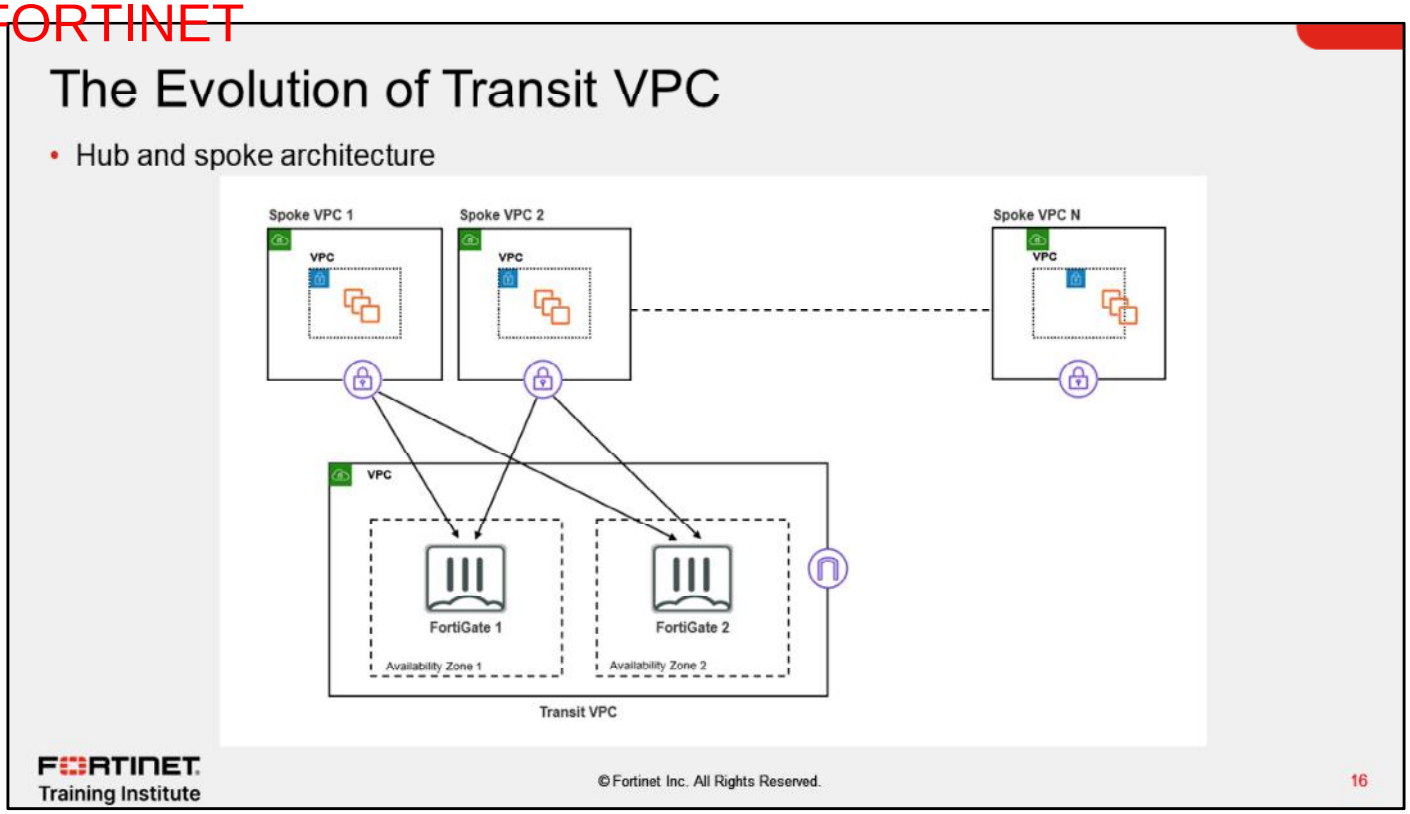
Flex-VM allows you to easily manage VM usage entitlements. You can use the Flex-VM portal to create VM configurations, generate licensing tokens, and monitor resource consumption in the form of points. Flex-VM subscribers can create multiple sets of a single VM entitlement that correspond to a licensed virtual machine. Resource consumption is based on predefined points that are calculated on a daily basis (PST/PDT time zone).

DO NOT REPRINT
© FORTINET



In this section, you will learn about the transit VPC and transit gateway.

DO NOT REPRINT
© FORTINET

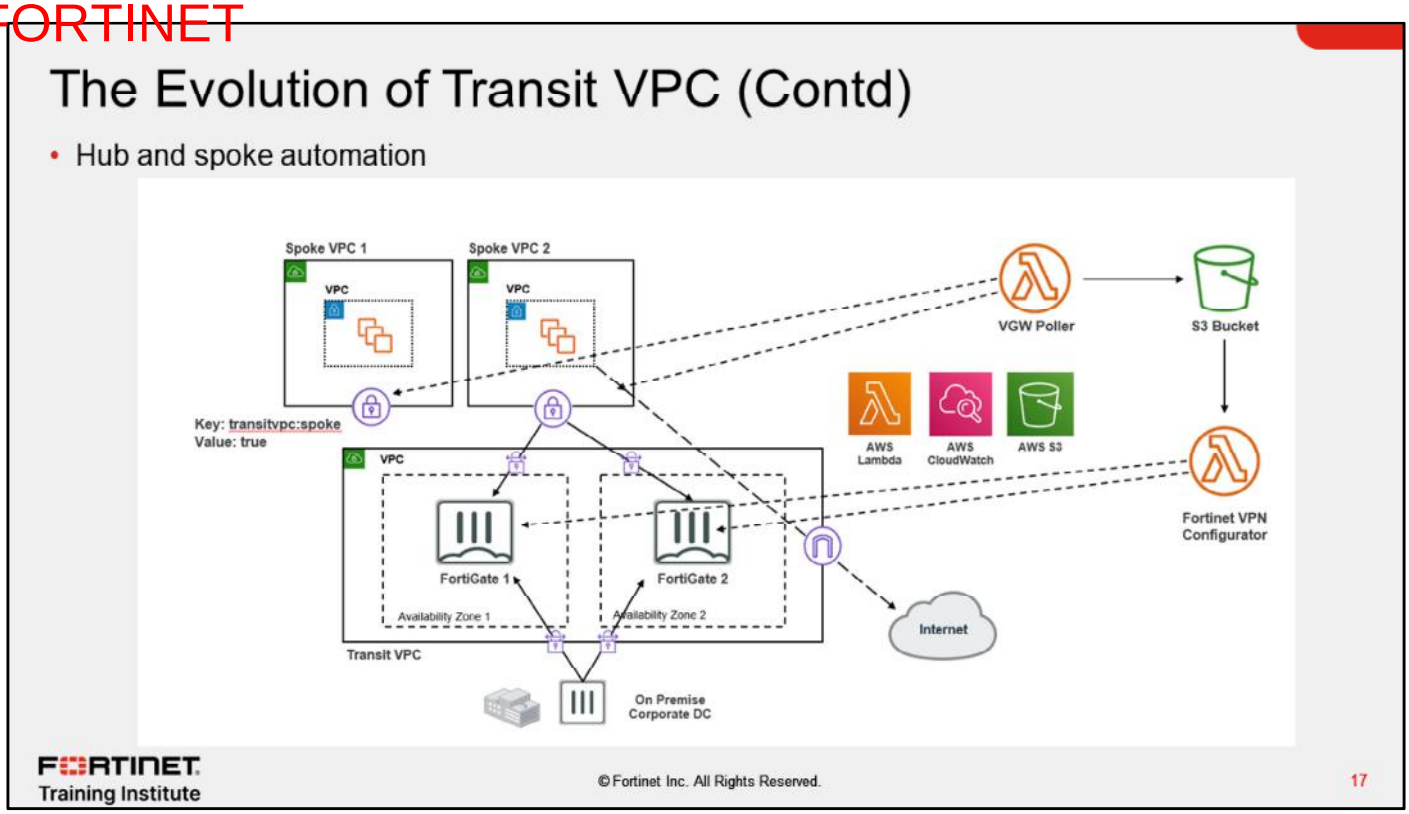


So, what is transit VPC?

A transit VPC connects multiple VPCs and remote networks in order to create a global network transit center. It adds flexibility by removing limitations such as the lack of transitivity with VPC peering. That means that if you have three VPCs, A, B, and C, and B is peered to both A and C, you cannot route from A to C through B. A transit VPC can also be used to route traffic from cloud environments to on-premises infrastructures.

The concept is simple and is based on a hub-and-spoke topology. FortiGate VM appliances in the hub VPC connect to all the spoke VPCs using redundant IPsec VPN tunnels. All traffic in and out of the spoke VPCs is securely routed through and inspected by the FortiGate devices. The VPN tunnels are built inside the AWS network, so latency is minimized.

DO NOT REPRINT
© FORTINET



As you start to add more environments and VPCs, manual configuration can be time consuming and prone to errors. For that reason, it's a good idea to automate the setup of the transit VPC.

This slide shows an example of how this can be accomplished. The automated process for adding a new spoke VPC, as part of this solution, is as follows:

1. Every five minutes, an Amazon CloudWatch event invokes the VGW Poller Lambda function, which iterates through each AWS region of one or more customer accounts, searching for appropriately tagged spoke VGWs (default tag key transitvpc:spoke, default tag value true) that do not have existing transit VPC VPN connections.

2. When the VGW poller identifies an applicable spoke VGW, it creates the corresponding customer gateways (if required) and VPN connections to each FortiGate device, and then saves this connection information to an Amazon S3 bucket using S3 SSE-KMS. All data in the S3 bucket is encrypted using a solution-specific AWS KMS-managed customer master key (CMK).

3. The S3 Put event invokes the VPN Configurator Lambda function, which parses the VPN connection information and generates the necessary configuration files to create new VPN connections.

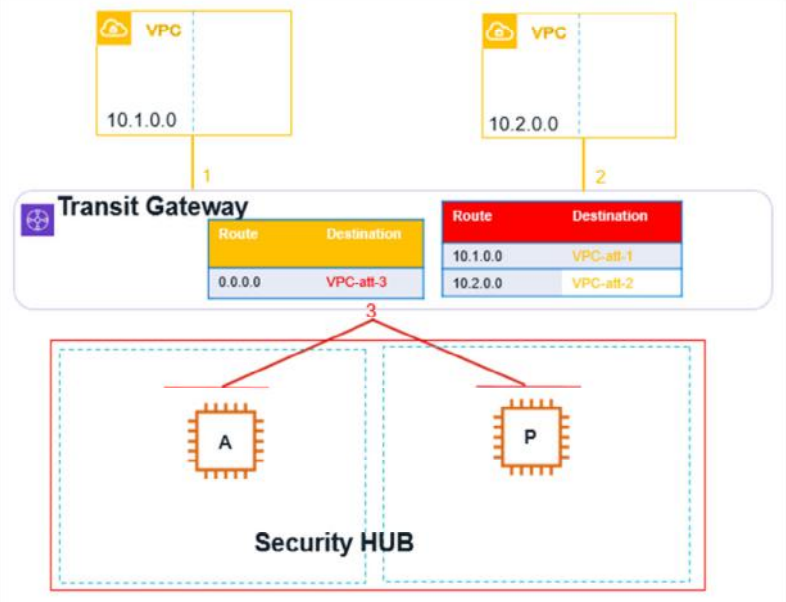
4. The VPN configuration (Lambda function) pushes the configuration to the VPN device instances using SSH.

5. As soon as the VPN configuration is applied to the FortiGate devices, the VPN tunnels come up and Border Gateway Protocol (BGP) neighbor relationships are established to the spoke VPCs.

DO NOT REPRINT
© FORTINET

Transit Gateway

- Multiple transit gateway route tables for routing control
- 10,000 routes per transit gateway
- 50 Gbps of bandwidth per attachment per availability zone
- 5000 Amazon VPC attachments per transit gateway
- Higher bandwidth with VPN connection with ECMP



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

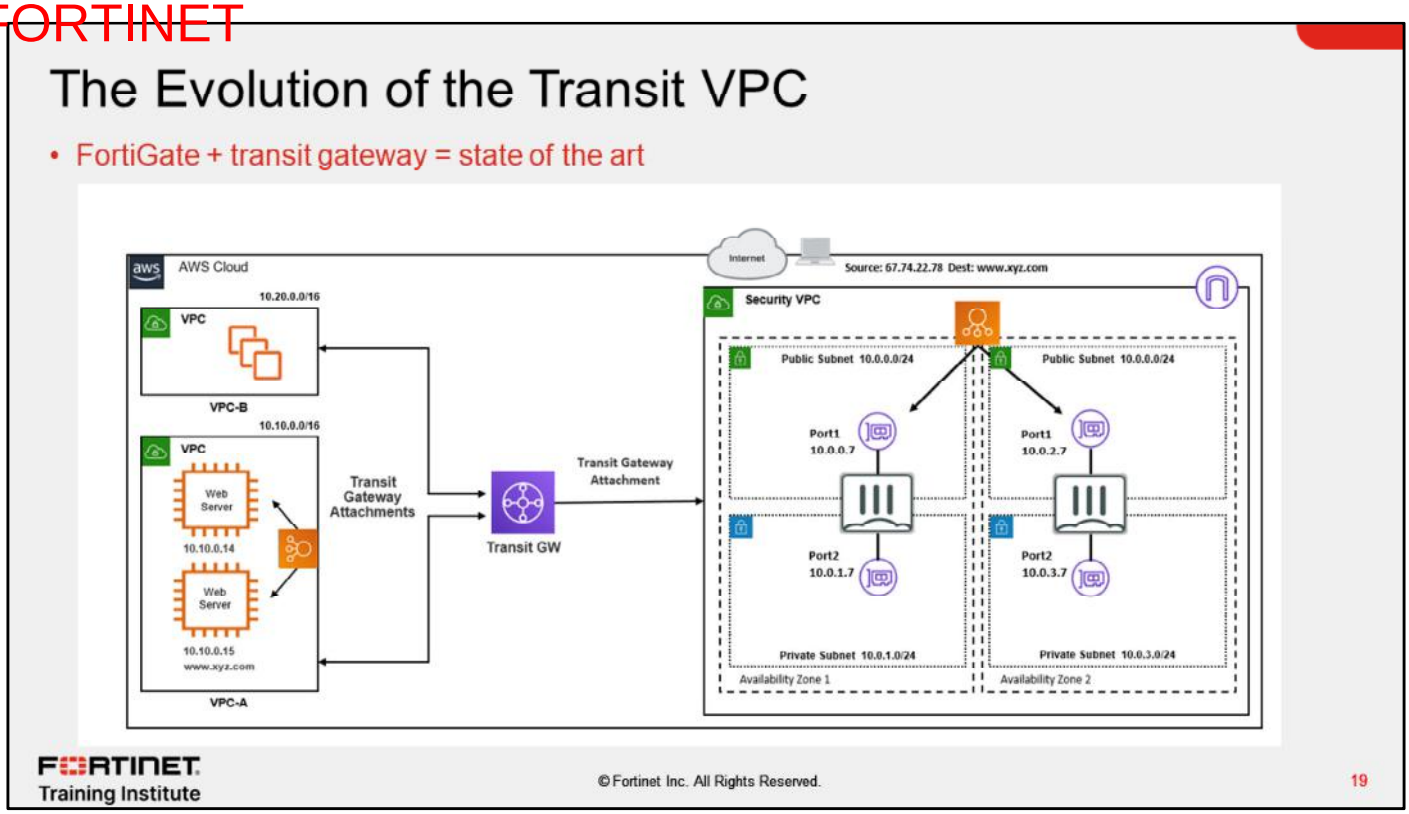
18

Transit gateway helps to solve multiple issues with VPC peering and transit VPC. Using transit gateway technology, you can create multiple transit gateway route tables inside the transit gateway for better traffic control. As shown in the example on this slide, you can create multiple attachments based on the number of VPCs you need to connect. For example, you will need only three attachments to create all three VPCs. This eliminates the full mesh requirement that is part of the VPC peering scenario.

As shown in the example, there are two route tables inside the transit gateway with three attachments. Any traffic coming to the transit gateway, except subnets `10.1.0.0` and `10.2.0.0`, goes to the security hub VPC through attachment `VPC-att-3`. At the same time, traffic going to the subnet `10.1.0.0` uses `VPC-att-1`, and subnet `10.2.0.0` uses the attachment `VPC-att-2`. This granular level of control means a lighter workload for the administrator when they are adding multiple VPCs to the existing environment.

Another main advantage is bandwidth. Customers can create multiple VPN connections from the transit gateway to the on-premises data center with ECMP to achieve higher bandwidth.

DO NOT REPRINT
© FORTINET

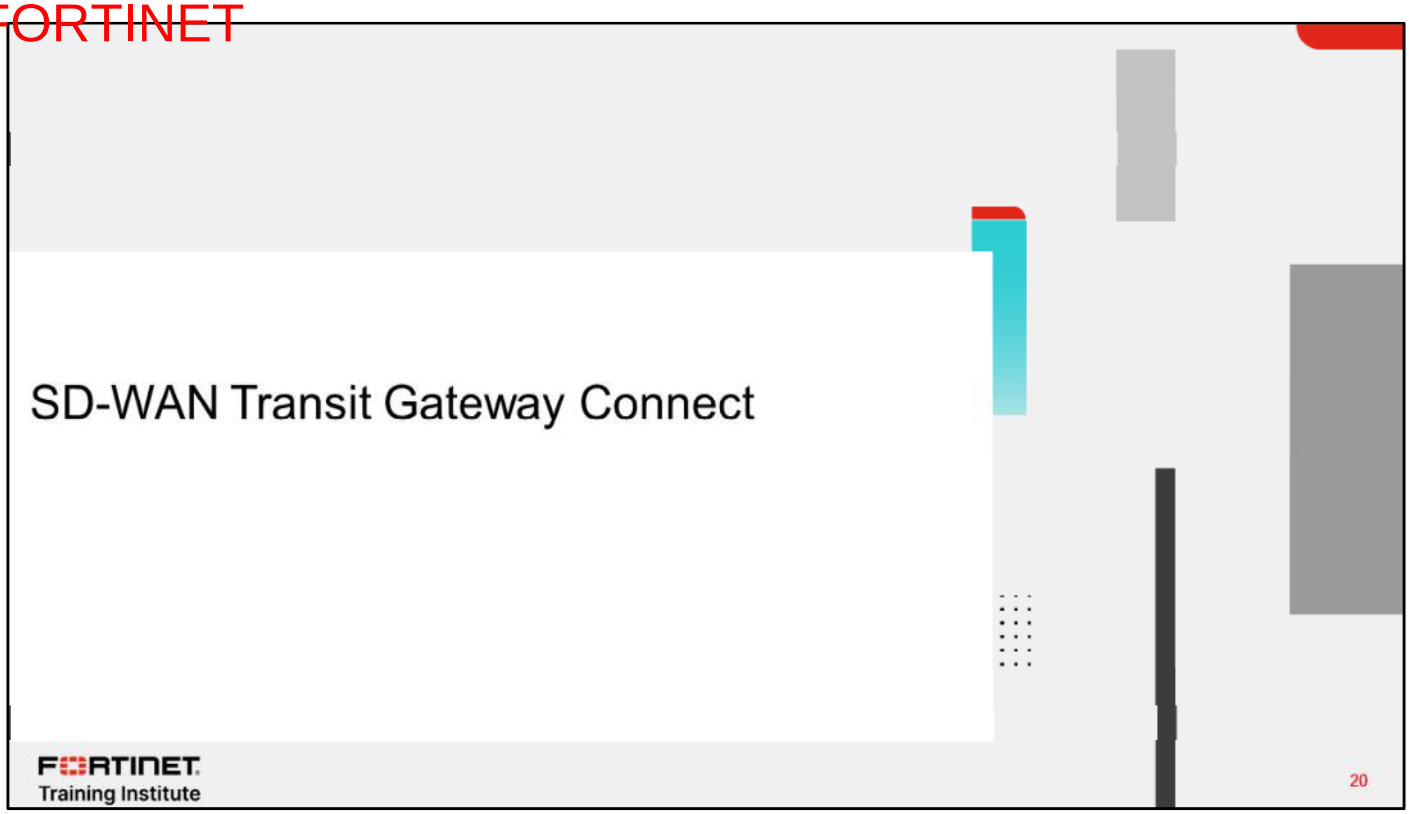


While the transit VPC design solves routing challenges and guarantees traffic inspection for all the VPCs, it's not without issues. First, having multiple VPN tunnels adds complexity. Second, bandwidth is limited to 1.25 Gbps, which is the maximum throughput supported by a single VPN tunnel on an AWS virtual private gateway.

The design shown on this slide is based on the usage of AWS transit gateways. The TGW is a BGP-equipped cloud router that connects VPCs and on-premises networks through a central hub. Now, instead of building VPN tunnels from the FortiGate devices to each VPC through a virtual private gateway, you attach each VPC to a transit gateway, which will be responsible for the routing between the multiple VPCs. On-premises networks can be connected to the cloud using the AWS Direct Connect service, or you can still leverage IPSec VPNs, but since the transit gateway supports ECMP, you can have multiple VPN tunnels to the same destination and scale beyond the default bandwidth limit of VPN tunnel. Also AWS inter-region peering allows you to connect VPCs hosted in different regions together.

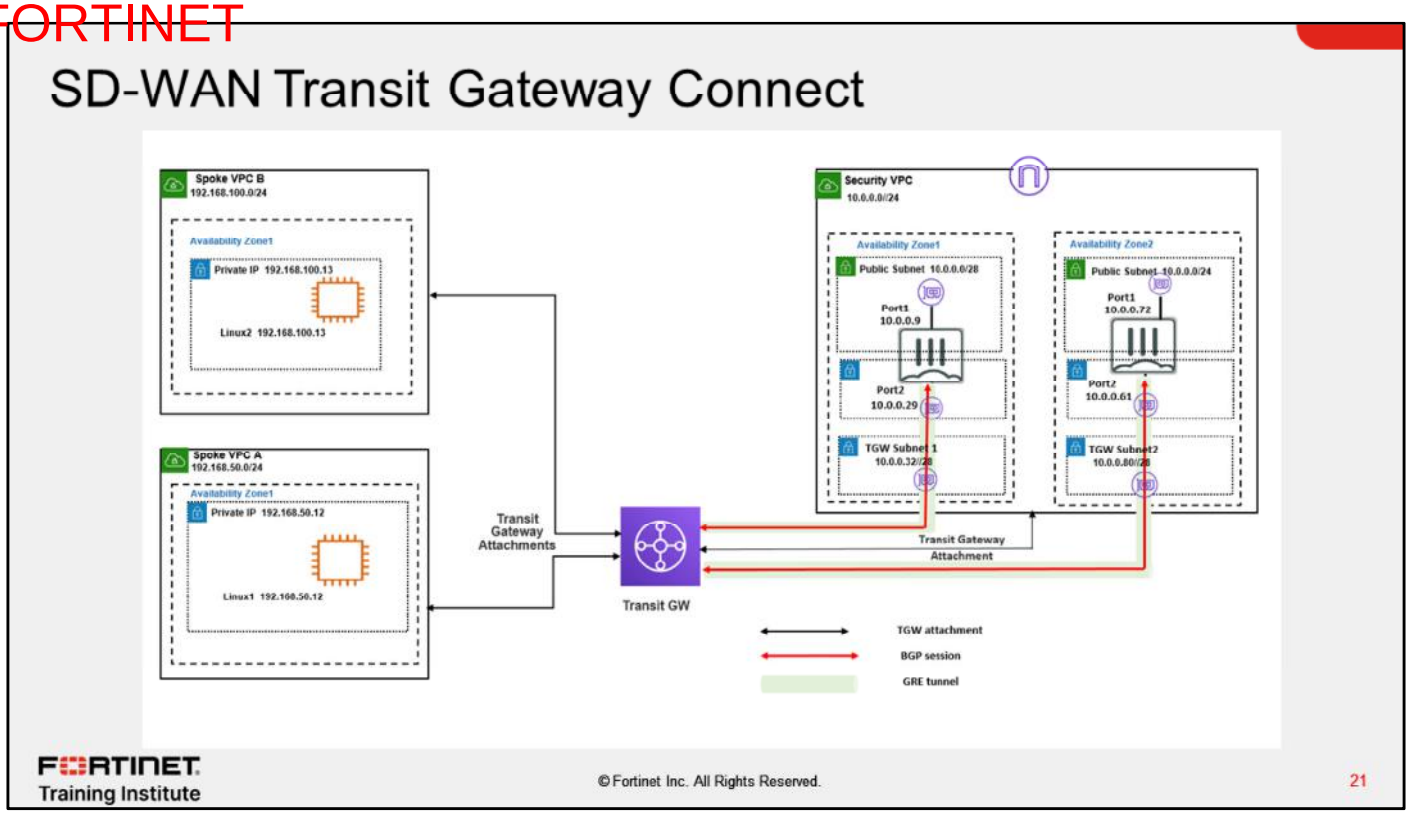
In this setup, the FortiGate devices still inspect all the traffic that goes in and out of the VPCs, with the added benefit of not having to act as the main router, being dedicated to security tasks.

DO NOT REPRINT
© FORTINET



In this section, you will learn about SD-WAN Transit Gateway Connect.

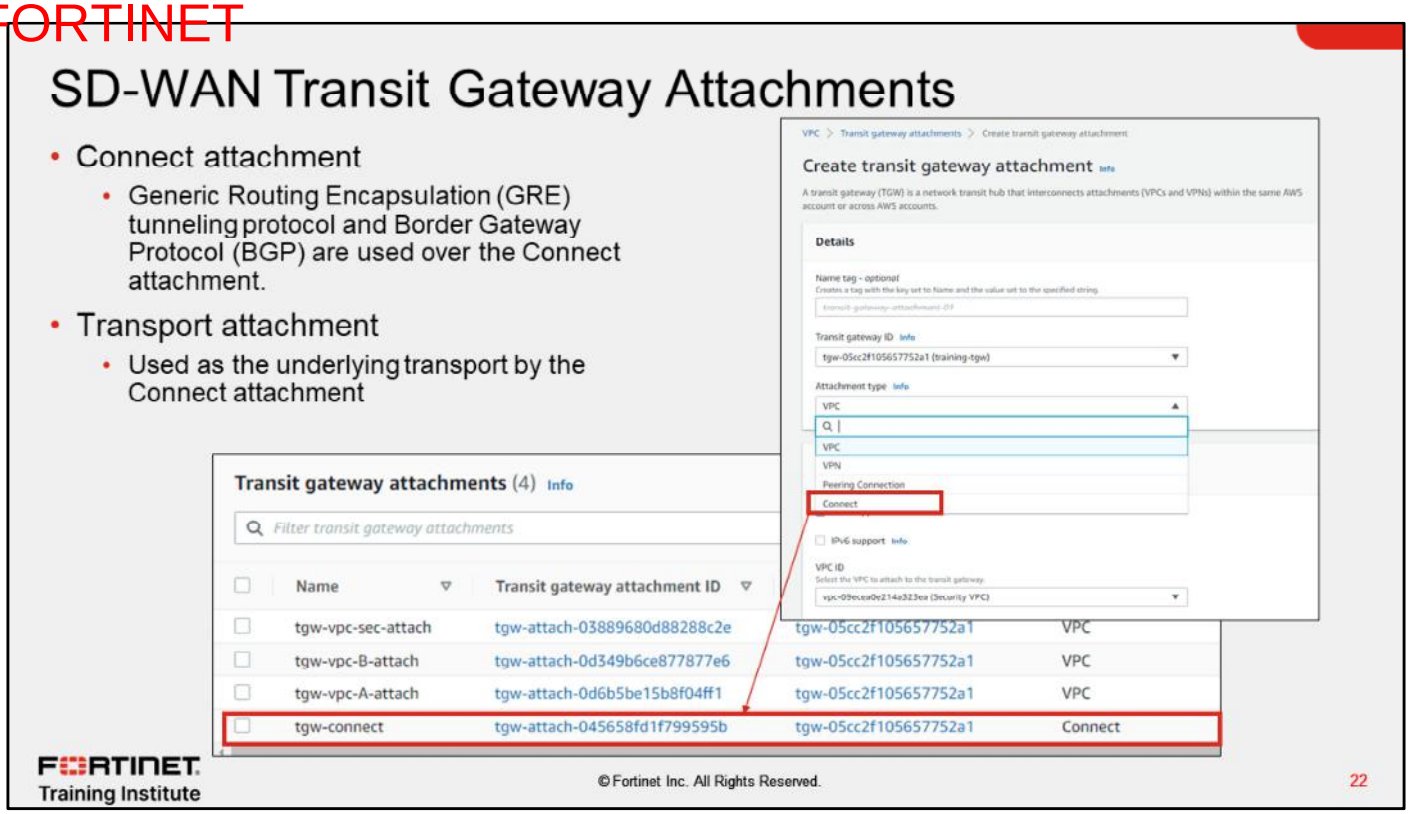
DO NOT REPRINT
© FORTINET



SD-WAN is the perfect solution to connect data centers and branch offices over the public internet. However, many customers need their existing infrastructure to connect to the cloud. So, the traditional SD-WAN itself is not very well-suited for this task because of increasing complexity and operational burden. SD-WAN TGW Connect helps to extend the capabilities of traditional SD-WAN to the cloud. This makes it easy to extend the SD-WAN into AWS without having to set up IPsec VPNs between SD-WAN network virtual appliances and Transit Gateway.

The TGW plugin provides a tighter and a more native integration between the partner gateway appliances and TGW through a tunnel attachment. The TGW plugin supports GRE-based tunnel attachments, which provide higher performance than IPsec connections, which are currently used for the same purpose. Native GRE-based tunnel attachments support triple the bandwidth as IPsec. Following are the main components of the TGW.

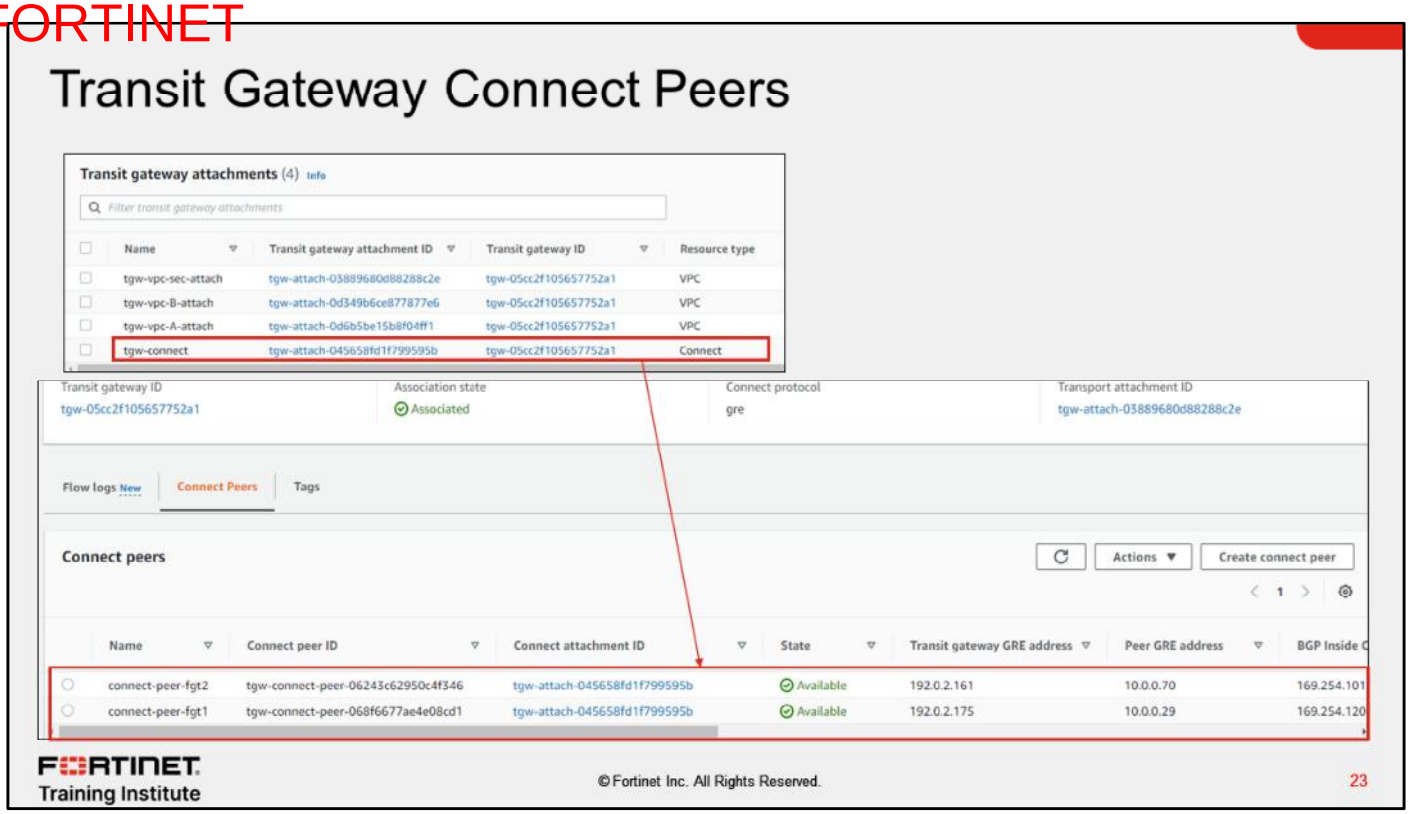
DO NOT REPRINT
© FORTINET



How do you connect TGW to your VPCs? You must create a TGW attachment to link separate VPCs and subnets to the TGW. Following are two main attachments of TGW.

- **Connect attachment**: Uses a transport transit gateway attachment (existing VPC or AWS Direct Connect attachment as transport) for the third-party device to connect to TGW. Generic Routing Encapsulation (GRE) tunneling protocol and Border Gateway Protocol (BGP) are used over the connect attachment.
- **Transport attachment**: This is an existing TGW attachment type (VPC or AWS Direct Connect attachment) that is used as the underlying transport by the connect attachment.

DO NOT REPRINT
© FORTINET

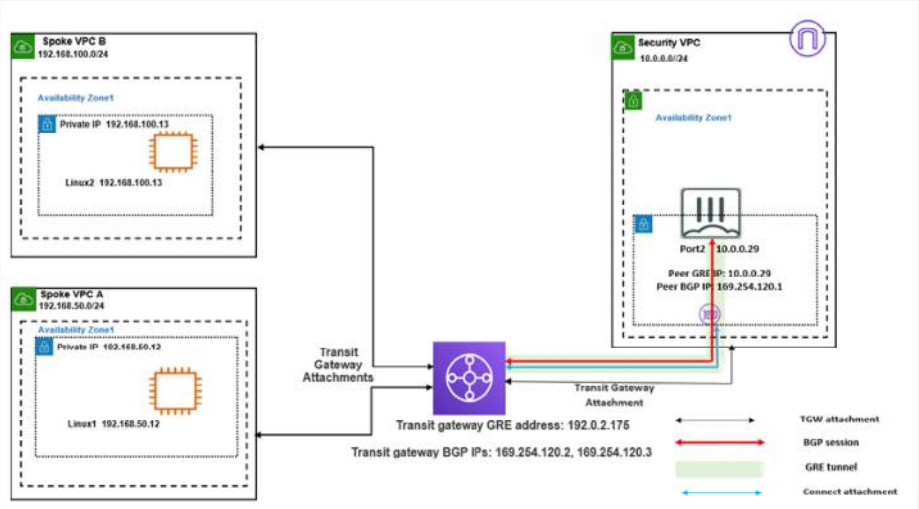


Connect peers are the combination of a GRE and BGP configuration between the FortiGate devices and TGW. As shown on this slide, there are two peering connections to both FortiGate-1 and FortiGate-2.

DO NOT REPRINT
© FORTINET

Transit Gateway Connect Peers (Contd)

- Inside CIDR blocks (BGP addresses) are used for BGP peering
  - `169.254.0.0/16` CIDR block
- Peer IP address (GRE outer IP address) is the FortiGate side of the TGW Connect peer
  - `10.0.0.29`
- Transit gateway side of the connect peer address is autogenerated from the TGW CIDR block
  - `192.0.2.175`



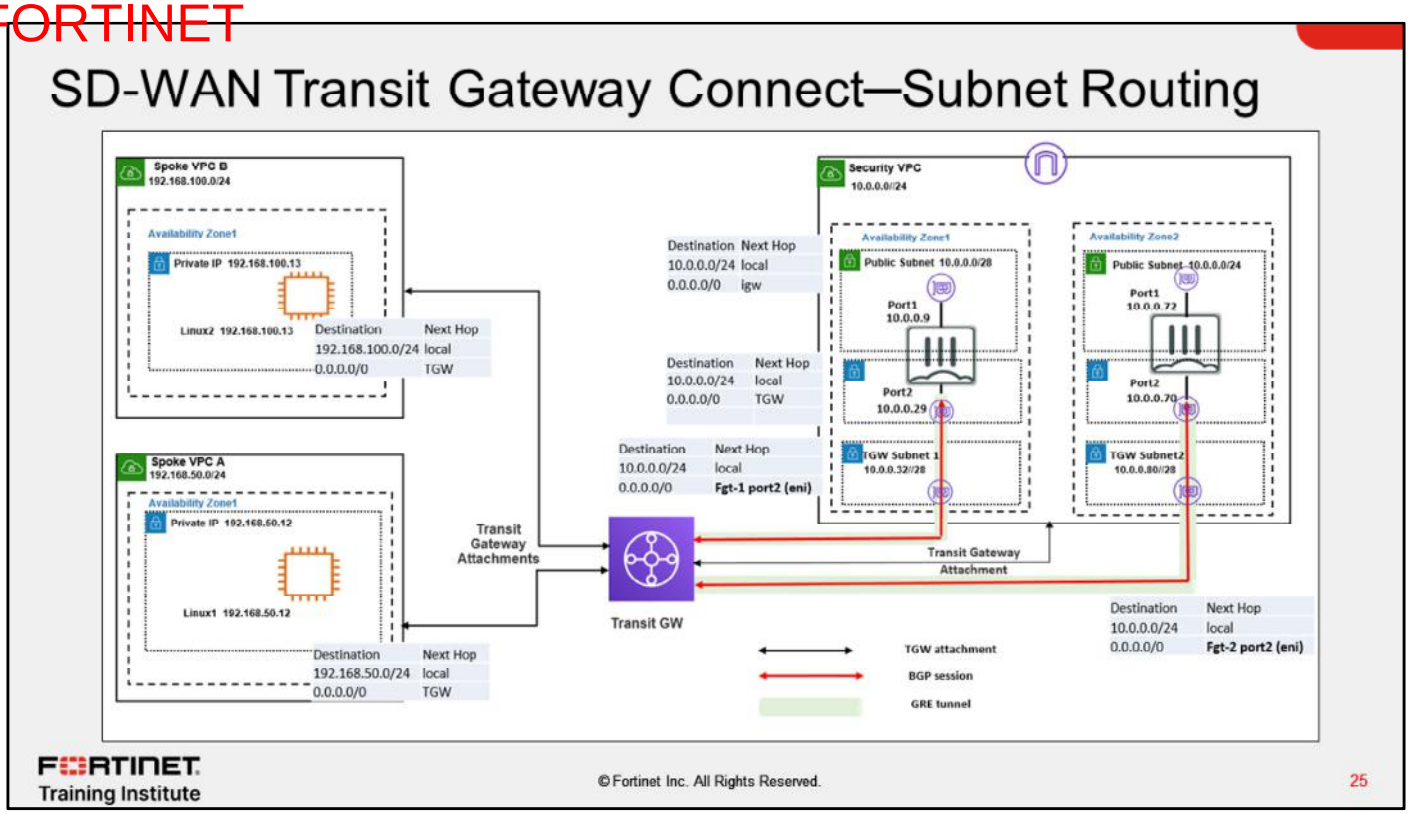
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

The example shown on the slide is the connect attachment between a TGW and FortiGate VM in the security VPC. A transit gateway connect peer is created on the connect attachment to establish a connection to the FortiGate VM in the VPC. You must specify a /29 CIDR block from the `169.254.0.0/16` range for IPv4. Those inside IP addresses are used for BGP peering. The TGW GRE IP address is `192.0.2.175`, which is autogenerated from the TGW CIDR block, and the range of BGP addresses is `169.254.120.0/29` block. The first IP address in the range (`169.254.120.1`) is configured on the FortiGate device as the peer BGP IP address and other two addresses, which are `169.254.120.2` and `169.254.120.3`, on the TGW side of the connect peer.

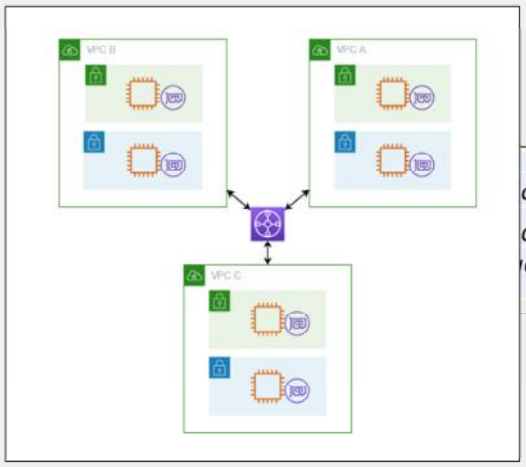
DO NOT REPRINT
© FORTINET



When you attach a VPC to a transit gateway, you must add routes to the subnet route table to route traffic through the transit gateway. As per the example shown, all traffic (0.0.0.0/0) except 192.168.50.0/24 subnet traffic in the **Spoke VPC A**, will use the TGW attachment as the next hop.

DO NOT REPRINT
© FORTINET

Transit Gateway Route Table



	Route type
chment for VPC A	propagated
chment for VPC B	propagated
chment for VPC C	propagated

FORTINET Training Institute

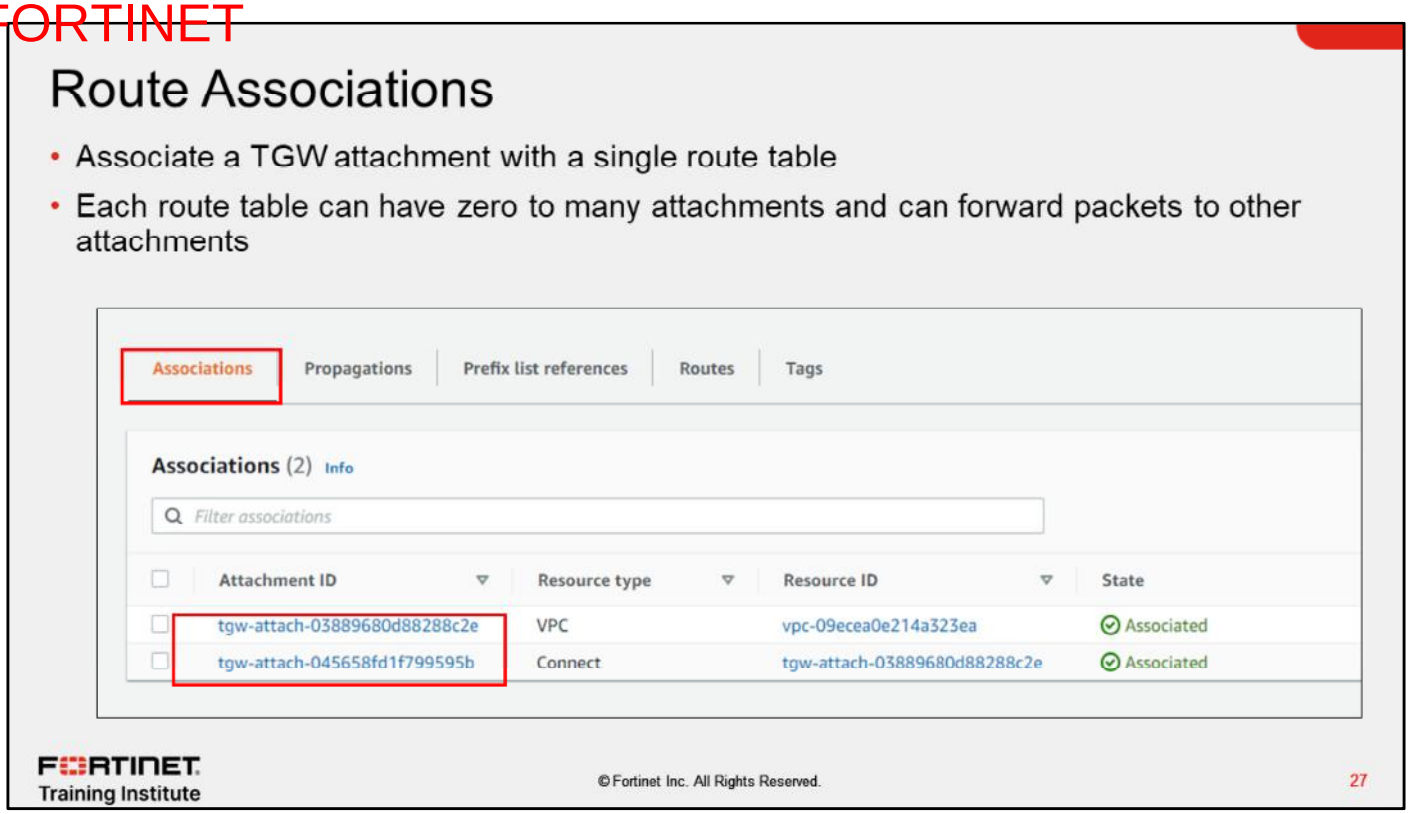
© Fortinet Inc. All Rights Reserved.

26

It is important to know that routing in the transit gateway. When you create a transit gateway, it also creates a transit gateway default route table. You can use this table as the default association and propagation route table for the transit gateway. You can also create additional route tables and disable the default route table by disabling route propagation and route table association. One use case is to create an additional route table is to isolate subsets of attachments and force traffic to flow through a certain attachment. As shown on this slide, The CIDR blocks for each VPC propagate to the route table, then each attachment can route packets to the other two attachments.

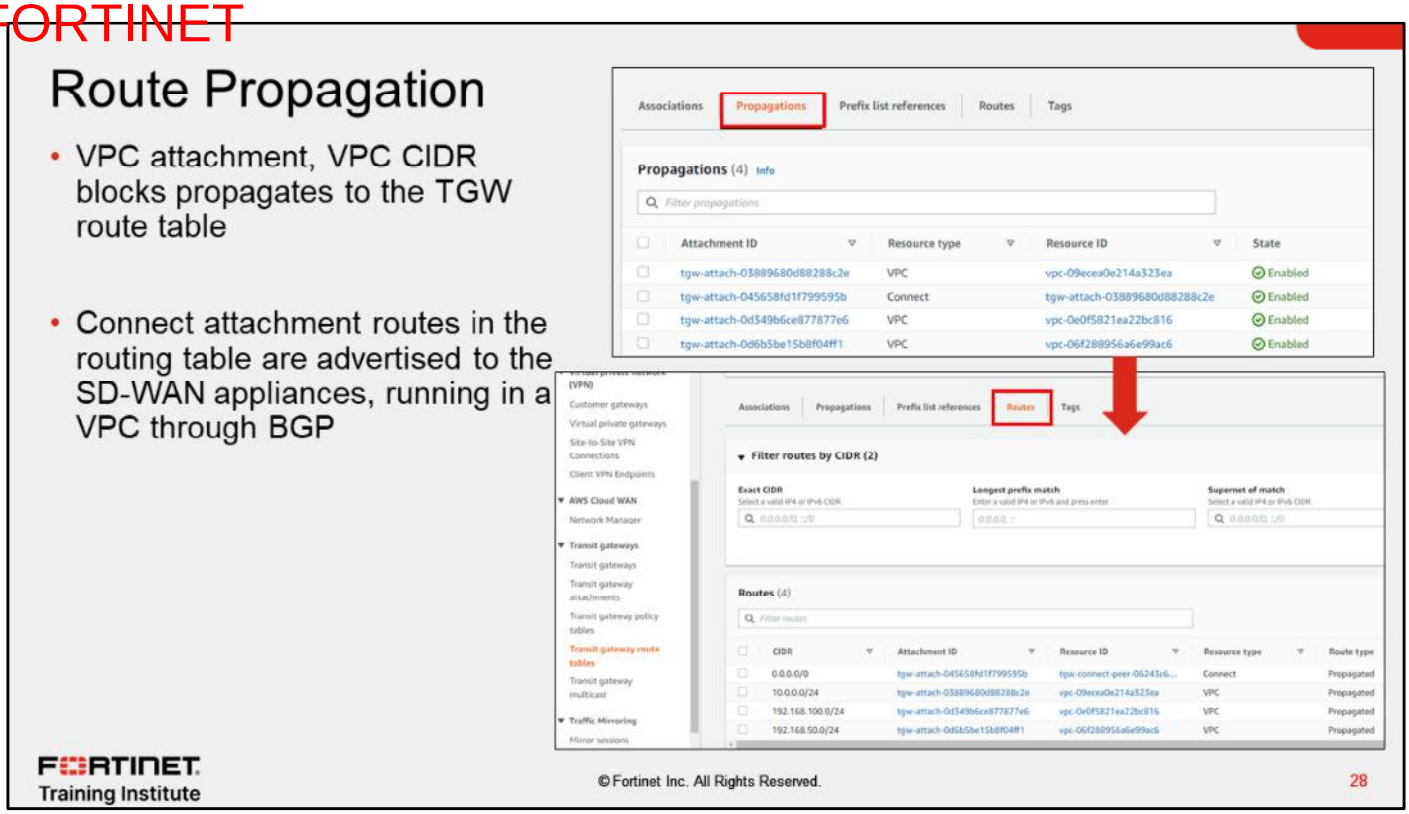
Your transit gateway routes IPv4 and IPv6 packets between attachments using transit gateway route tables. You can configure these route tables to propagate routes from the route tables for the attached VPCs, VPN connections, and direct connect gateways. You can also add static routes to the transit gateway route tables. When a packet comes from one attachment, it is routed to another attachment using the route that matches the destination IP address.

DO NOT REPRINT
© FORTINET



You can associate a transit gateway attachment with a single route table. You can associate each route table with zero to many attachments and forward packets to other attachments. You cannot associate the same attachment in a route table with another TGW route table. However, you can use route propagation to propagate routes to other TGW route tables.

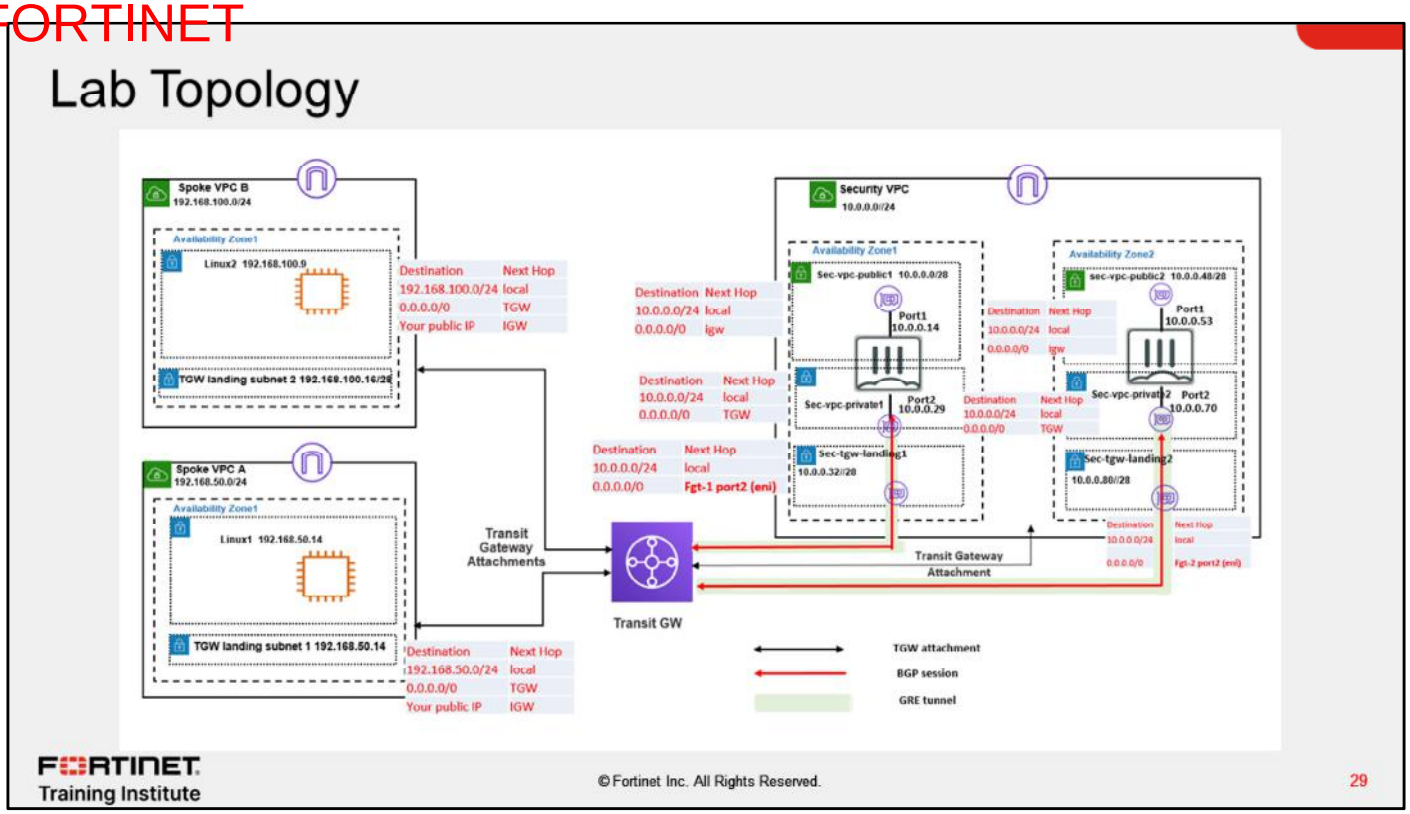
DO NOT REPRINT
© FORTINET



When you create an attachment in the transit gateway, each attachment comes with routes that can be installed in one or more transit gateway route tables. When an attachment is propagated to a transit gateway route table, these routes are installed in the route table.

VPC attachment: For a VPC attachment, the CIDR blocks of the VPC are propagated to the transit gateway route table.
Connect attachment: For a connect attachment, routes in the route table associated with the connect attachment are advertised to the third-party virtual devices, such as SD-WAN devices, running in a VPC through BGP.

DO NOT REPRINT
© FORTINET



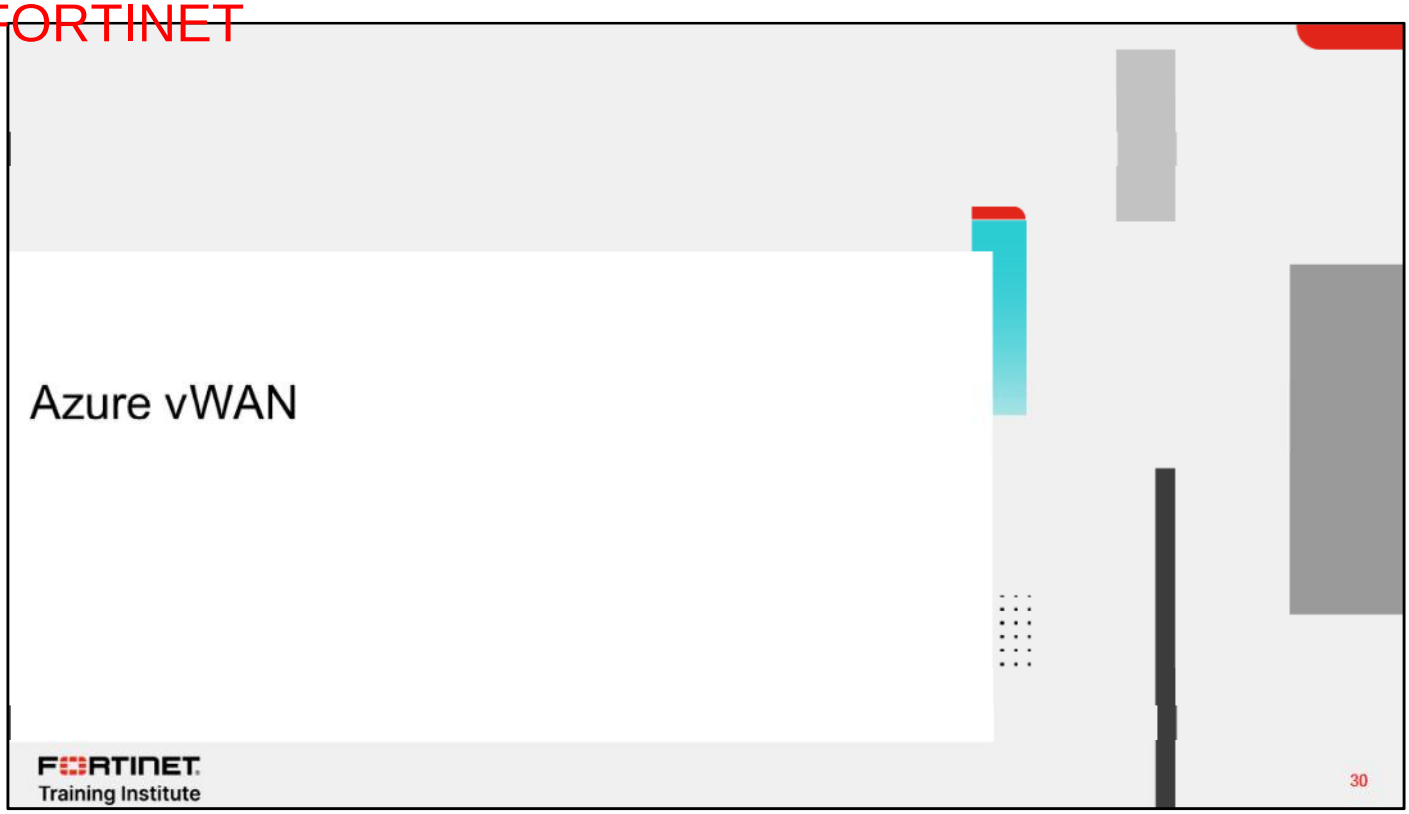
Now you will learn about the lab environment. The security VPC has two availability zones. Each availability zone in the security VPC has a FortiGate VM with public, private, and transit gateway landing subnets. It is highly recommended to use a separate subnet for each transit gateway VPC attachment. For each subnet, use a small CIDR, for example /28, so that you have more addresses for EC2 resources.

When you use a separate subnet, you can configure the following:
- Keep the inbound and outbound network ACLs associated with the transit gateway subnets open.
- Depending on your traffic flow, you can apply network ACLs to your workload subnets.

The Security and Spoke VPCs need the transport VPC attachments. For the Spoke VPCs, you can create it in one of the App subnets or on a dedicated subnet. In this topology, you will use the two dedicated subnets (landing subnets). When you create an attachment from the TGW for the Security VPC , you must create an attachment for each AZ. The architecture includes a dedicated subnet in each AZ for TGW creation.

There are two internet gateways in the spoke VPCs (Spoke VPC A and Spoke VPC B), however, in this lab you will use the IGW to gain access to the Linux1 and Linux2 instances only.

DO NOT REPRINT
© FORTINET

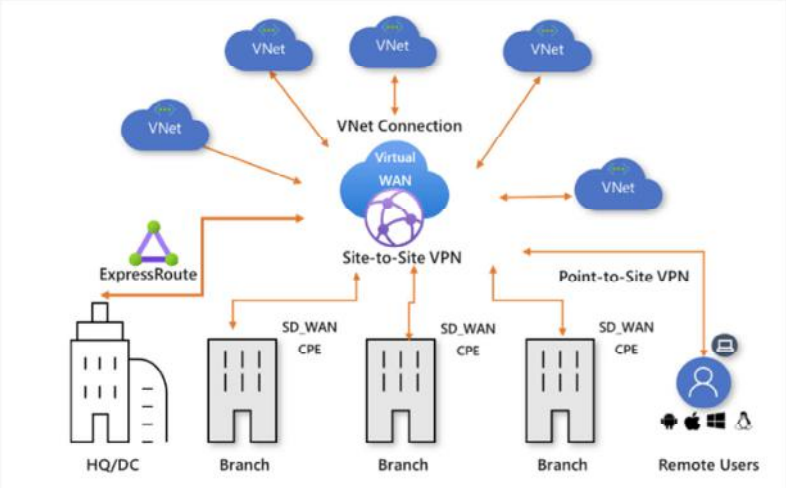


In this section, you will learn about the Azure vWAN.

DO NOT REPRINT
© FORTINET

What Is Azure vWAN?

- Managed networking service brings together:
  - Networking connectivity
  - Security
  - Monitoring
  - Routing
- Connection solutions
  - ExpressRoute
  - VPN Gateway
  - Routing, Azure Firewall, and so on
- vWan and on-premises SD-WAN can be combined to create a healthy SD-WAN ecosystem



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

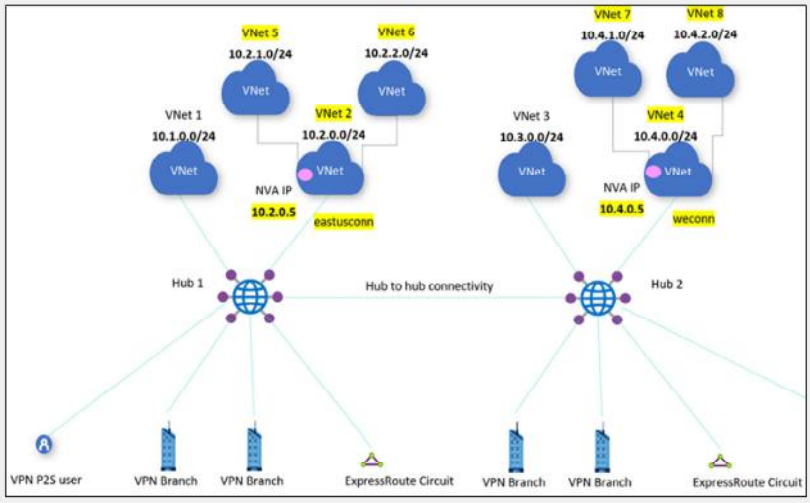
31

You have learned about AWS transit gateway and how it can be used to connect different VPCs with simple attachments. Now you will learn about a similar concept, Microsoft Azure. What is Azure vWAN? Azure vWAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. One of the main benefits of the Azure vWan is the single management interface for all the services. Combining the Azure vWAN and Fortinet SD-WAN solutions can give the customer a healthy SD-WAN ecosystem.

DO NOT REPRINT
© FORTINET

FortiGate Integrations With Azure vWAN

- FortiGate inside NVA VNET
  - Normal VNET hub and spoke deployment
  - A/A, A/P, VMSS
- Ideal solution to isolate and secure VNets



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

Before you deep dive into Azure vWAN, examine a few use cases.

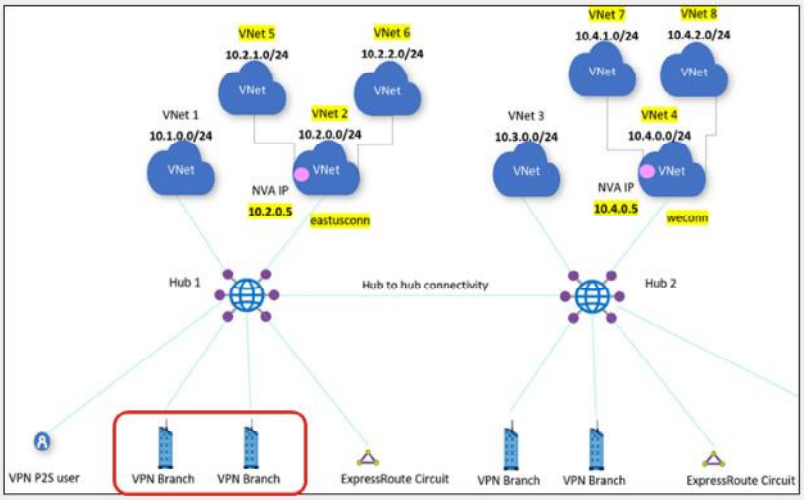
The first use case is FortiGate VM inside the NVA VNet. When examining the example on this slide, assume that the pink dot represents a FortiGate VM. VNet 5 and VNet 6 are connected to VNet 2. Also, both VNets are isolated and have no direct connection from the branch or hub. All the east-west traffic between Vnets is secured by VNet 2 and VNet 4, and it is a hub-and-spoke architecture. At the same time, any branch side connection to the VNets 5, 6, 7, or 8 will go through the FortiGate VMs and the traffic will be inspected. VNet1 and VNet3 are also isolated, and any traffic going through the branch to those two VNets can also be routed to the FortiGate for traffic inspection.

NVA VNets will know about their own NVA spokes, but not about NVA spokes connected to other NVA VNets. For example, as shown on this slide, VNet 2 knows about VNet 5 and VNet 6, but not about other spokes such as VNet 7 and VNet 8. A static route is required to inject the prefixes of other spokes into NVA Vnets.

DO NOT REPRINT
© FORTINET

FortiGate Integrations With Azure vWAN (Contd)

- FortiGate at branch site
  - Fortinet is listed as a virtual WAN partner
  - An ARM template is provided to automatically configure branch-to-site IPsec VPN connections



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

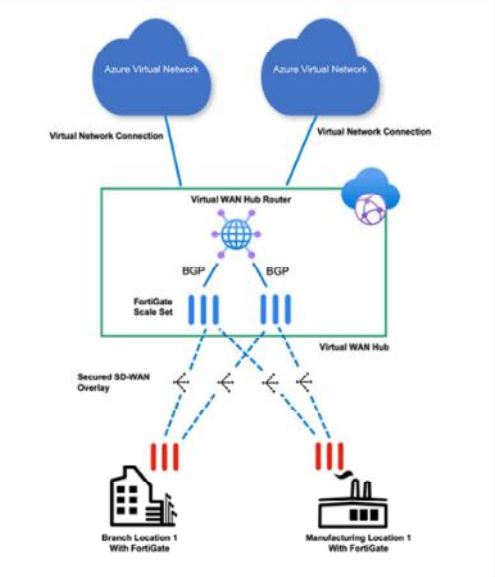
33

The second use case also involves a FortiGate VM at a branch site. Fortinet is listed as a virtual WAN partner and the FortiGate SD-WAN solution can be used in an on-premises customer branch site with a FortiGate device.

DO NOT REPRINT
© FORTINET

FortiGate Integrations With Azure vWAN (Contd)

- FortiGate Secure SD-WAN (inside virtual WAN hub)



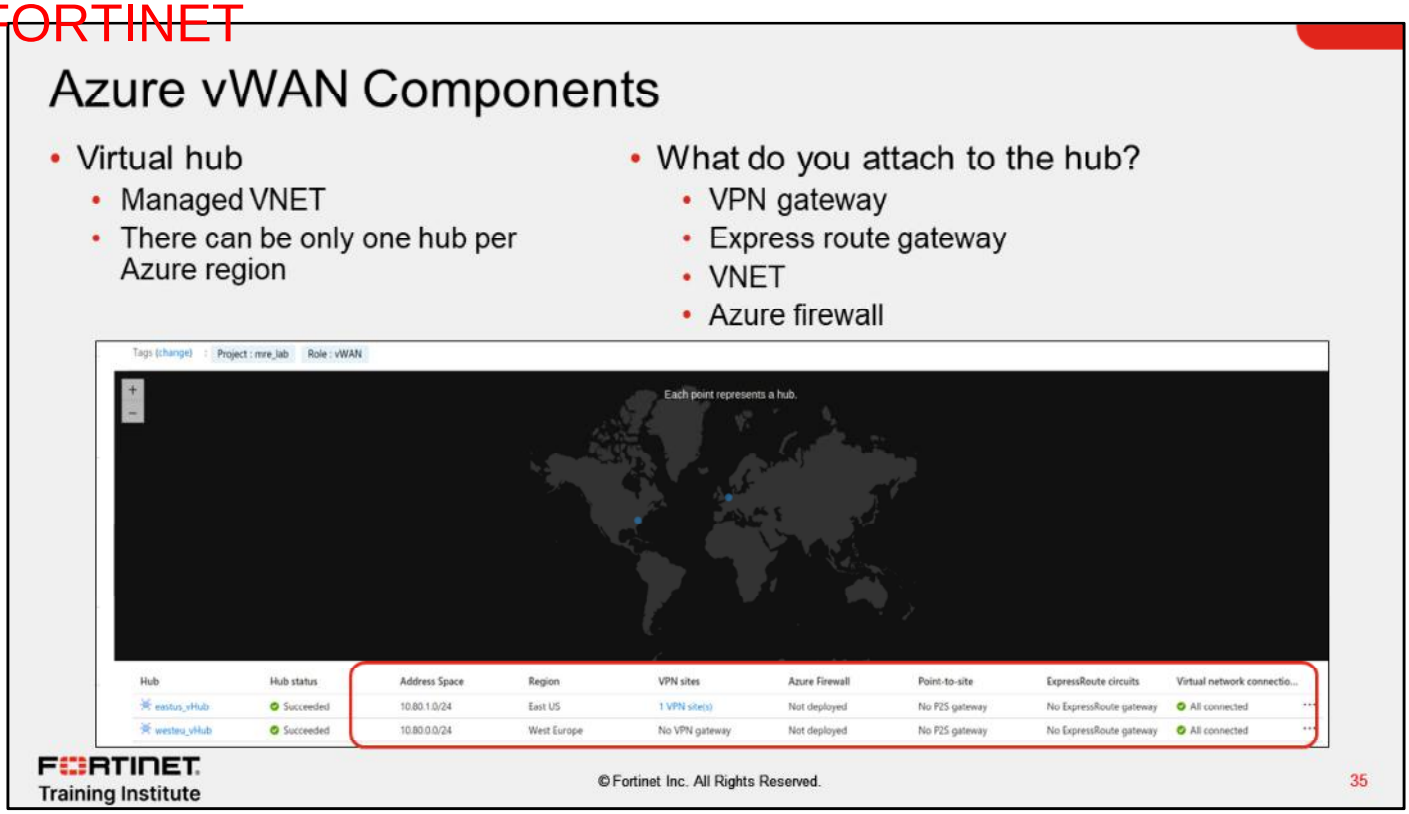
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

In the scenario shown on this slide, a FortiGate-VM active-active cluster is deployed and runs natively inside the virtual WAN hub. With this integration, the FortiGate-VMs are deployed in the virtual WAN hub using a managed application on Azure Marketplace. During deployment, the FortiGate-VMs are configured to peer using BGP with the virtual WAN hub router, as well as link it with FortiManager for further management. The solution is load balanced and configured for active-active highly resilient deployments. The integration of the FortiGate inside the virtual WAN hub requires FortiManager to manage the FortiGate instances and the SD-WAN configuration.

DO NOT REPRINT
© FORTINET

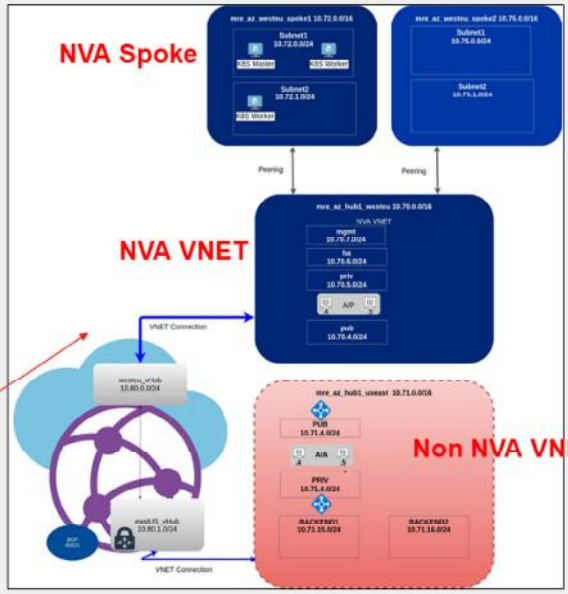


Now you will learn about Azure vWAN components. Azure regions serve as hubs that you can choose to connect to. All hubs are connected in full mesh in a standard virtual WAN making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity.

DO NOT REPRINT
© FORTINET

Azure vWAN Components (Contd)

- Virtual network connections
  - Managed VNET peering between the VNET and virtual hub
  - Can you modify peering settings? No
- Virtual network terminology
  - NVA VNET
  - NVA spoke: Not managed by vWAN hub
    - Routing to NVA spokes is maintained by the user
  - Non-NVA VNET



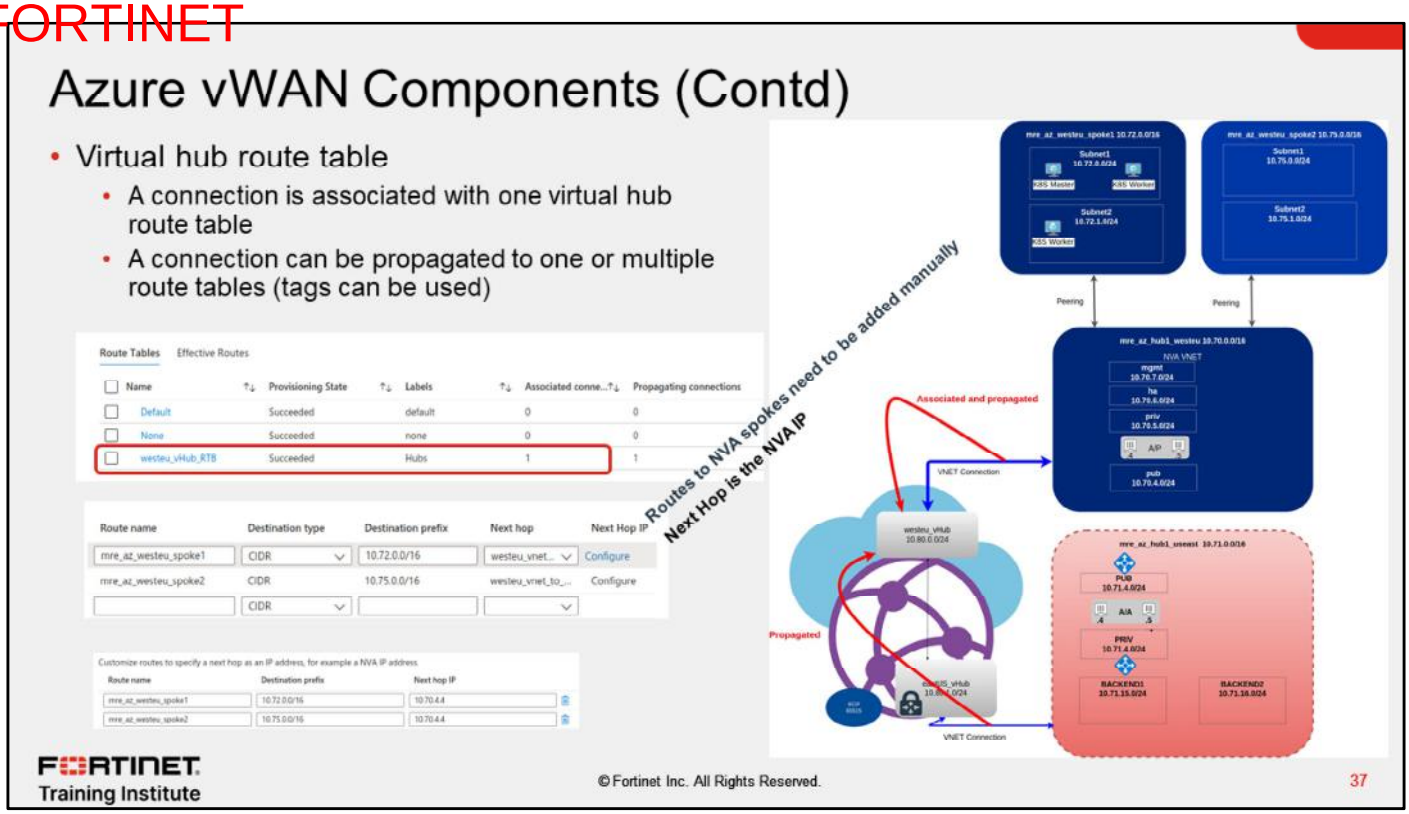
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

The virtual hub is the connection point in Azure for all the sites. The hub virtual network connection lets you have a connection point for the hub to the virtual network. As shown on this slide, NVA VNET is directly connected to the vWan hub, so, NVA Spoke is not directly connected the hub but through the NVA VNET. The non-NVA Vnet is connected to the hub, however, without any NVA. What is the VNET connection? It is a peering connection between the VNET and Azure virtual hub.

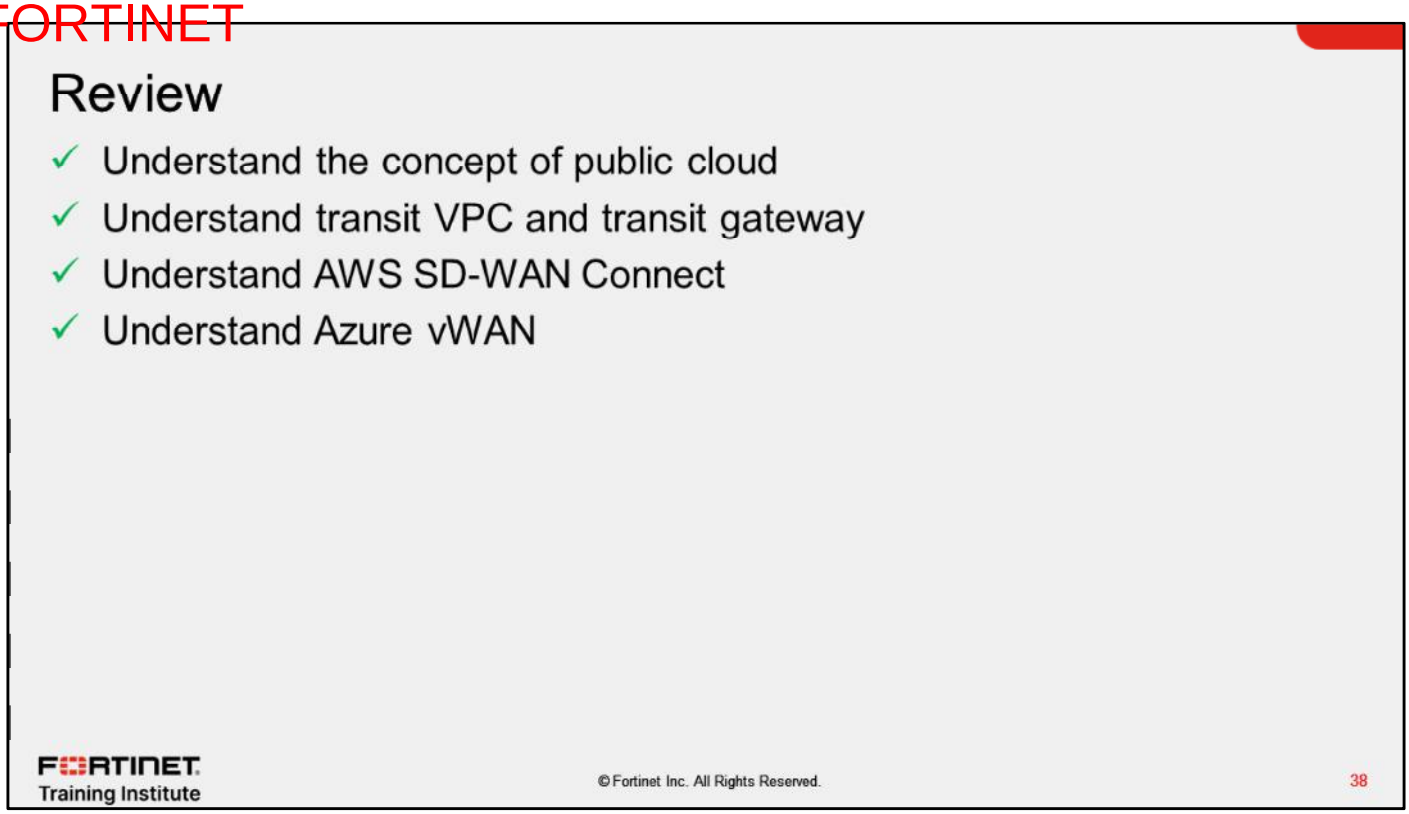
DO NOT REPRINT
© FORTINET



The virtual hub is the connection point in Azure for all the sites. This is the virtual hub route table and similar to the AWS TGW route table that you learned about earlier. The Vnet connection is attached to the route table, similar to the AWS transit gateway attachment associated with the route table. Also, the connection can be propagated to the route table. It means that all those Vnet CIDRs will be propagated. It is important to know that routes to the NVA spokes must be added manually. Add an aggregated static route entry for NVA spokes to the hub default route table.

As shown in this example, next hop IP for the route from hub to spoke is the NVA `10.70.4.4`.

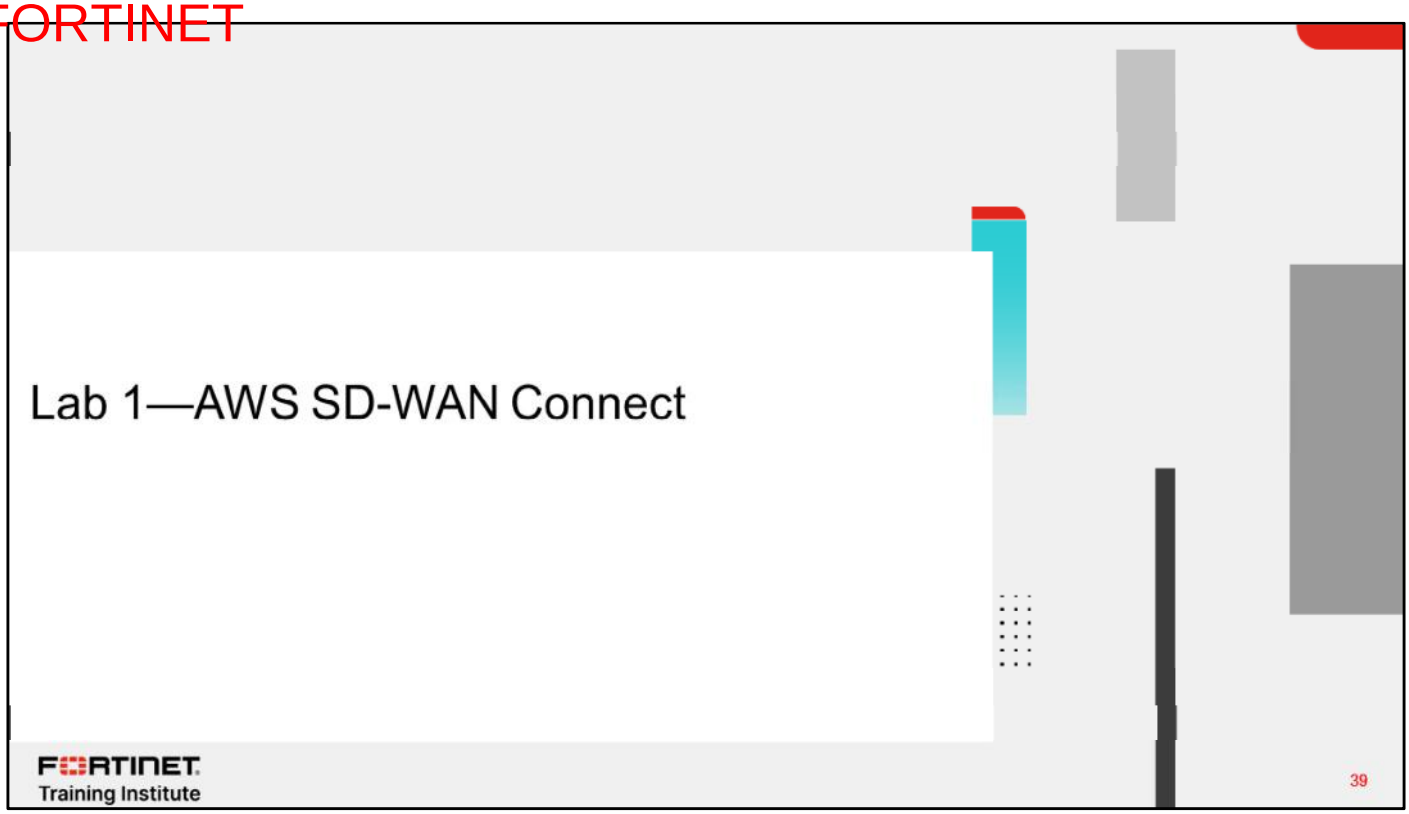
DO NOT REPRINT
© FORTINET



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

By mastering the objectives covered in this lesson, you learned about FortiGate deployment.

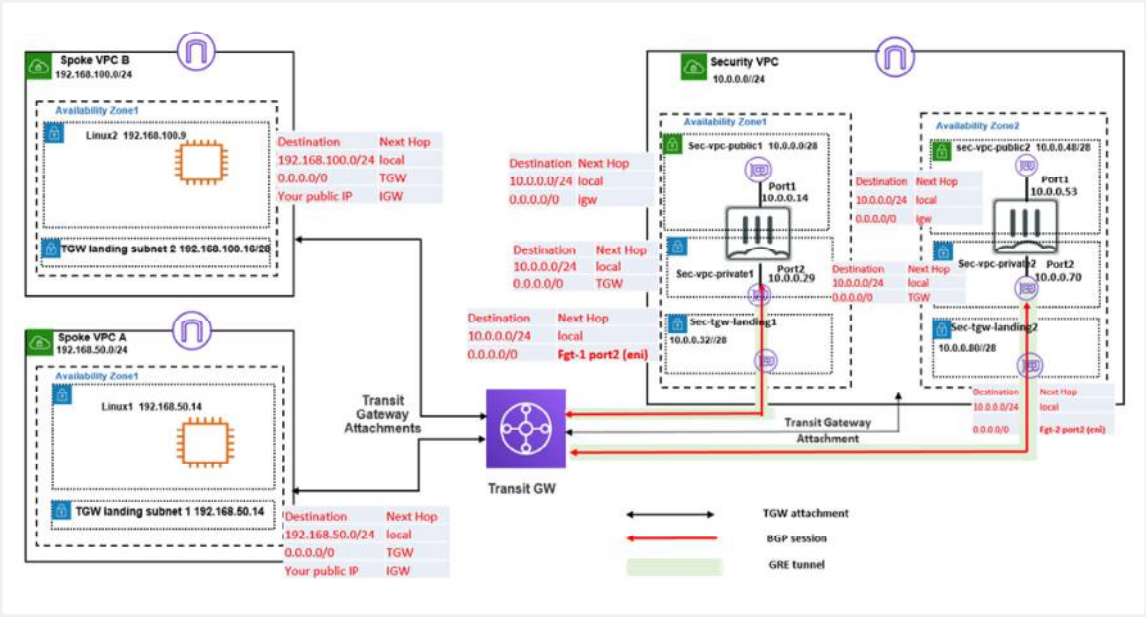
DO NOT REPRINT
© FORTINET



Now, you will work on *Lab 1–AWS SD-WAN Connect*.

DO NOT REPRINT
© FORTINET

Lab 1—AWS SD-WAN Connect



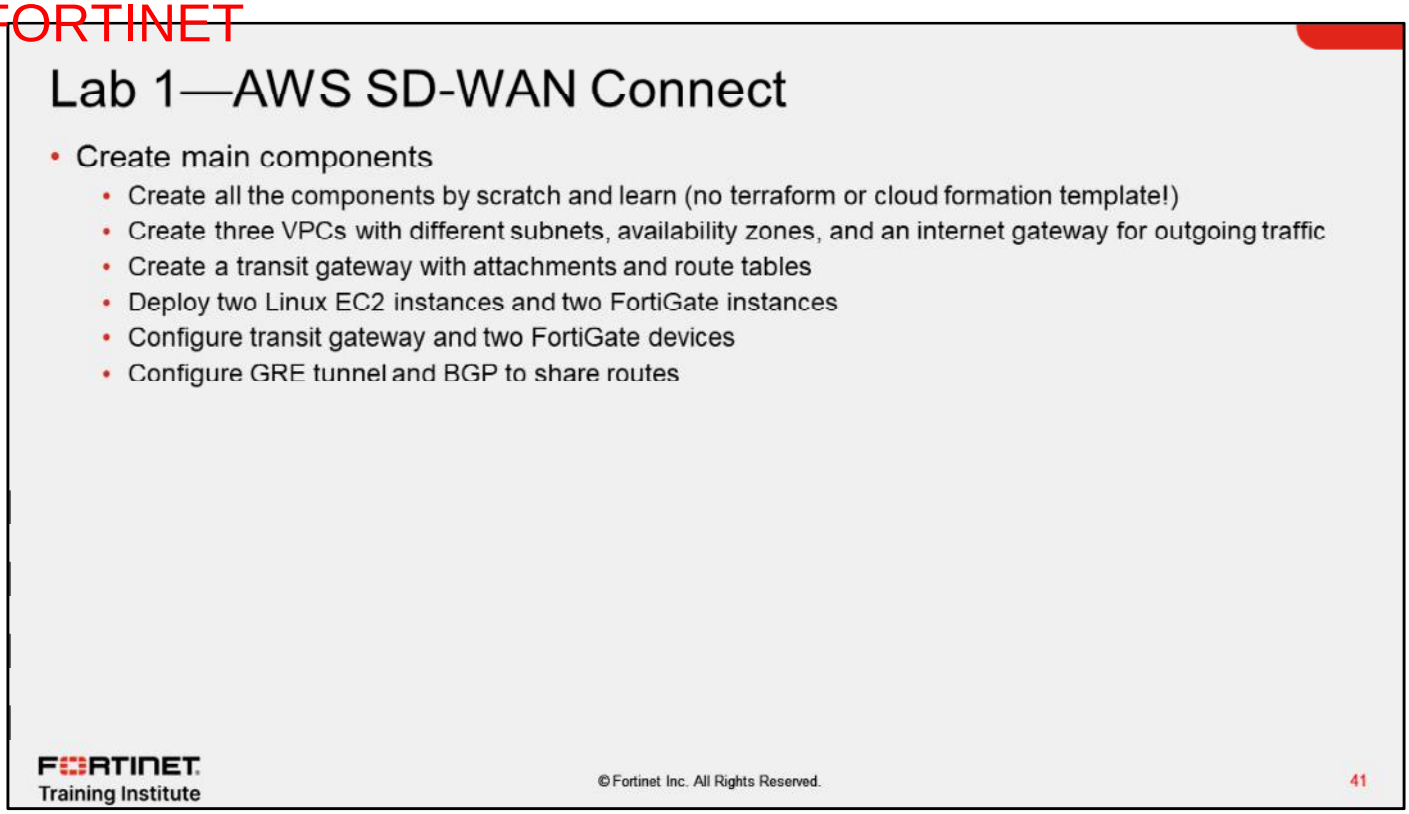
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

In this lab, you will configure the AWS topology shown on this slide.

DO NOT REPRINT
© FORTINET

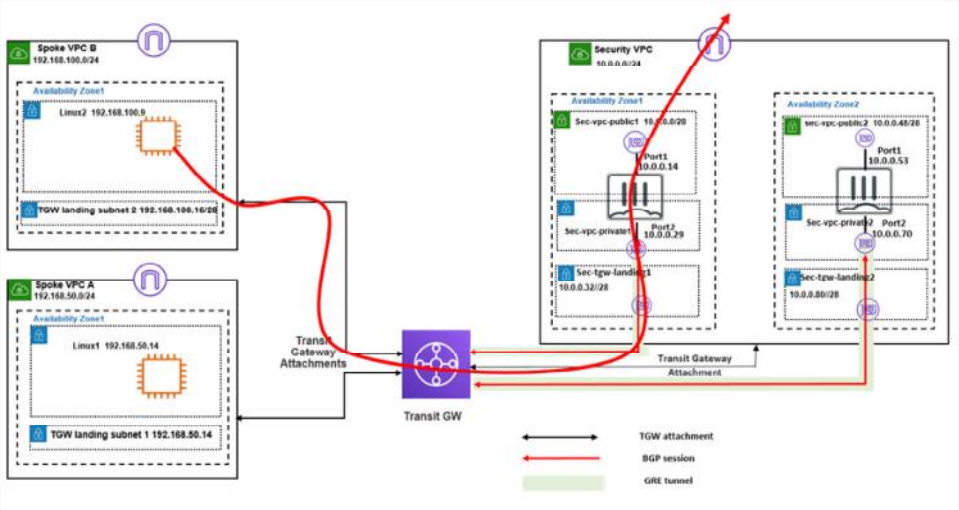


In this lab, you will create all the components on AWS. You could create this environment by using Terraform or a cloud formation template. However, you will create all the components manually, which will help you to understand each component in depth.

DO NOT REPRINT
© FORTINET

Lab 1—AWS SD-WAN Connect

- North-south traffic
  - Configure the necessary components that enable Spoke VPC A and Spoke VPC B traffic to flow through the Security VPC



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

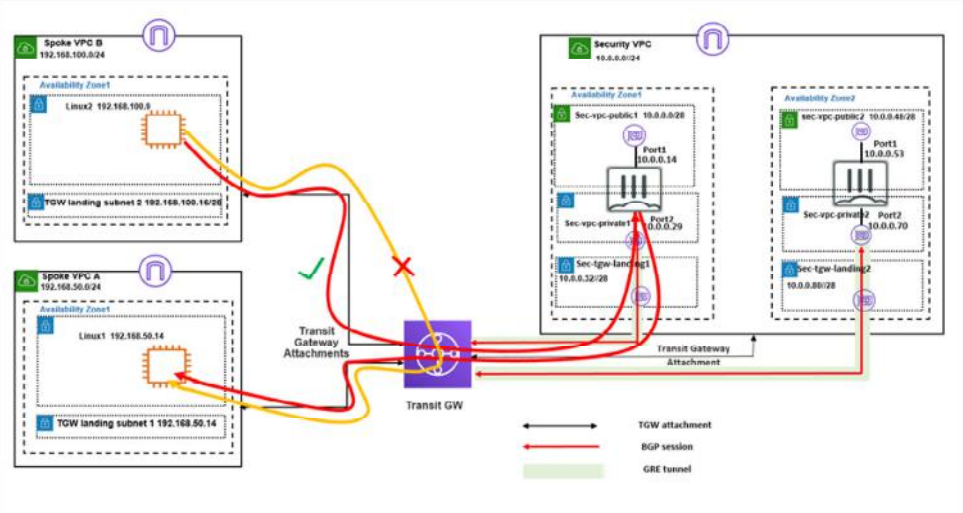
42

Your traffic from Spoke VPC A and Spoke VPC B should flow through the FortiGate VMs in the Security VPC. This is the north-south traffic.

DO NOT REPRINT
© FORTINET

Lab 1—AWS SD-WAN Connect

- East-west traffic
  - Configure the necessary components that enable traffic between Spoke VPC A and Spoke VPC B to flow through the FortiGate VM in the Security VPC



FORTINET Training Institute

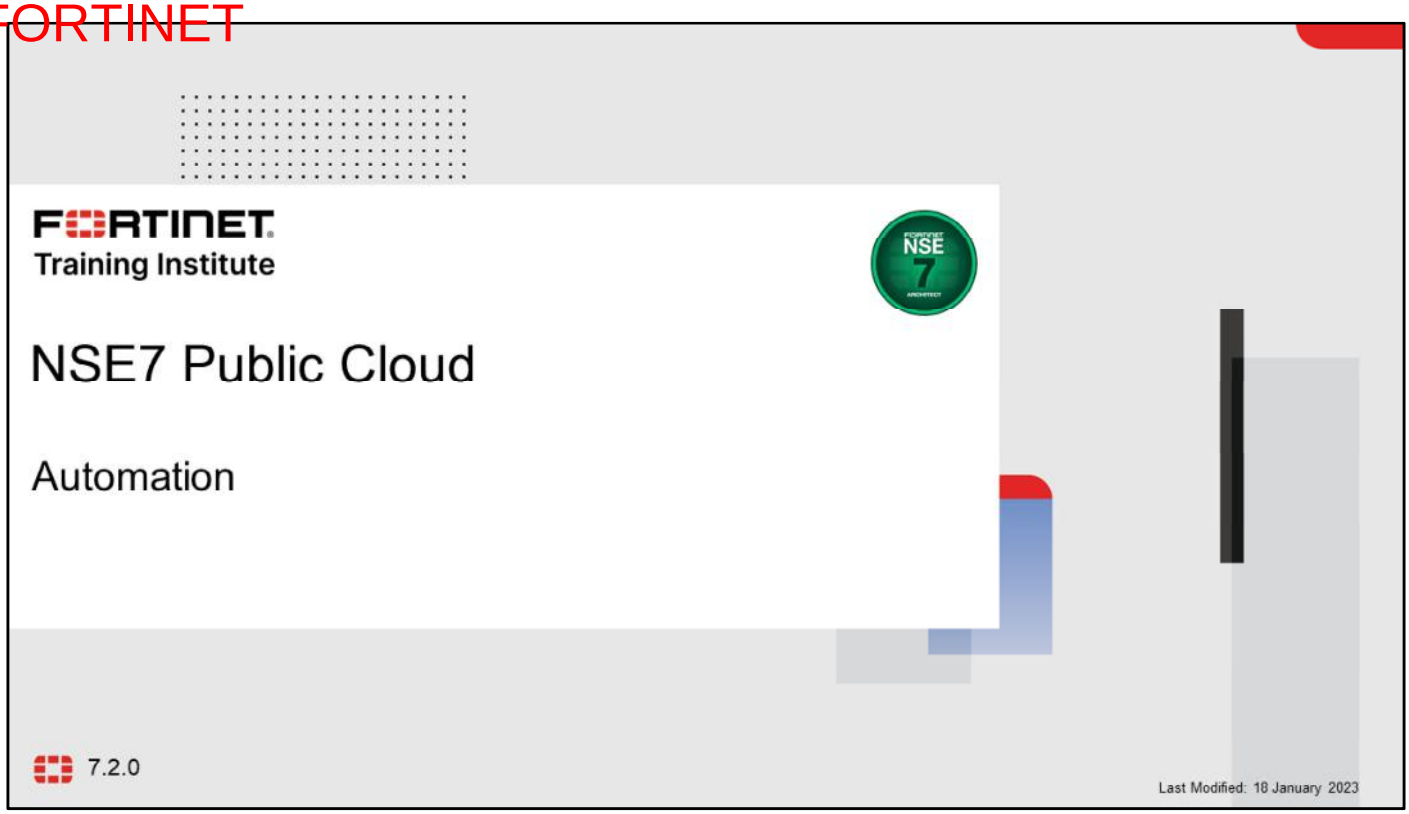
© Fortinet Inc. All Rights Reserved.

43

The issue is that east-west traffic is not flowing through the Security VPC and being inspected by FortiGate devices. Your goal is to check your transit gateway routing table and make the necessary changes to get east-west traffic working.

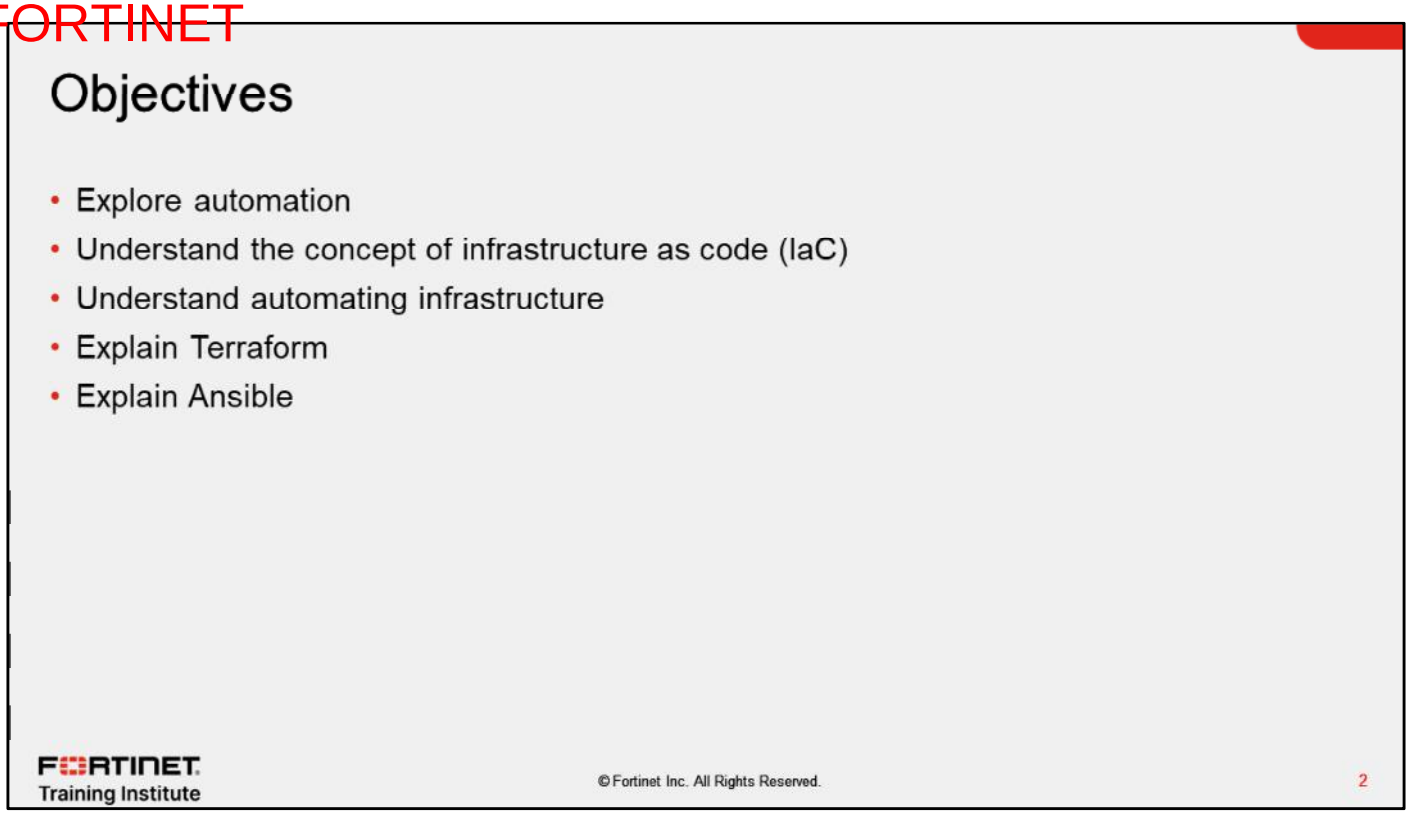
If you are successful, the traffic between Spoke VPC A and Spoke VPC B (Linux1 and Linux2), will flow through the Security VPC and be inspected by the FortiGate VMs.

DO NOT REPRINT
© FORTINET



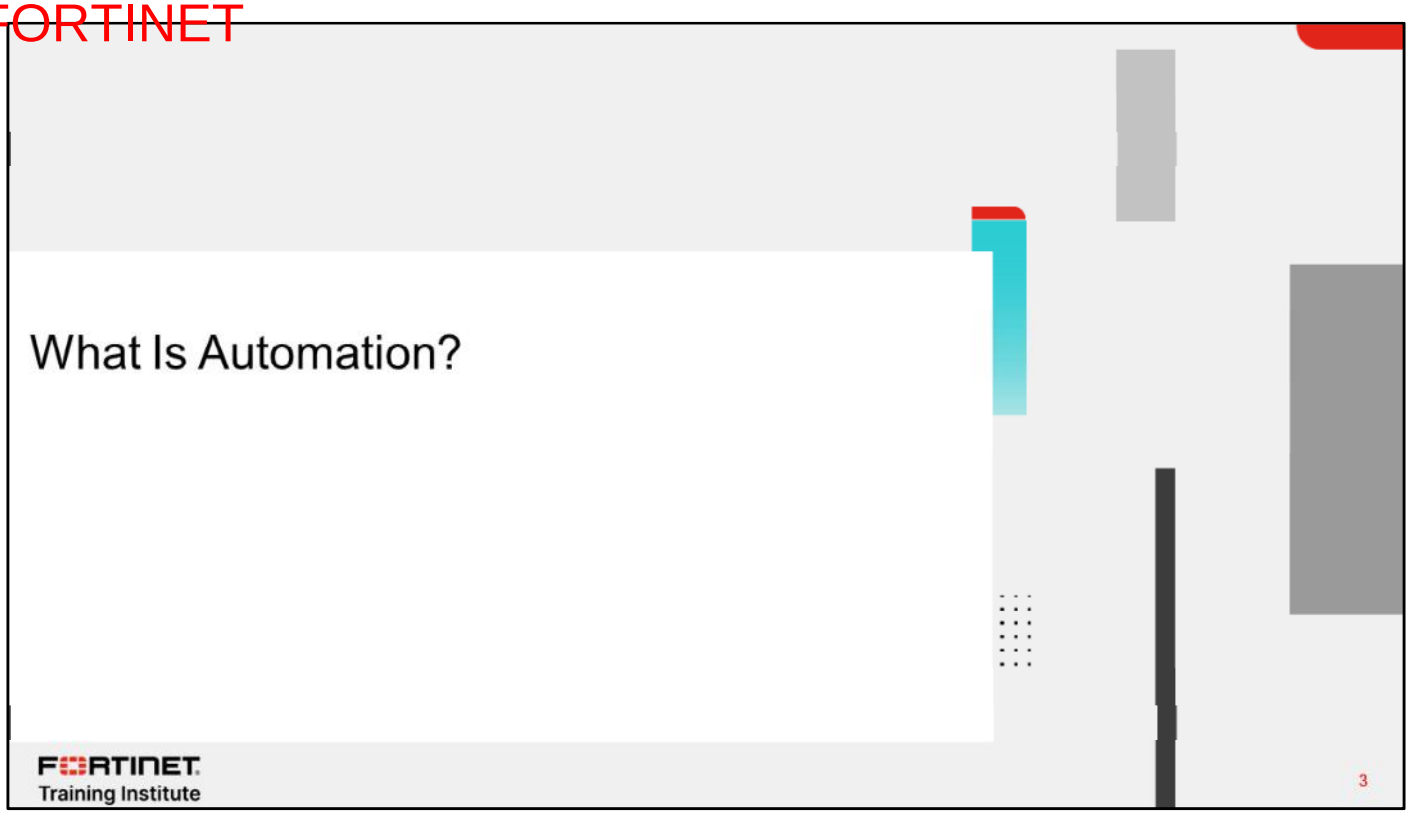
In this lesson, you will learn about automation.

DO NOT REPRINT
© FORTINET



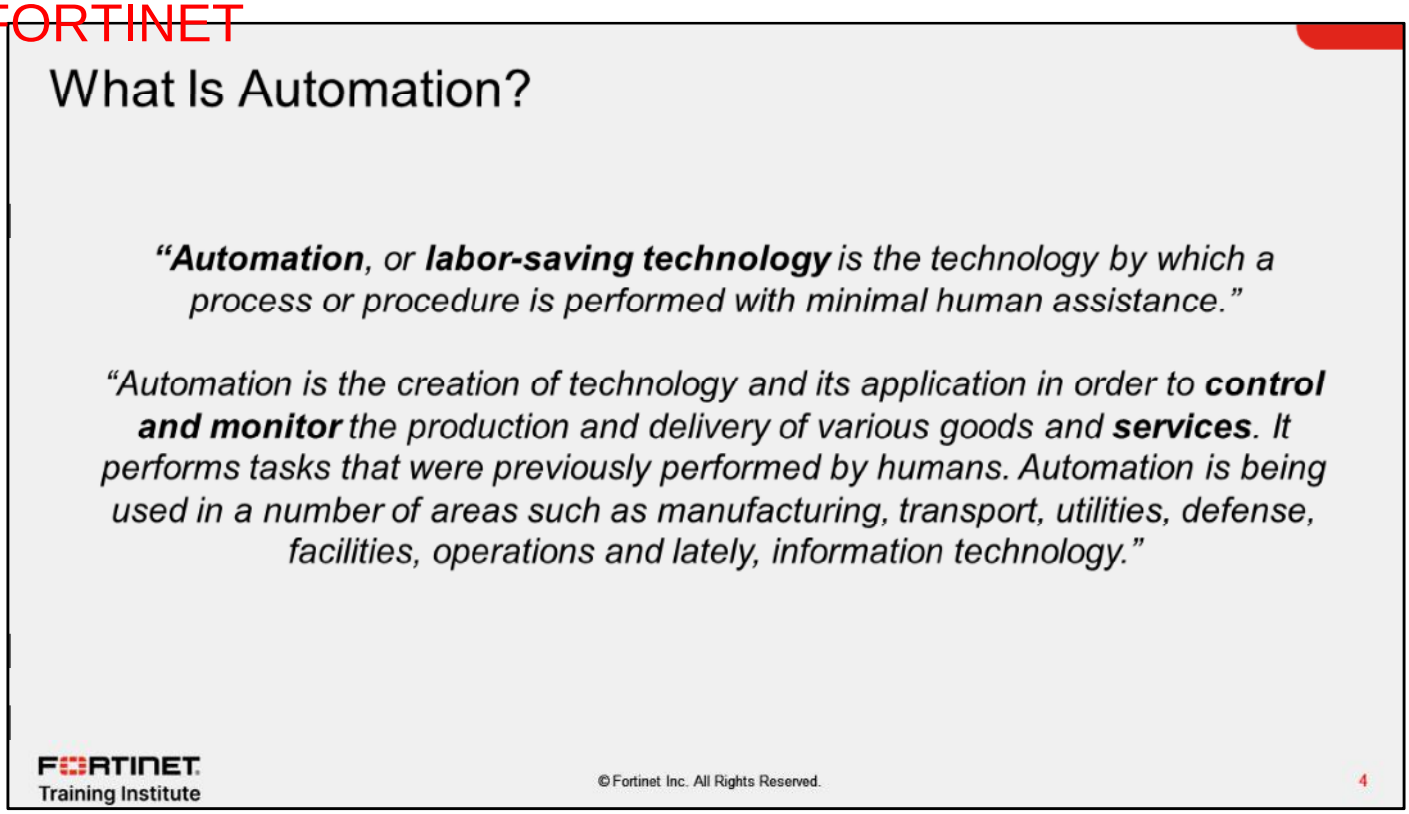
After completing this section, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn about automation and how to use it.

DO NOT REPRINT
© FORTINET

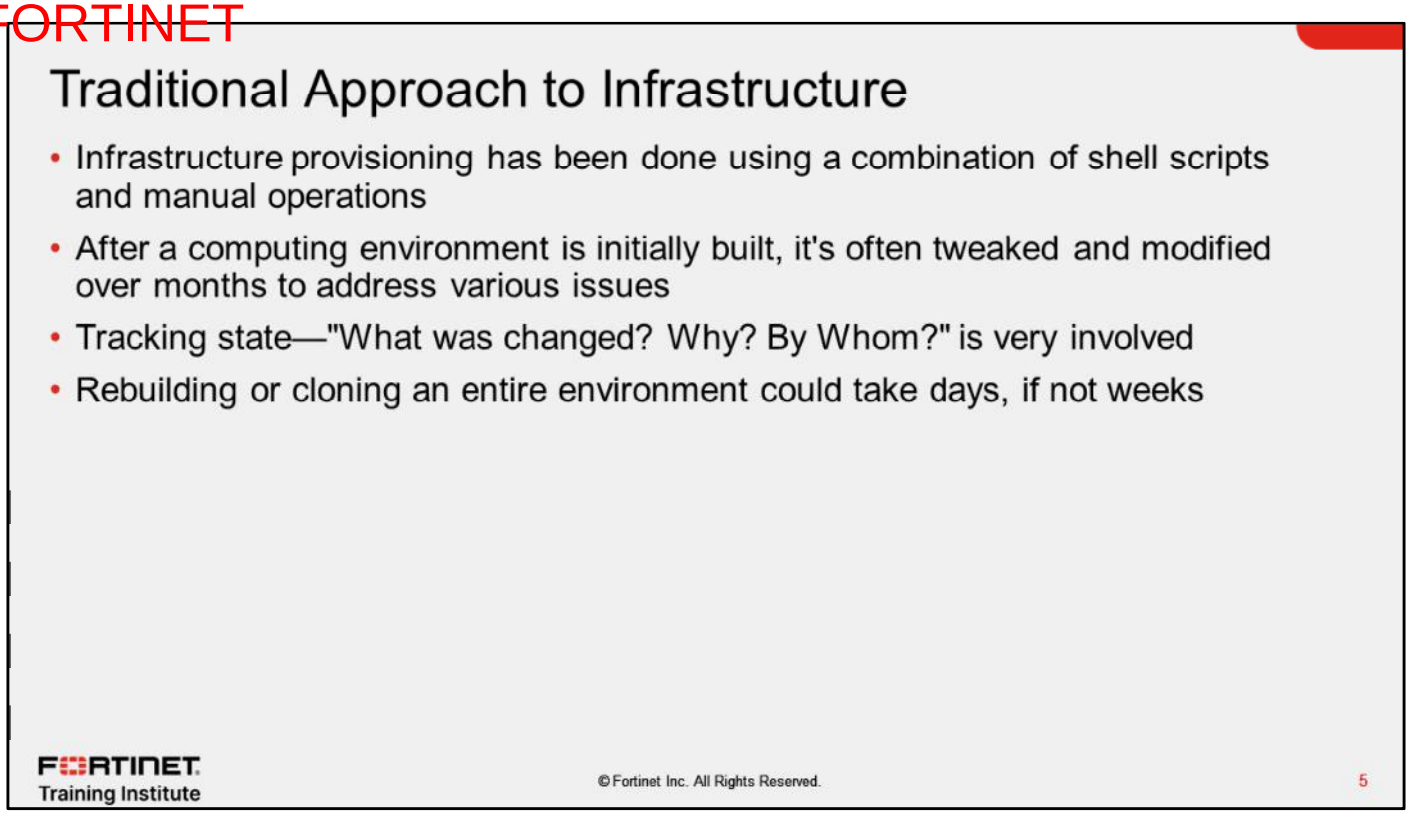


So, what do we mean by "automation"? Automation has many different aspects associated with it. First, it is a labor-saving technology. This certainly applies to the IT industry where there continues to be a shortage of qualified staff. This shortage can be partly mitigated by applying automation where possible for executing repetitive tasks.

Automation is also used to control and monitor production environments and services. A good example of this type of automation is the implementation of self-service portals, where customers are able to execute their own changes in a controlled environment. Automated back-end systems apply those changes to the production systems, in much the same way as a firewall-as-a-service like FortiSASE is implemented.

There are a lot of benefits when it comes to automation, and the result is that automation features are being added to many products, including network and security solutions.

DO NOT REPRINT
© FORTINET



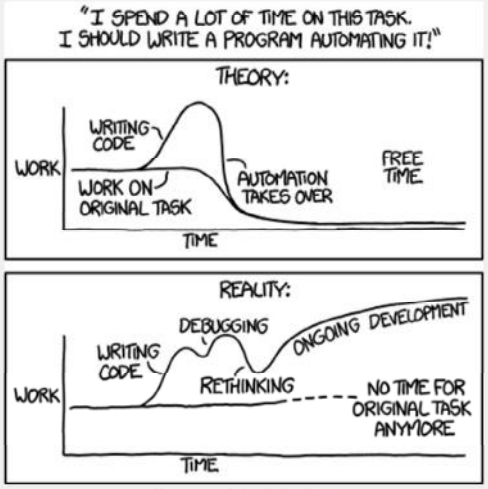
So what is the traditional approach to infrastructure? The provisioning has been done through a combination of shell scripts and manual operations. After the computer environment is initially built, it often need constant attention and more work over months to address various issues. At the same time, administrators must be heavily involved in tracking changes to ensure the integrity of the system.

DO NOT REPRINT
© FORTINET

Why Do You Need Automation?

- Efficiency
- Scalability
- Speed
- Error reduction
- Improved productivity
- Faster team collaboration
- Repetitive tasks are boring

Among other reasons...



Source: XKCD: Automation

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

So, why do you need automation? As shown on this slide, there are many reasons and benefits. At the same time, automation can become a drawback in which writing and maintaining the automation code might take more time than the time spent doing the task manually. Also, the time component is not always relevant, for example, when the main goal for automation is to repeat a task that requires a very high level of accuracy and needs to be reproducible on demand without any delay.

DO NOT REPRINT
© FORTINET

Infrastructure Immutability

- Configuration drift can happen if there are frequent configuration changes
- Changing the configuration of the running server may lead to unintended behavior
- Maintaining an immutable infrastructure is the best practice to avoid configuration drift
- *Immutable Infrastructure is a practice of provisioning a new server for every configuration change and deprovisioning the old ones*

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

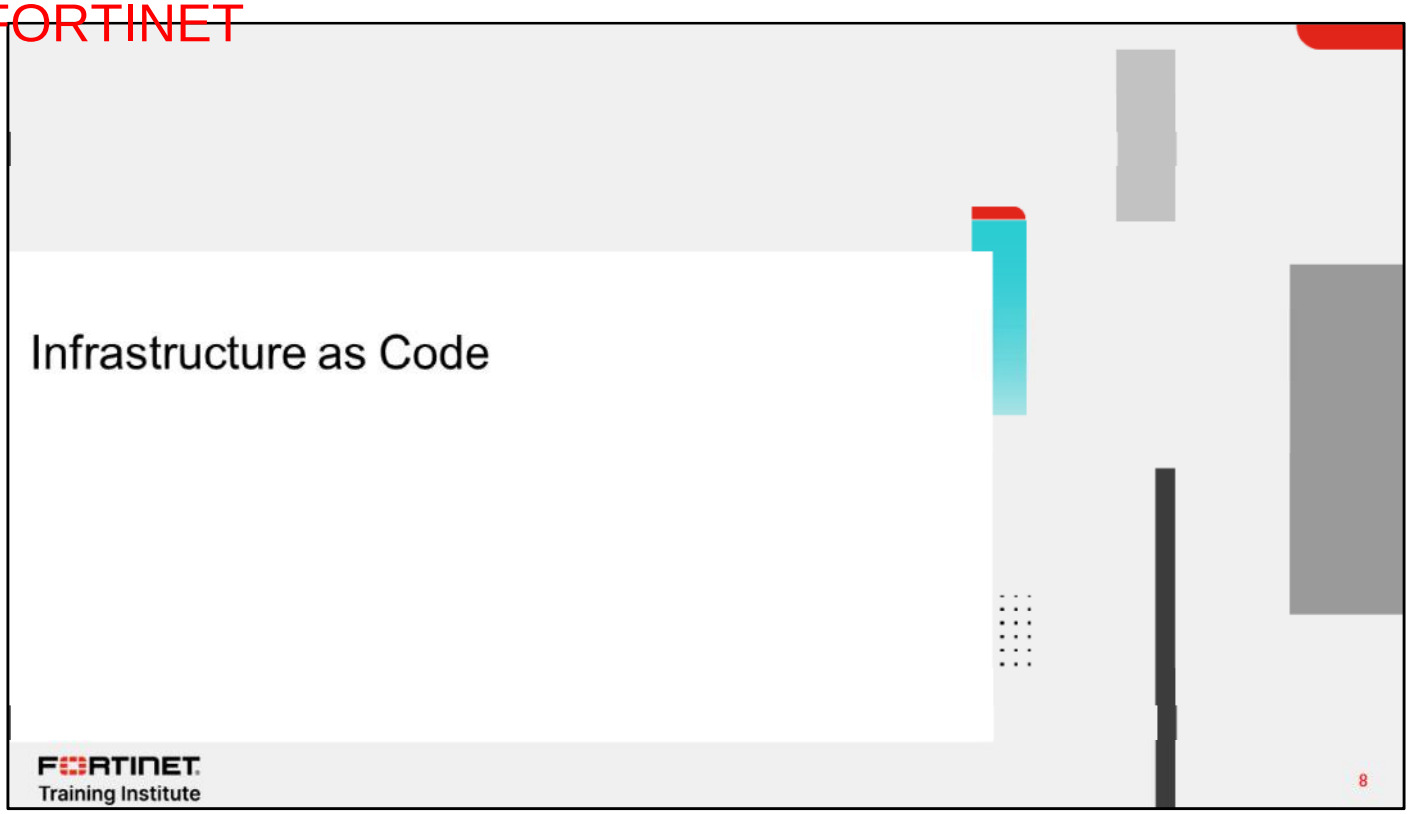
7

Another aspect to consider is the mutability of an infrastructure.

Even when you use configuration management tools to maintain the infrastructure, there is a chance of configuration drift in the servers if there are frequent changes being applied. This is especially true in organizations that have larger teams. In order to avoid this situation, it's becoming a practice among the DevOps community not to modify the configuration of an existing server after it is deployed. This is called an Immutable Infrastructure. An immutable infrastructure basically consists of provisioning a new server for every configuration change. There is no longer a need to worry about configuration changes and their impact over time.

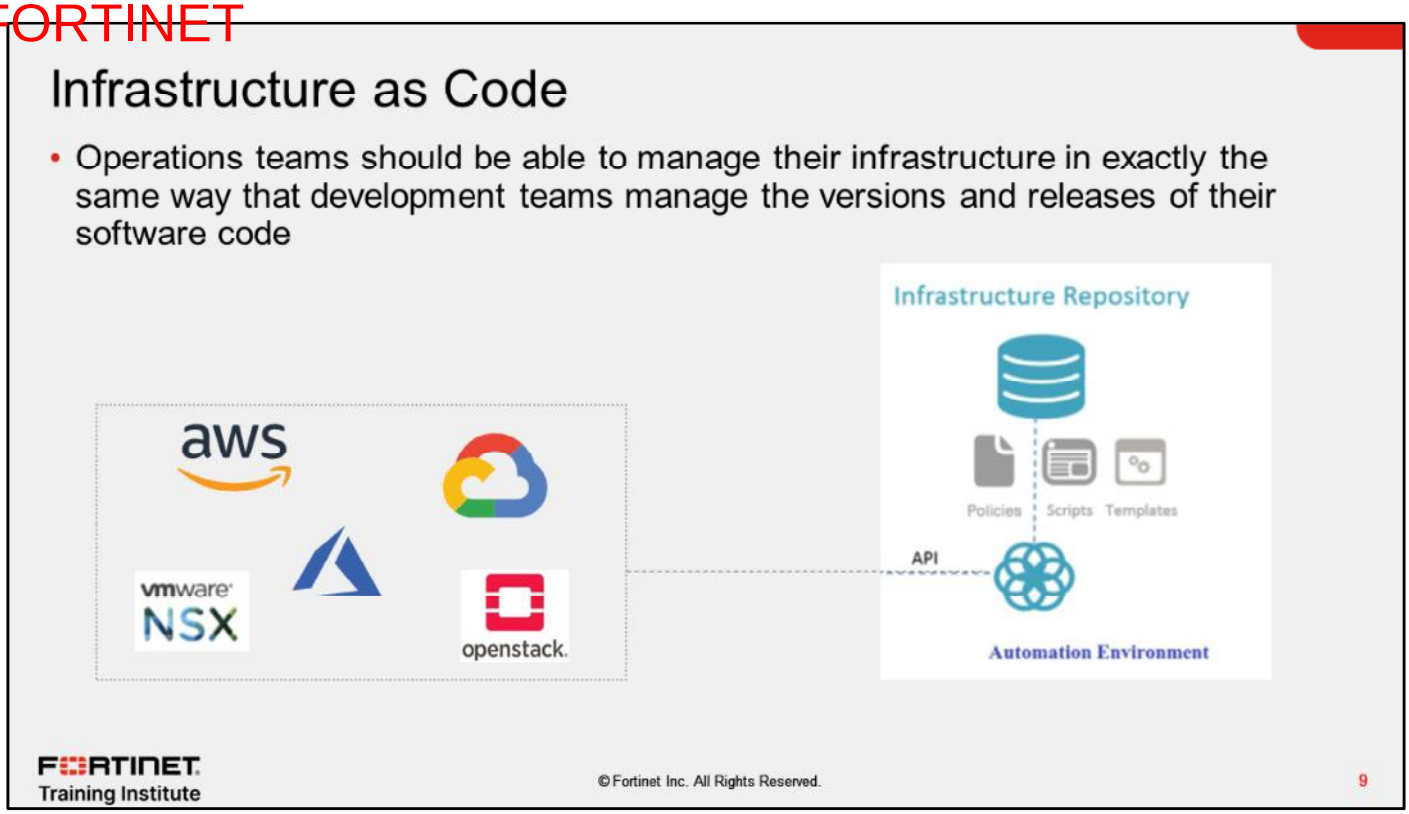
In modern production environments, DevOps engineers often follow a blue-green deployment strategy, which consists of deploying new resources for configuration changes and validating the deployment before deleting the old ones. In case of problems with the new configuration, rollback is very easy because the former deployment hasn't been changed.

DO NOT REPRINT
© FORTINET



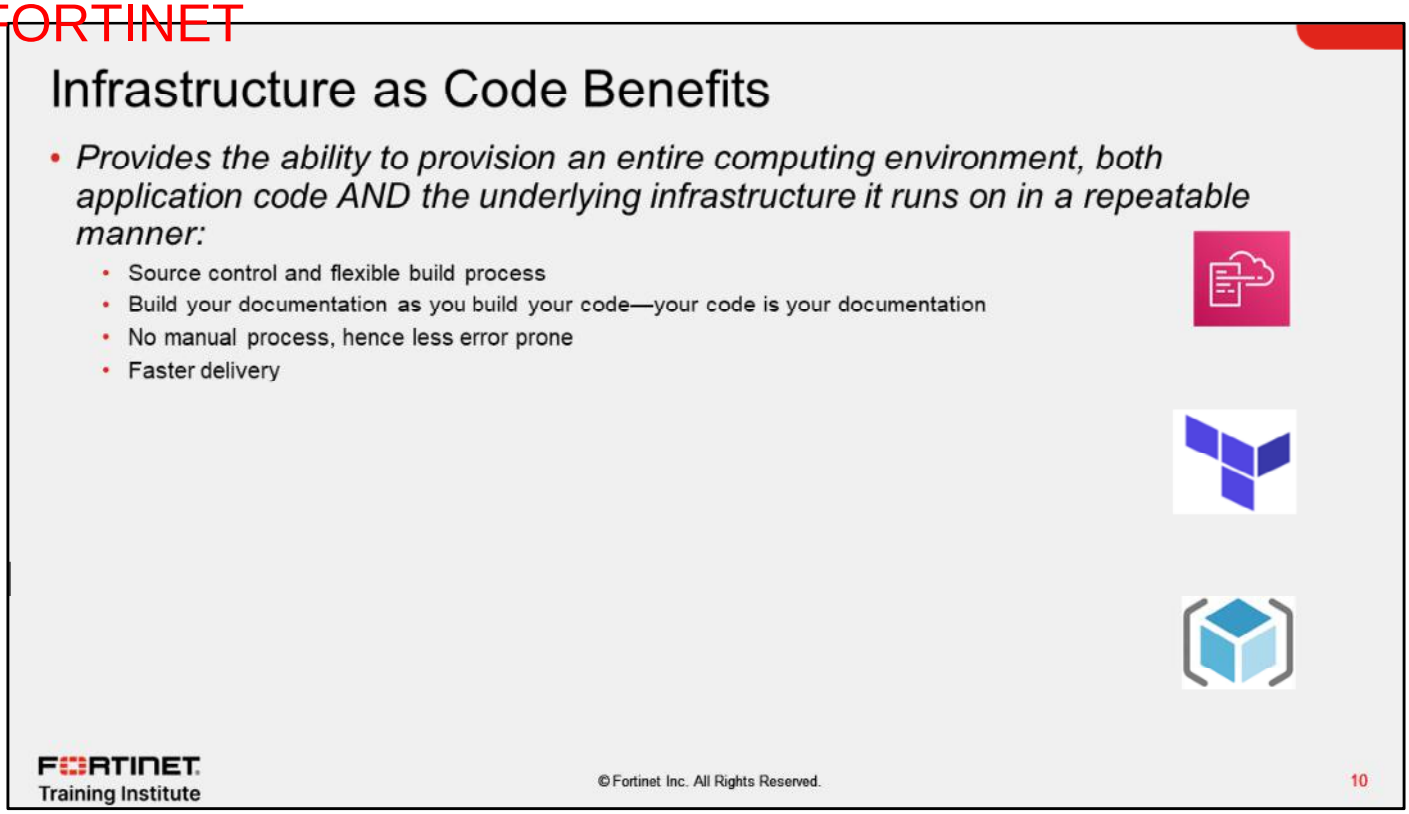
In this section, you will learn about infrastructure as code (IaC).

DO NOT REPRINT
© FORTINET



In the past, managing IT infrastructure was not an easy job. There were many administrators involved, and many hours were spent to deploy a single server. After getting the server up and running, there is more work to install the software that is needed for the applications to run. Now, with the help of cloud computing, operation teams can manage their infrastructure in the same way as development teams manage their software code with versions.

DO NOT REPRINT
© FORTINET



Administrators can now provision an entire computing environment, both application code and underlying infrastructure, in a repeatable manner. This gives the ability, for example, to leverage source control tools for the code that represents the infrastructure, which makes it much easier for a team to review changes before they are deployed, catching problems before they happen. Also, the source code becomes your documentation. Not to mention that the reduction manual process means less errors that cost time and money.

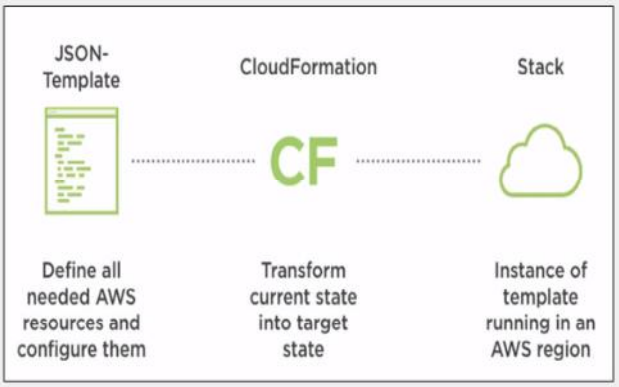
DO NOT REPRINT
© FORTINET

In this section, you will learn about automating infrastructure.

DO NOT REPRINT
© FORTINET

AWS CloudFormation

- Template-driven IaC solution
- Templates can be written in either JSON or YAML
- Very flexible and can be coupled with a graphical interface
- *Can only be used to provision resources on AWS*
- *Powerful, but a task in and of itself to work with and maintain*



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

AWS CloudFormation is a template-driven IaC solution. An administrator can deploy a whole network environment with a template that is easy to understand. It supports configurations using JSON or YAML language that describe resources, dependencies and runtime parameters. There is no need to define the order in which the AWS services should be provisioned. A template can be written in either JSON or YAML format.

DO NOT REPRINT
© FORTINET

AWS CloudFormation (Contd)

- *This code is approximately 25% of the JSON definition needed to build a single EC2 instance in a single VPC*

```
        }
      }
    },
    "Fgt2": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "ImageId": {
          "Fn::FindInMap": ["RegionMap", {
            "Ref": "AWS::Region"
          }, "fgtami"]
        },
        "InstanceType": {
          "Ref": "FGTInstanceType"
        },
        "KeyName": {
          "Ref": "KeyName"
        },
        "NetworkInterfaces": [{
            "NetworkInterfaceId": {
              "Ref": "FGT2ENI0"
            },
            "DeviceIndex": "0"
          }
        ],
        "Tags": [{
          "Key": "Name",
          "Value": {
            "Fn::Join": [
              "", [{
                  "Ref": "AWS::StackName"
                },
                "-fgt2"
              ]
            ]
          }
        }],
        "UserData": {
          "Fn::Base64": {
            "Fn::Join": ["\n", [
              "config system global",
              "set hostname Fgt2",
              "set admintimeout 60",
              "end"
            ]]
          }
        }
      }
    }
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

As shown on this slide, the code on the right side represents approximately 25% of the JSON definition that is needed to build a single EC2 instance in a single VPC.

DO NOT REPRINT
© FORTINET

Google Cloud Deployment Manager

- Similar to AWS CloudFormation but using a simpler YAML markup structure to work with Google Compute Engine (GCE) and Google Cloud Platform (GCP)

```
resources:
- type: compute.v1.instance
  name: vm-my-first-deployment
  properties:
    zone: us-central1-f
    machineType: https://www.googleapis.com/compute/v1/projects/bentest/zones/us-central1-f/machineTypes/f1-micro
    disks:
    - deviceName: boot
      type: PERSISTENT
      boot: true
      autoDelete: true
      initializeParams:
        sourceImage: https://www.googleapis.com/compute/v1/projects/debian-cloud/global/images/debian-8-jessie-v20160301
    networkInterfaces:
    - network: https://www.googleapis.com/compute/v1/projects/bentest/global/networks/default
      accessConfigs:
      - name: External NAT
        type: ONE_TO_ONE_NAT
```

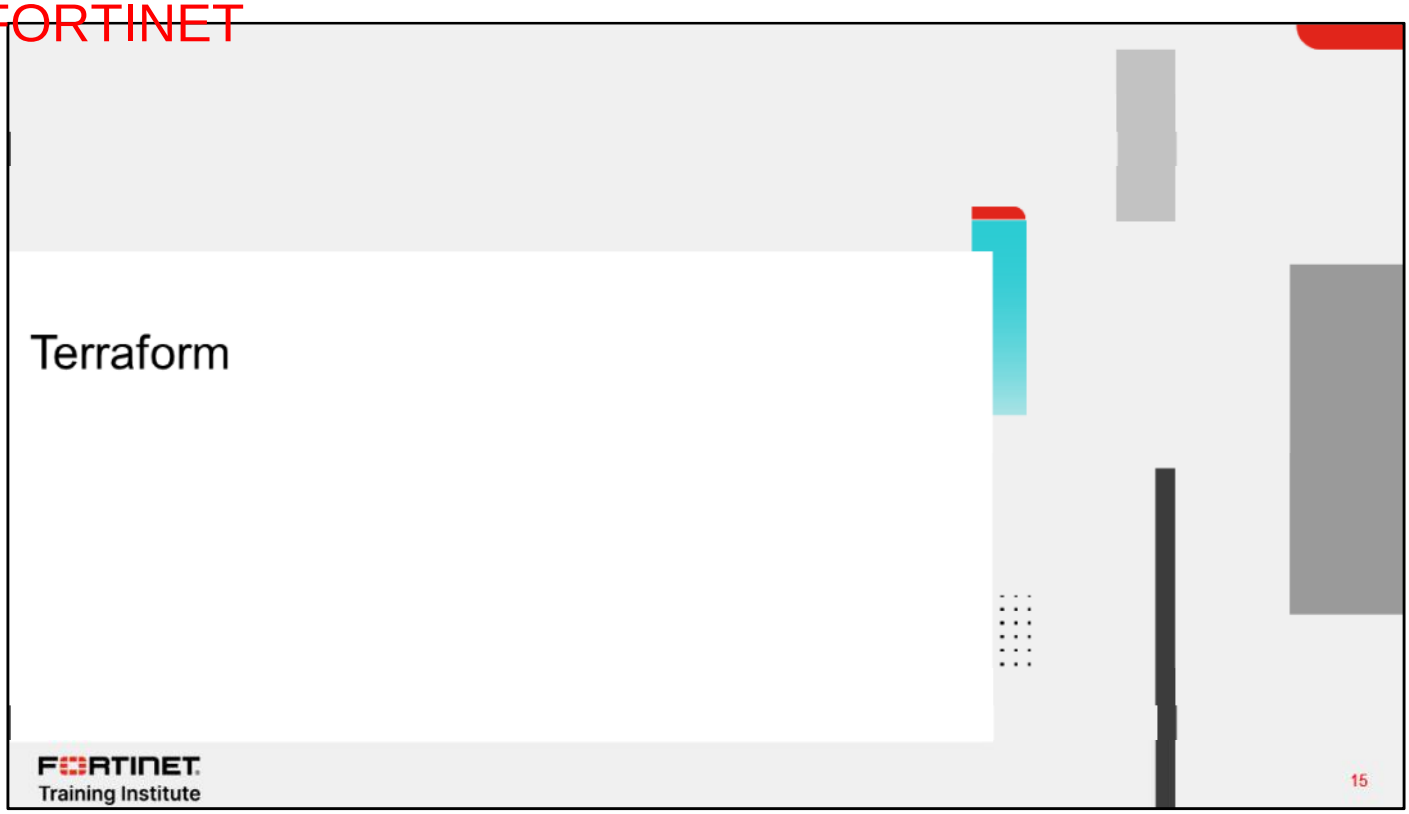
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

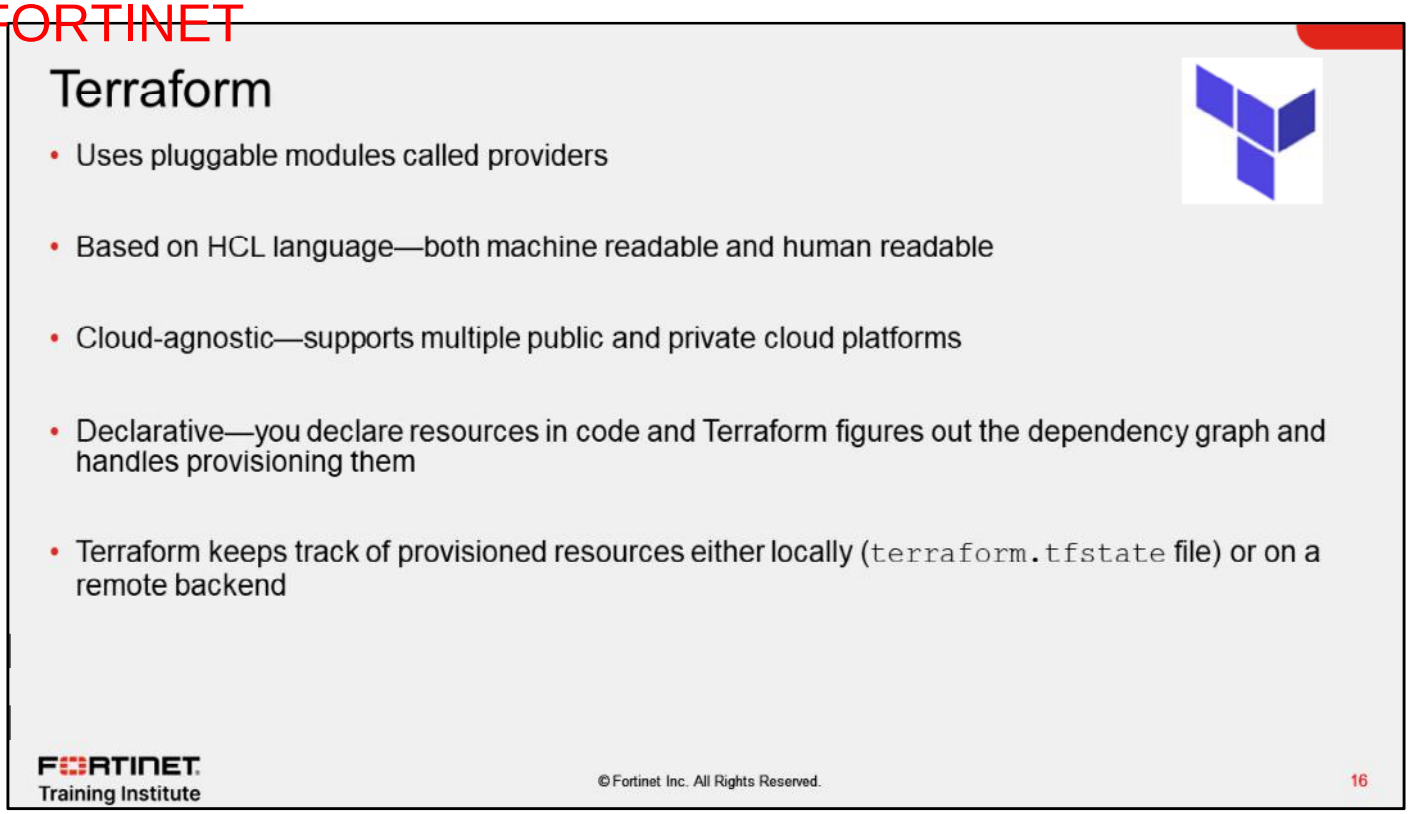
The Google Cloud Deployment Manager allows you to specify all the resources needed for your application in a declarative format using YAML. You can also use Python or Jinja2 templates to create the configuration and allow reuse of common deployment paradigms, such as a load balanced, auto-scaled instance groups.

DO NOT REPRINT
© FORTINET



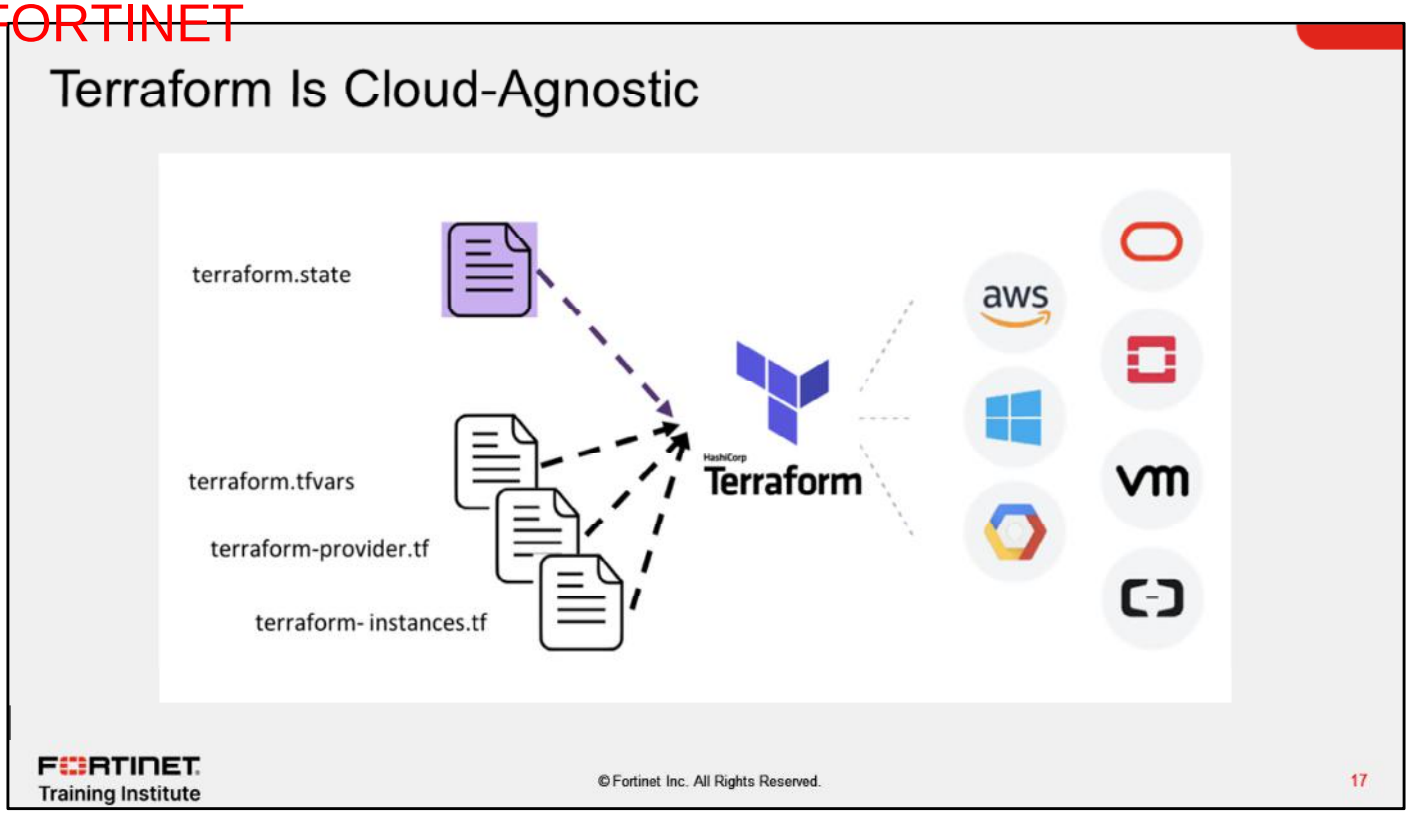
In this section, you will learn about Terraform and its components.

DO NOT REPRINT
© FORTINET



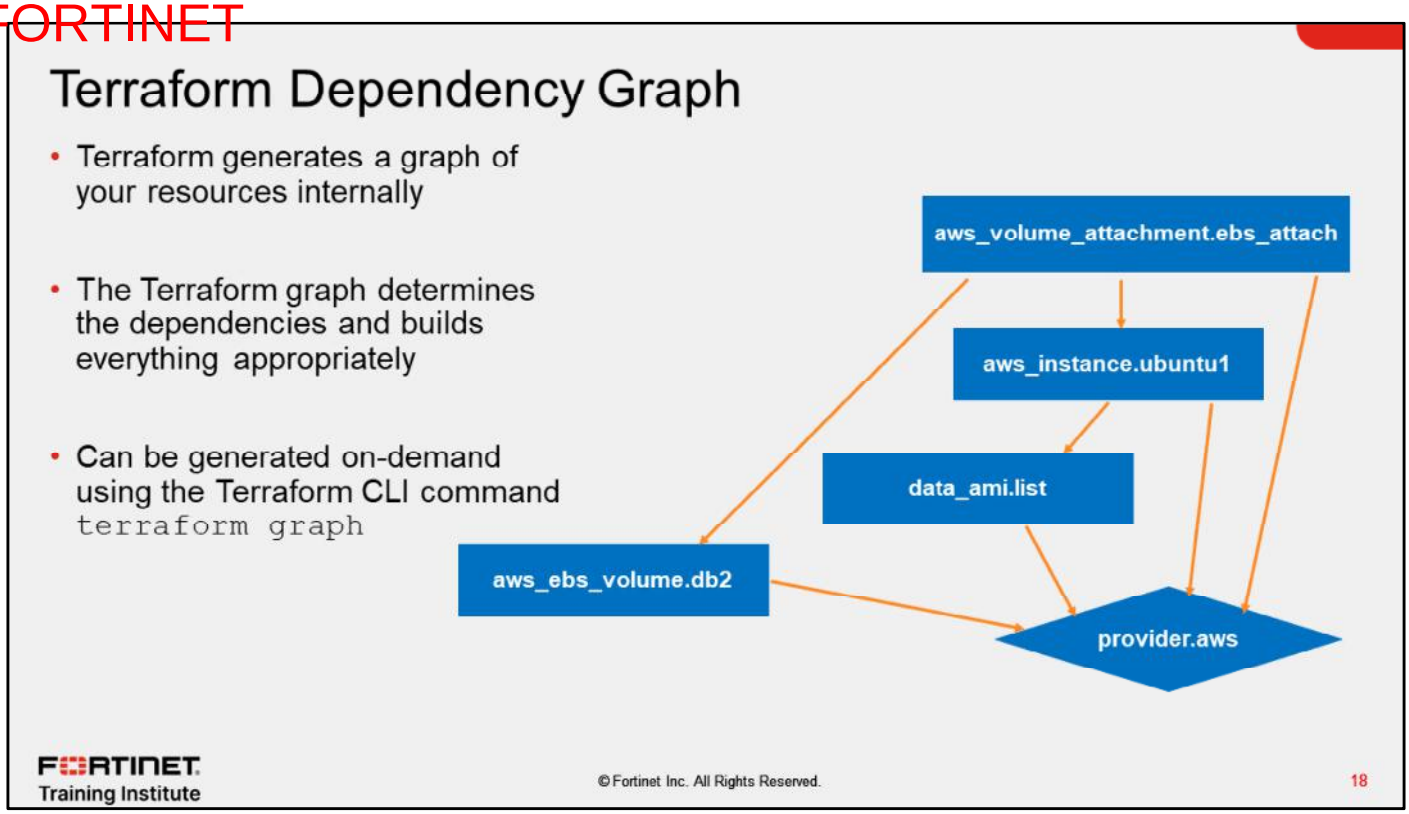
Terraform by HashiCorp is an open-source tool used to manage infrastructure as code. It is used for building, changing, and versioning infrastructure safely and efficiently. It can manage existing and popular service providers, as well as custom in-house solutions. It can use a single (or multiple) text file to describe the environment created and managed by Terraform. The files follow the format of the HashiCorp Configuration Language (HCL).

DO NOT REPRINT
© FORTINET



Terraform is cloud-agnostic, which means it supports and works with multiple cloud providers. The main advantage of Terraform is that it can be used to maintain the same workflow when provisioning resources among cloud and infrastructure providers.

DO NOT REPRINT
© FORTINET



Terraform generates a graph of your resources internally. You can view and generate all the dependencies using the Terraform CLI command `terraform graph`. You can also convert the results to an image and visualize the dependencies.

DO NOT REPRINT
© FORTINET

Terraform Provider

- A provider is responsible for understanding API interactions and exposing resources
- Providers can be of the following types: IaaS, PaaS, virtual, or physical platforms
- Custom plugins can be implemented by third-party vendors outside of HashiCorp
- FortiOS is a new member of the official Terraform providers club!

```
provider "aws" {
 region = "eu-west-1"
 version = "~> 1.19"
 access_key = "${var.aws_access_key}"
 secret_key = "${var.aws_secret_key}"
}
```

Docker	Nutanix	UCloud
Dyn	1&1	UltraDNS
External	OpenStack	Vault
F5 BIG-IP	OpenTelekomCloud	VMware NSX-T
Fastly	OpsGenie	VMware vCloud Director
FlexibleEngine	Oracle Cloud Infrastructure	VMware vRA7
FortiOS	Oracle Cloud Platform	VMware vSphere
GitHub	Oracle Public Cloud	Yandex

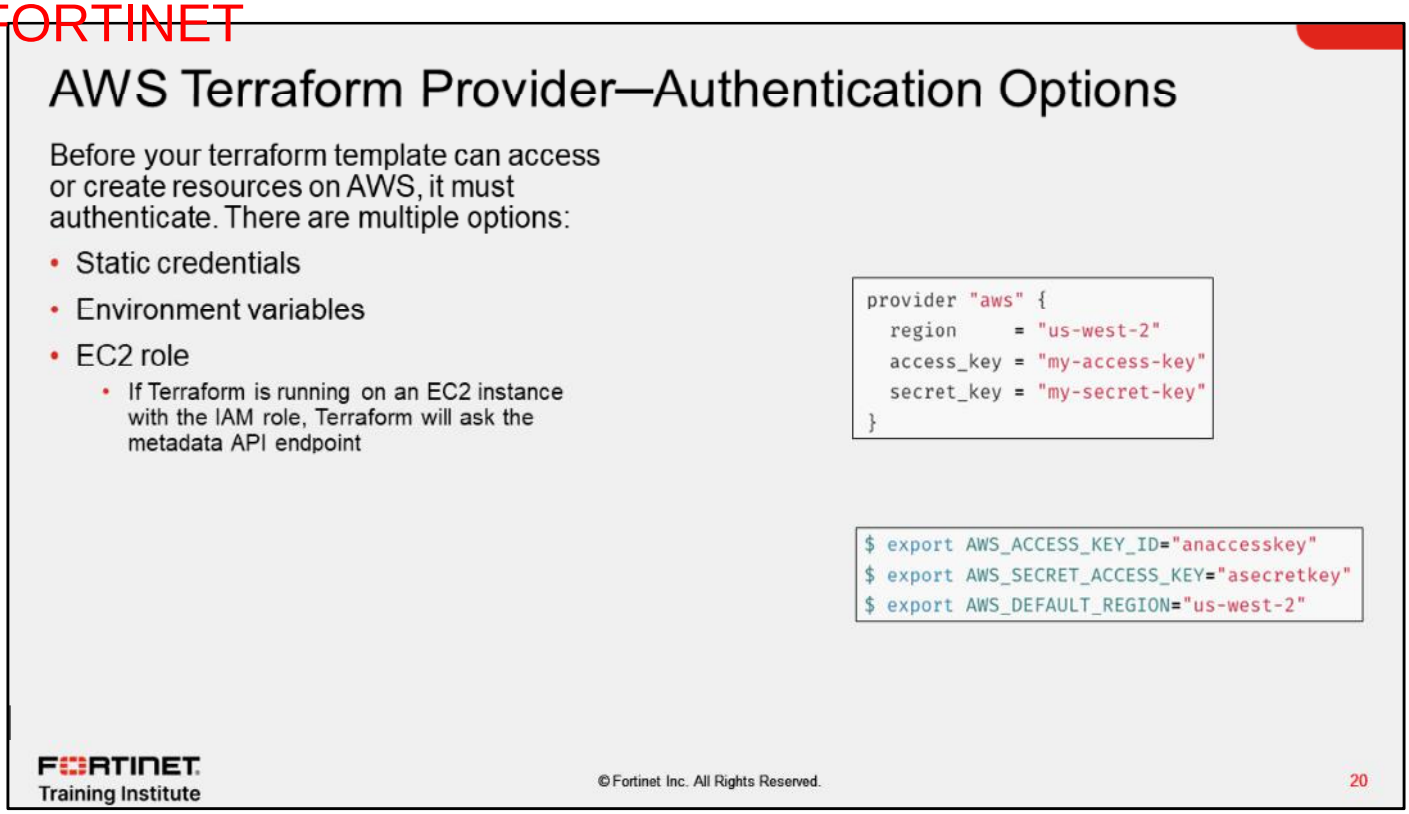
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

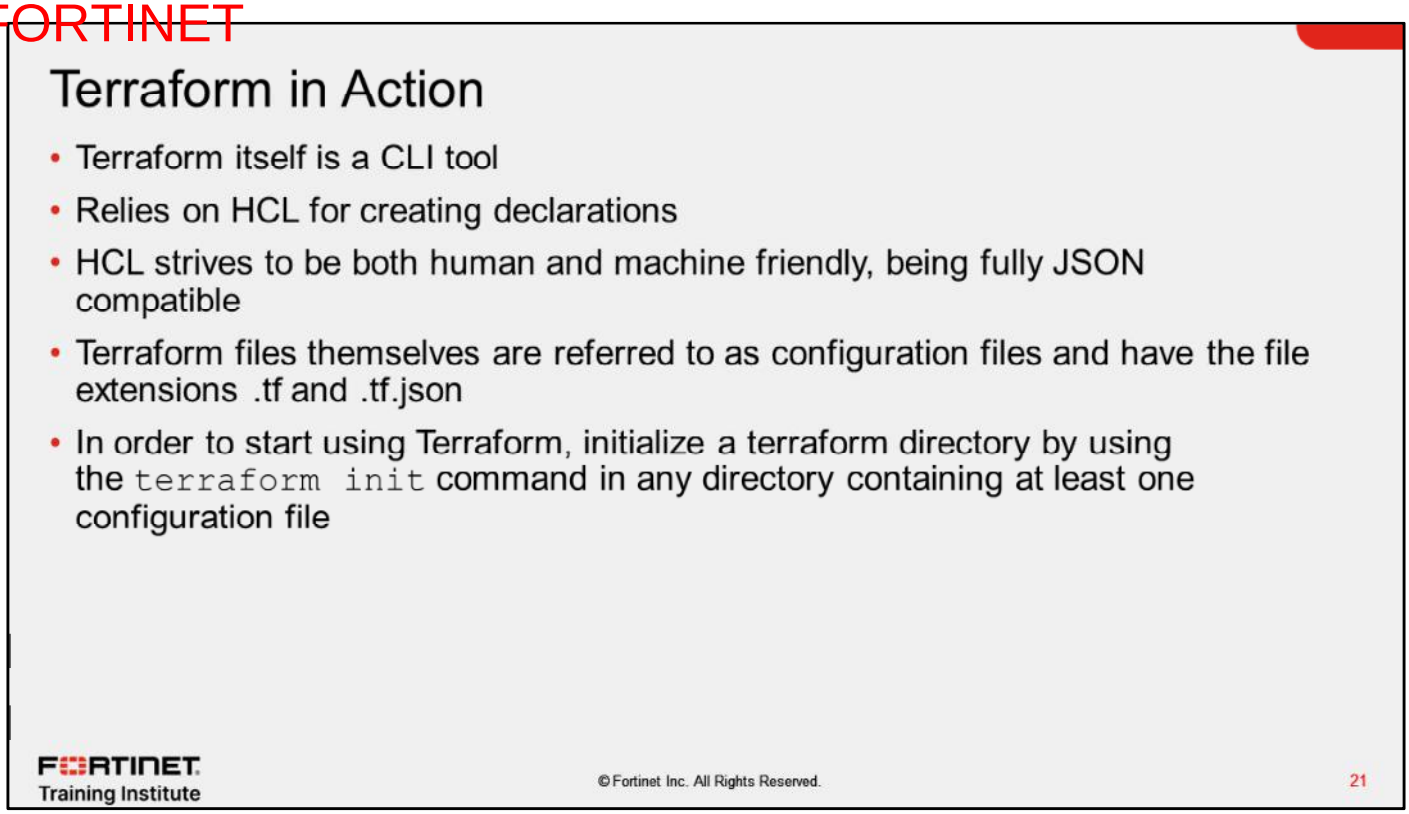
A provider is responsible for understanding API interactions and exposing those resources to Terraform. This means that each provider represents a vendor or product and how Terraform interacts with them.

DO NOT REPRINT
© FORTINET



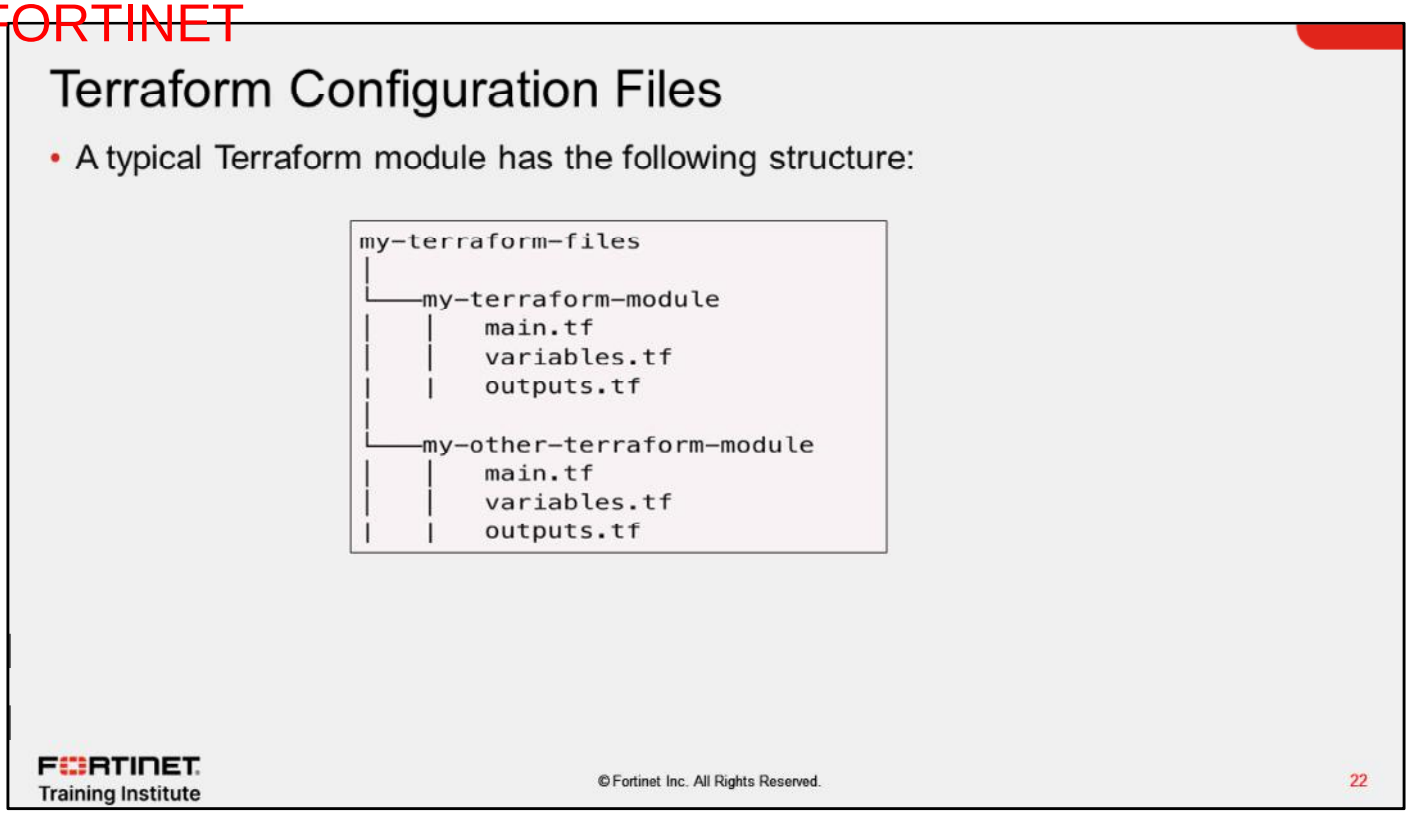
There are three options for authentication. Terraform must authenticate on AWS to access or create resources using static credentials, environment variables, or the EC2 role.

DO NOT REPRINT
© FORTINET



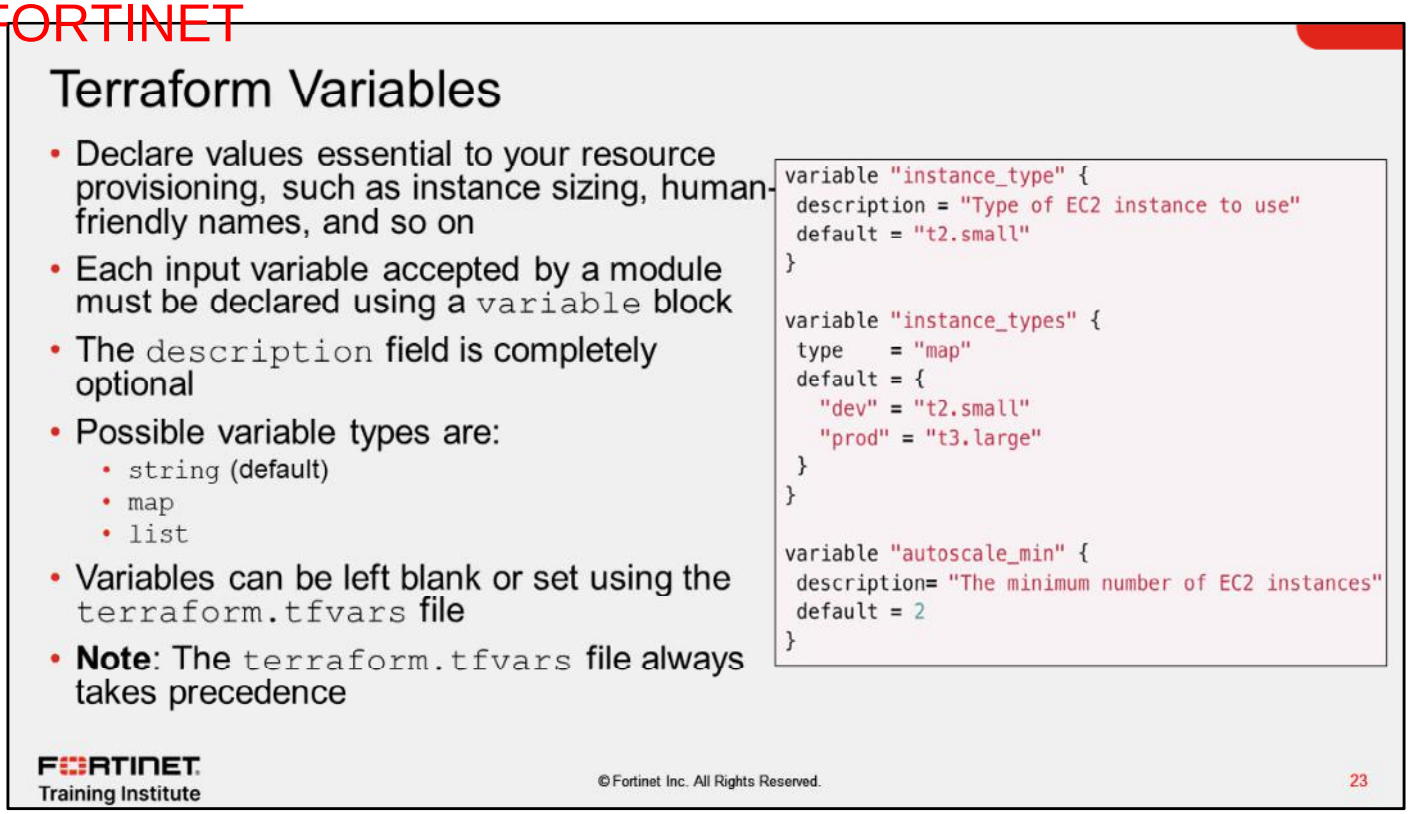
Terraform files themselves are referred to as configuration files and have the file extensions `.tf` and `.tf.json`. With the configuration contained in the file(s), Terraform can plan (dry run), apply (deploy), or destroy (delete) its controlled environment. To start using Terraform, initialize a Terraform directory by using the `terraform init` command in any directory containing at least one configuration file.

DO NOT REPRINT
© FORTINET



A typical Terraform module has `main.tf`, `variables.tf`, and `outputs.tf` files.

DO NOT REPRINT
© FORTINET



The Terraform variable file declares the values that are essential to your resource provisioning, such as instance sizing, human-friendly names, and so on. You can leave the variables blank or set then through the `terraform.tfvars` file. It is important to understand that the `terraform.tfvars` file always takes precedence.

DO NOT REPRINT
© FORTINET

Terraform Outputs

- Output values are the return values of a Terraform module
- Each output value exported by a module must be declared using an `output` block
- Output values are a way to expose some of the attributes exported by Terraform resources to the user of a module
- A root module can use outputs to print values in the CLI output after running `terraform apply`
- You can use the `sensitive` argument to suppress values in CLI output

```
output "vpc_id" {
  value = "${aws_vpc.default.id}"
}

output "subnet_private_1" {
  value = "${aws_subnet.private_1.id}"
}

output "subnet_private_2" {
  value = "${aws_subnet.private_2.id}"
}

output "subnet_private_3" {
  value = "${aws_subnet.private_3.id}"
}
```

```
output "instance_ip_addr" {
  value       = aws_instance.server.private_ip
  description = "The private IP address of the main server instance."
}
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

Terraform output values are the return values of a Terraform module. The output values help you see the end values of the project. For example, when deploying FortiGate in the cloud, the output file can show the details of the public IP address and credentials of the FortiGate device.

DO NOT REPRINT
© FORTINET

Terraform Resources

- Resources are the most essential components of configuration files
- Allows users to declare the type of resource and all of the resource-specific settings
- After the `resource` keyword, the type and a local identifier as string are specified
- Terraform keeps track of all resources in the `.tfstate` file
- Can provide explicit dependencies to resources where necessary, instructing Terraform to wait until the dependent resources exist by specifying a *depends_on* field

```
resource "aws_instance" "myapp_ec2_instance" {
 ami               = "ami-21f78e11"
 availability_zone = "${var.availability_zone}"
 instance_type     = "${var.instance_type}"

 tags {
   Name = "myapp-EC2-instance"
 }
}

resource "aws_ebs_volume" "myapp_ebs_volume" {
 availability_zone = "${var.availability_zone}"
 size              = 1

  tags {
   Name = "myapp-EBS-volume"
 }
}
```

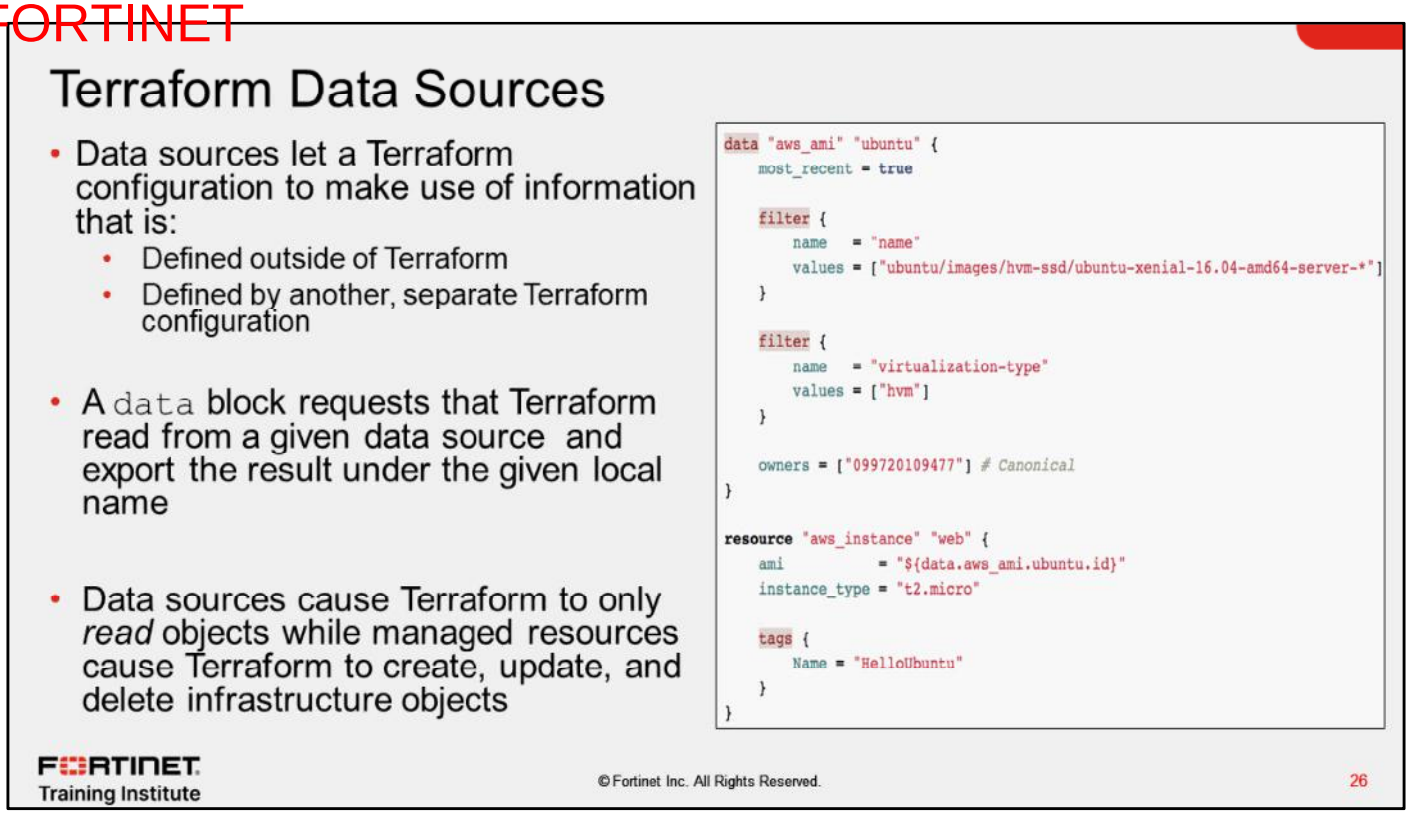
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

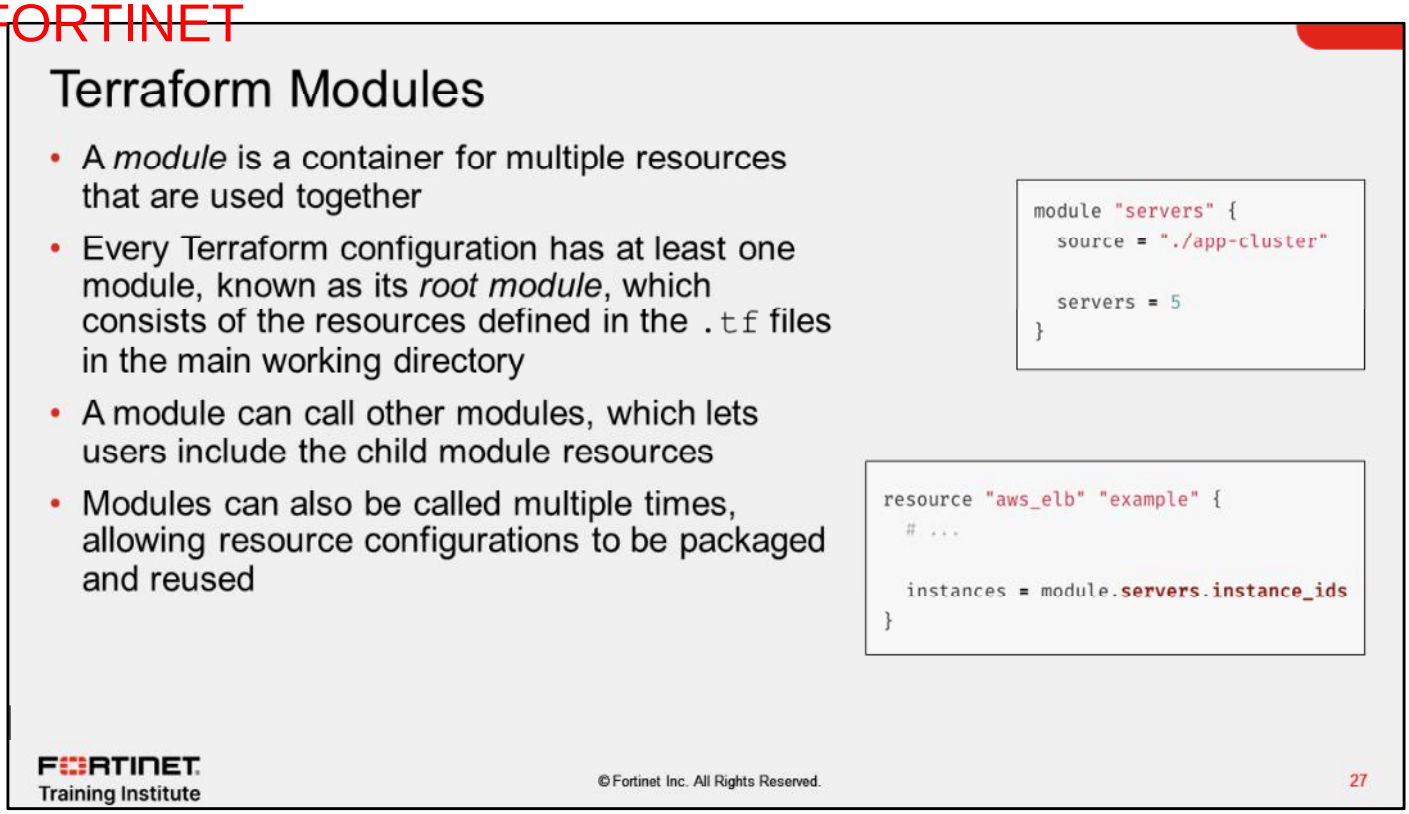
This slide shows that resources are the most essential components of configuration files. Terraform resources allow user to define type and all of the resource-specific settings.

DO NOT REPRINT
© FORTINET



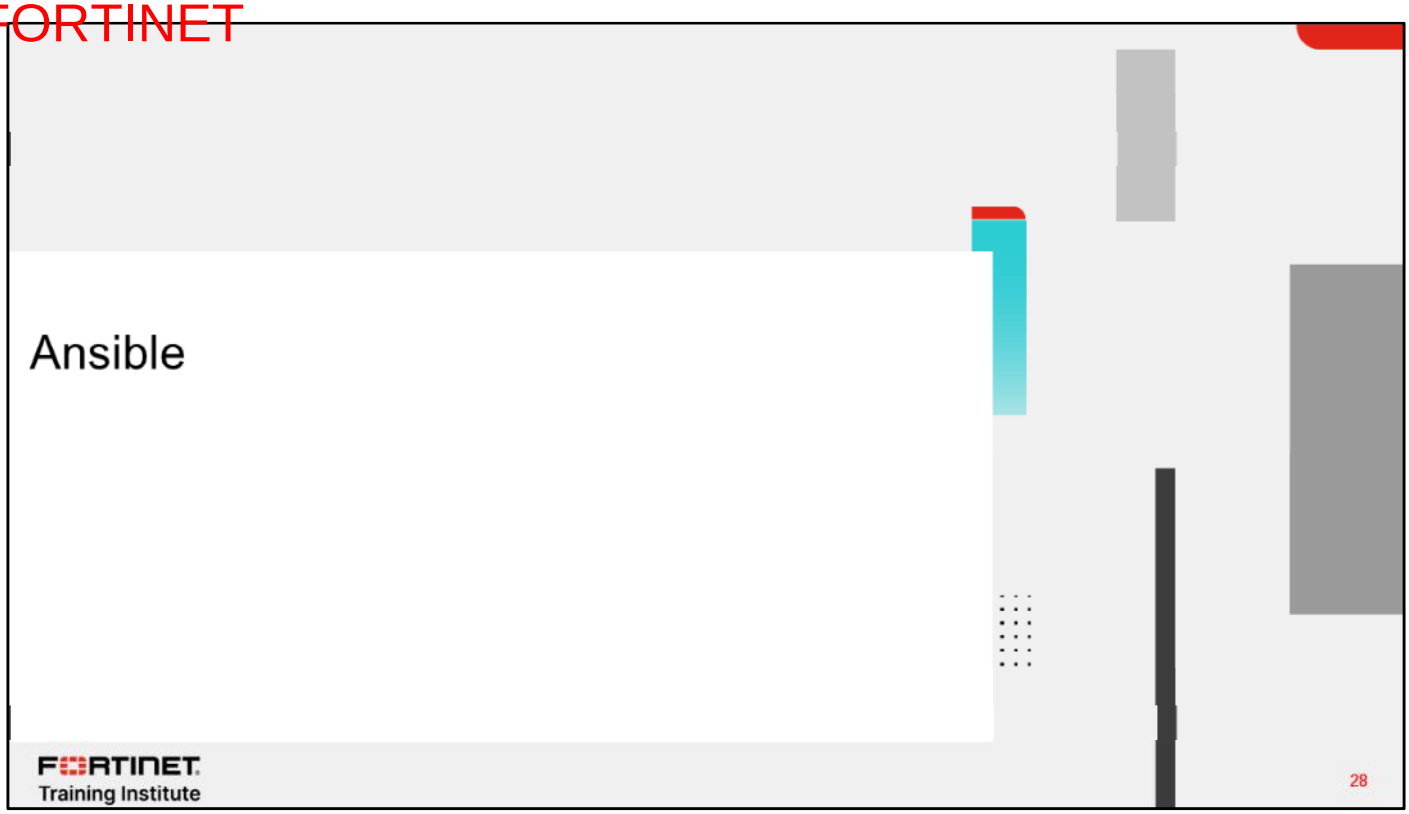
Terraform data sources let a Terraform configuration make use of information that is defined outside of Terraform or by another, separate, Terraform configuration. How it works is that a `data` block requests that Terraform read from a given data source, `aws_ami`, and export the result under the given local name, `ubuntu`.

DO NOT REPRINT
© FORTINET



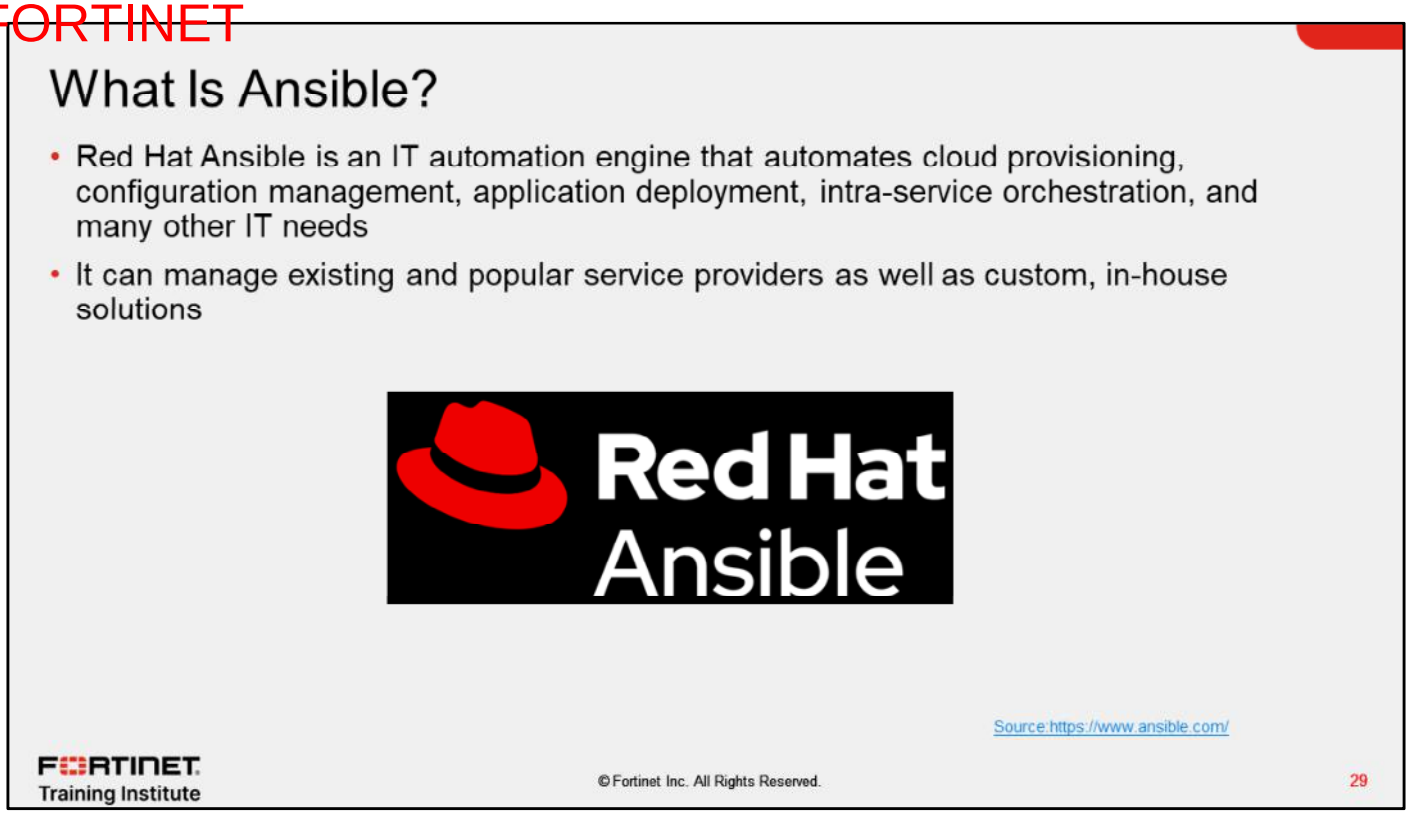
A *module* is a container for multiple resources that are used together. Every Terraform configuration has at least one module, known as its *root module*, which consists of the resources defined in the `.tf` files in the main working directory. A module can call other modules, which lets users include the child module resources. Modules can also be called multiple times, allowing resource configurations to be packaged and reused.

DO NOT REPRINT
© FORTINET



In this section, you will learn about Ansible and how it can be a useful tool to configure FortiOS.

DO NOT REPRINT
© FORTINET



What is Ansible? Ansible is a suite of software tools that enables IaC to provide automation and orchestration. For example, customers can use Ansible to execute repetitive tasks, such as deploying a new application servers and backing up servers on the network. In this lesson, you will learn more about how Fortinet is integrated with Ansible.

DO NOT REPRINT
© FORTINET

What Is Ansible Used For?

- It is used to manage machines in a central and automated way
- By default, Ansible represents what machines it manages using a very simple file that puts all of your managed machines in groups of your own choosing
- It uses no agents and no additional custom security infrastructure
- It uses YAML, in the form of Ansible playbooks, letting you describe your automation jobs in a way that approaches plain English

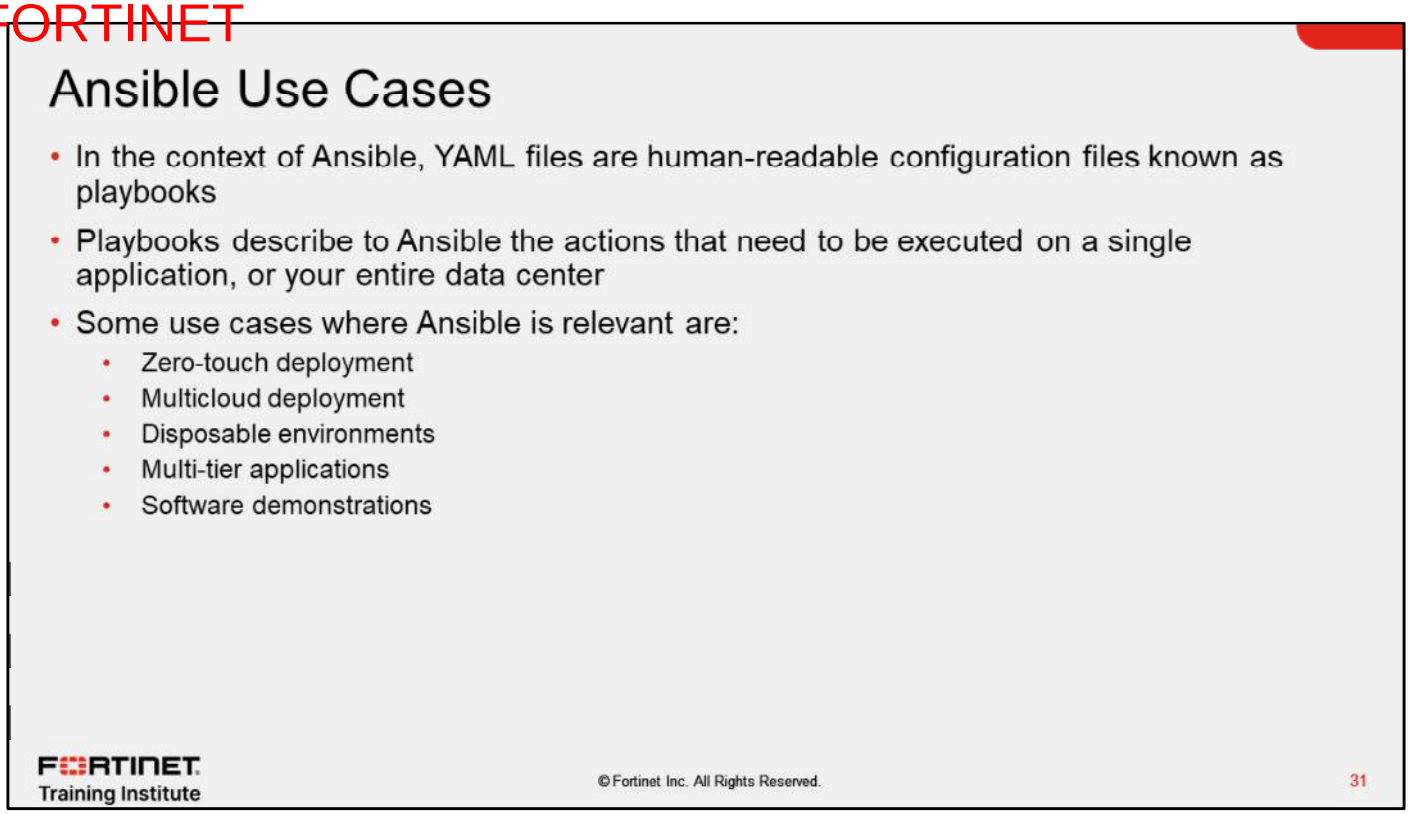
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

Ansible helps to automate repetitive tasks with simplicity. Ansible uses YAML, in the form of playbooks, making it possible for you to describe your automation jobs in a way that approaches plain English. You can see and read all the files that contain all the tasks. You can use Ansible to configure FortiGate devices and FortiManager.

DO NOT REPRINT
© FORTINET



Now you will learn about some use cases for Ansible. Ansible is used mainly in multicloud deployments—disposable environments where you must deploy resources often and quickly. For example, during a popular sports event, customers may need to deploy more servers with more processing power to cater to the demand, and then retire them quickly if they are not needed. Also, during peak sales times, for example, during the Christmas season, websites must be able to handle more traffic. Customers can use Ansible to deploy more resources as demand increases. Ansible is also useful when deploying zero touch in multiple locations with minimal effort.

DO NOT REPRINT
© FORTINET

Ansible Modules

- Ansible is used to create, manage, and update infrastructure resources, such as physical machines, VMs, network switches, containers, and more
- *Almost any infrastructure type can be configured using Ansible*
- A *module* is responsible for understanding interactions and exposing those resources to Ansible
  - This means that each vendor or product can have one or more modules used by Ansible to interact with their products

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

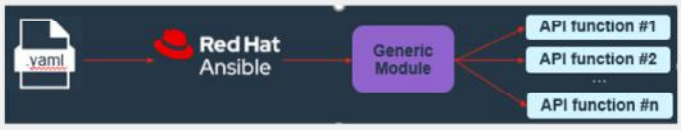
An Ansible module is a component inside Ansible that creates integration between the Ansible core and devices that are being managed by Ansible. In the case of FortiGate and FortiManager configuration changes, Ansible uses APIs that are available for FortiGate and FortiManager. For many other devices, Ansible uses SSH to reach devices to make configuration changes. A *module* is responsible for understanding interactions and exposing many resources to Ansible. Each vendor or product can interact with one or more modules used by Ansible.

DO NOT REPRINT
© FORTINET

Ansible Modules (Contd)

- Specific or generic?
- Specific modules:
  - Dedicated function
  - Used to execute a single known function on the target device, for example, a module that will execute a call to a specific API to change a route

- Generic modules:
  - Generic function
  - Used to execute any API call on the target system
  - Can be considered an API proxy or packager
  - Not supported by Ansible



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

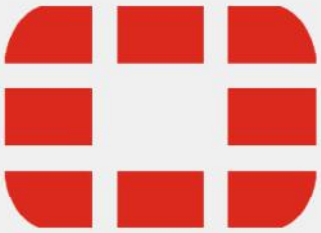
33

There are different types of Ansible modules. Specific modules can perform only a single function, for example, a module that is able to connect FortiOS using a FortiOS API and change the route entry on FortiGate. Generic modules can perform many functions and execute any API call on the target system. The generic module is more complex and you must understand how each function works. Ansible does not support generic modules. Ansible prefers to work with specific modules.

DO NOT REPRINT
© FORTINET

Fortinet Modules in Ansible

- Who develops the Fortinet modules for Ansible?
- The Fortinet development team is responsible for the provider code
  - FortiOS:
    - https://galaxy.ansible.com/fortinet/fortios
    - https://github.com/fortinet-ansible-dev/ansible-galaxy-fortios-collection
  - FortiManager:
    - https://galaxy.ansible.com/fortinet/fortimanager
    - https://github.com/fortinet-ansible-dev/ansible-galaxy-fortimanager-collection/tree/galaxy/1.0.2



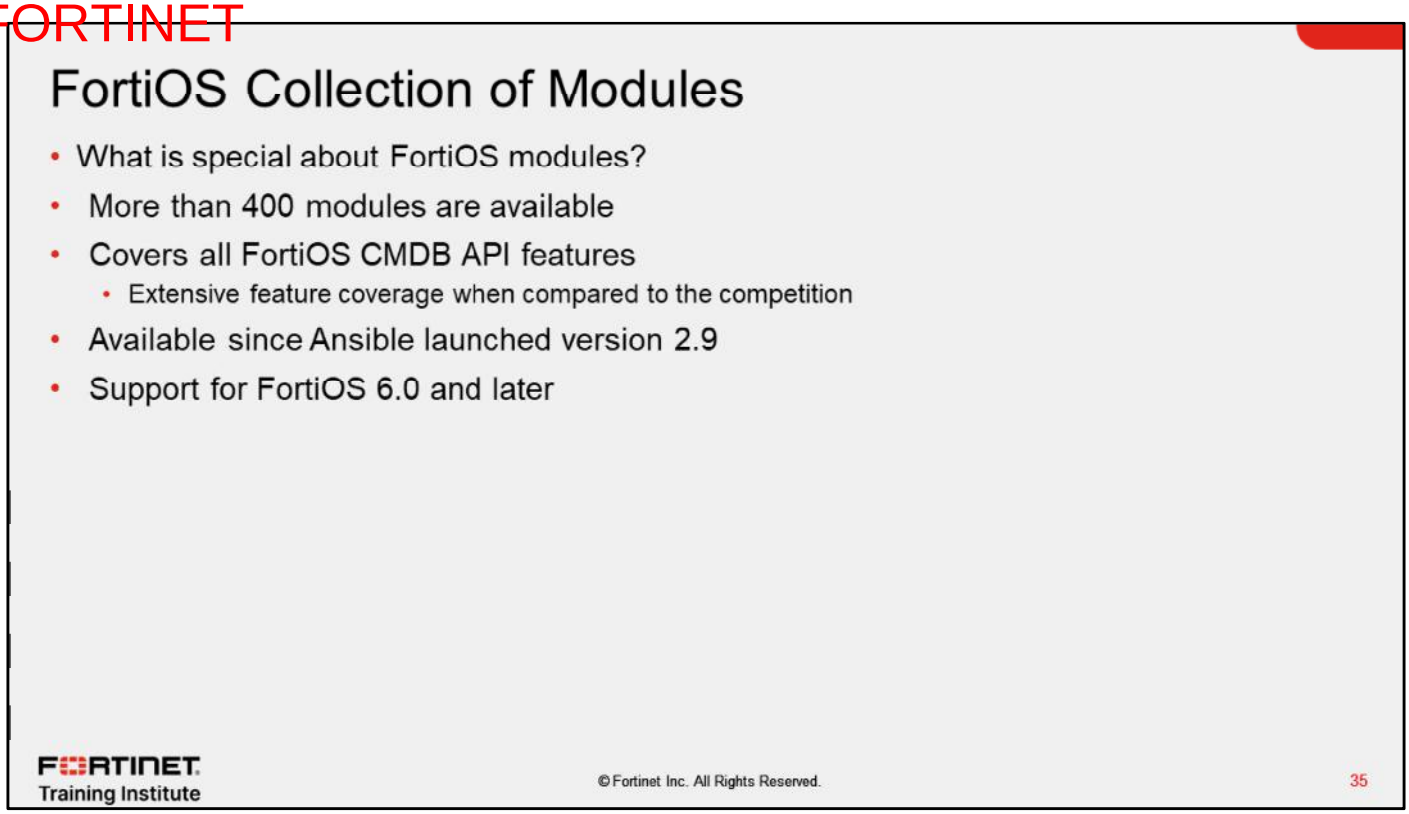
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

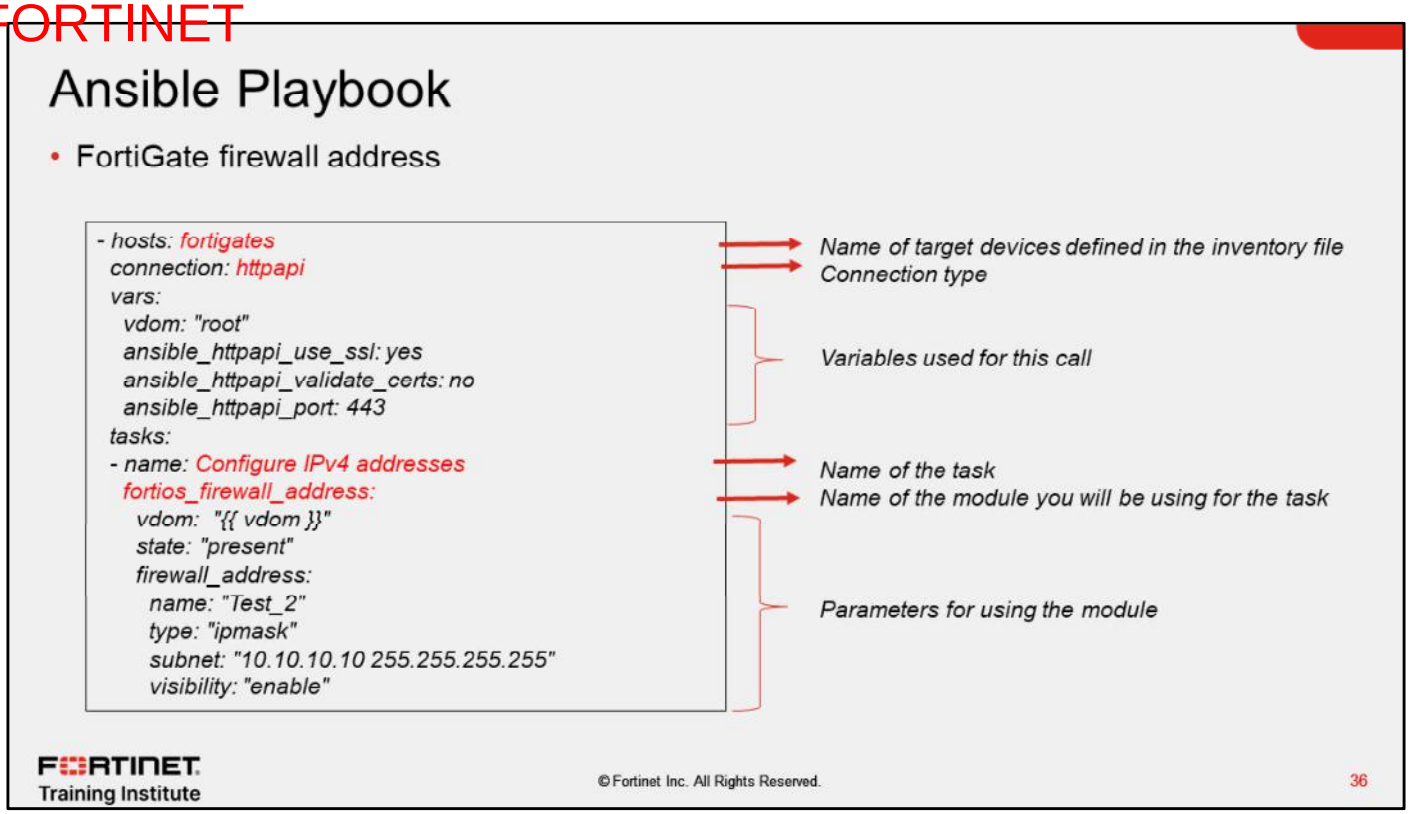
You can get all the FortiOS and FortiManager collections developed by Fortinet developers from the sites shown on this slide. The links provide all the information you need.

DO NOT REPRINT
© FORTINET



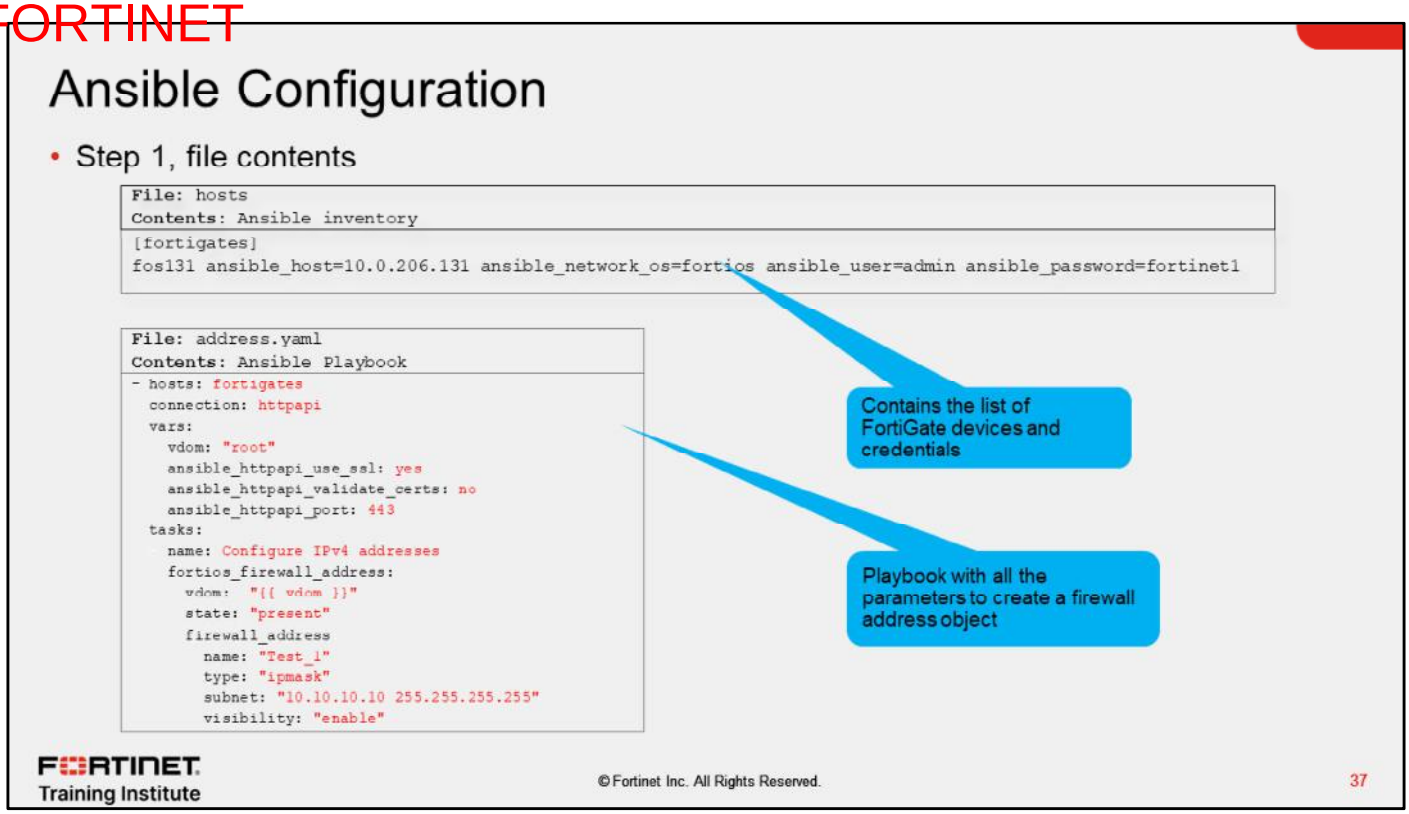
Ansible does not support generic modules, so Fortinet developers developed specific modules for FortiOS. There are more than 400 modules available, which cover all the FortiOS CMDB API features for FortiOS 6.0 and later.

DO NOT REPRINT
© FORTINET



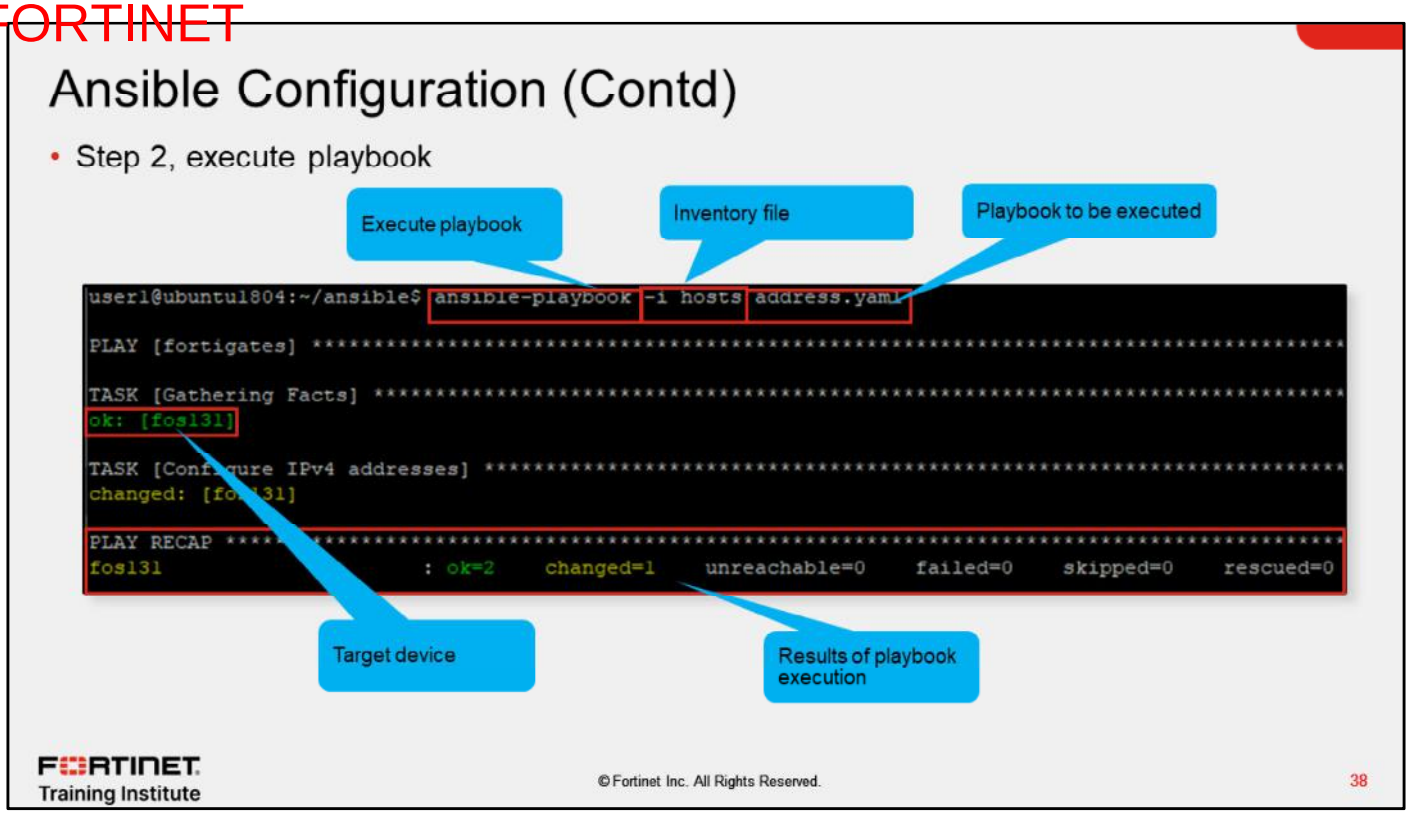
This slide shows an example of a playbook file. A playbook is a text file that contains hosts, connection type, variables, tasks, the name of the module, and several parameters for the module. As per the example shown on the slide, Ansible uses HTTPAPI to connect to FortiOS, but for other devices, such as servers, Ansible uses an SSH connection. There are more modules available in the *Ansible Galaxy FortiOS* documentation. You can use the documents in the Fortinet Developer Network (FNDN), GitHub, and Ansible for more detailed instructions.

DO NOT REPRINT
© FORTINET



This slide shows the two main files required to execute Ansible. The `hosts` file contains the Ansible inventory, which contains information about the target device. The `address.yaml` file contains all the playbook contents.

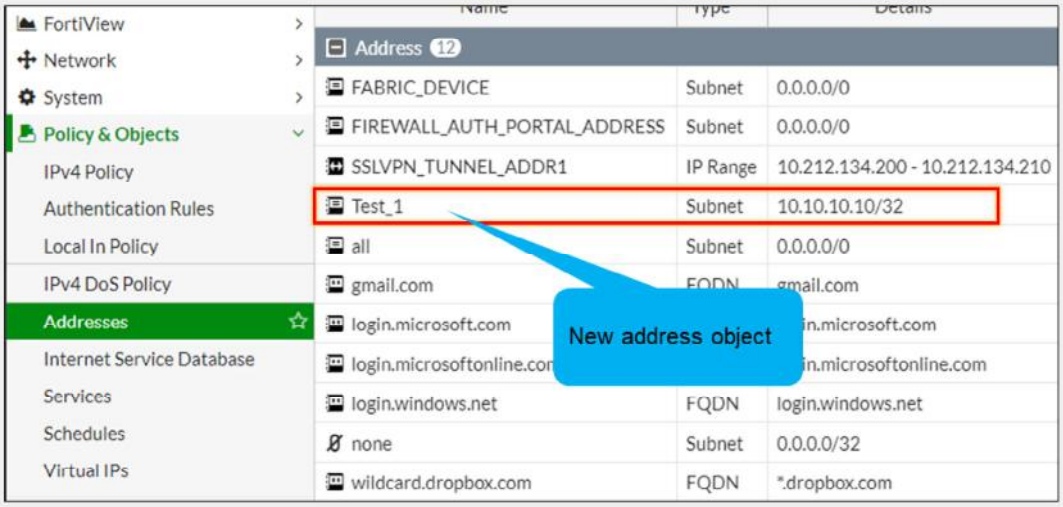
DO NOT REPRINT
© FORTINET



In order to execute the playbook, you must enter the name of the inventory file and playbook you want to execute on the Linux CLI. After the playbook executes successfully, you will see the results.

DO NOT REPRINT
© FORTINET

Ansible Configuration (Contd)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

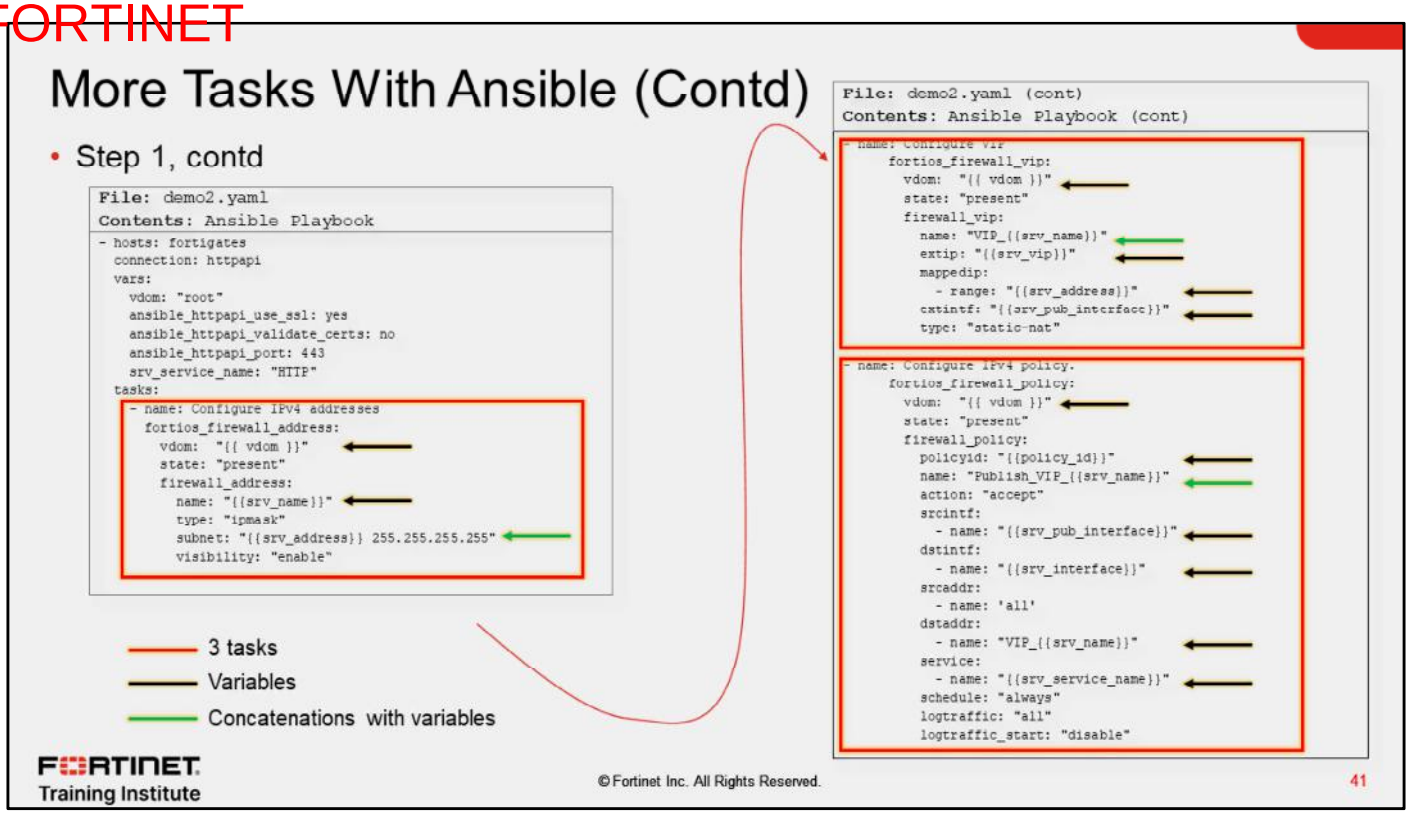
39

The firewall address object is created on the target FortiGate device within a few seconds.

DO NOT REPRINT
© FORTINET

This slide shows an example of creating more tasks using Anisble. The host inventory file is similar to the previous example containing targeted device details.

DO NOT REPRINT
© FORTINET



This slide shows an example of a playbook with multiple tasks and variables. This playbook also uses concatenating text, which are other parameters with variables. The goal is to publish a web server by creating an IPv4 address, virtual IP (VIP), and firewall policy.

DO NOT REPRINT
© FORTINET

More Tasks With Ansible (Contd)

- Step 2, execute playbook

```
ansible-playbook -i hosts demo2.yaml --extra-vars "srv name=WebSrv12 srv
address=12.12.12.12 srv vip=50.50.50.50 srv pub interface=port1 policy id=100 srv
interface=port2"
```

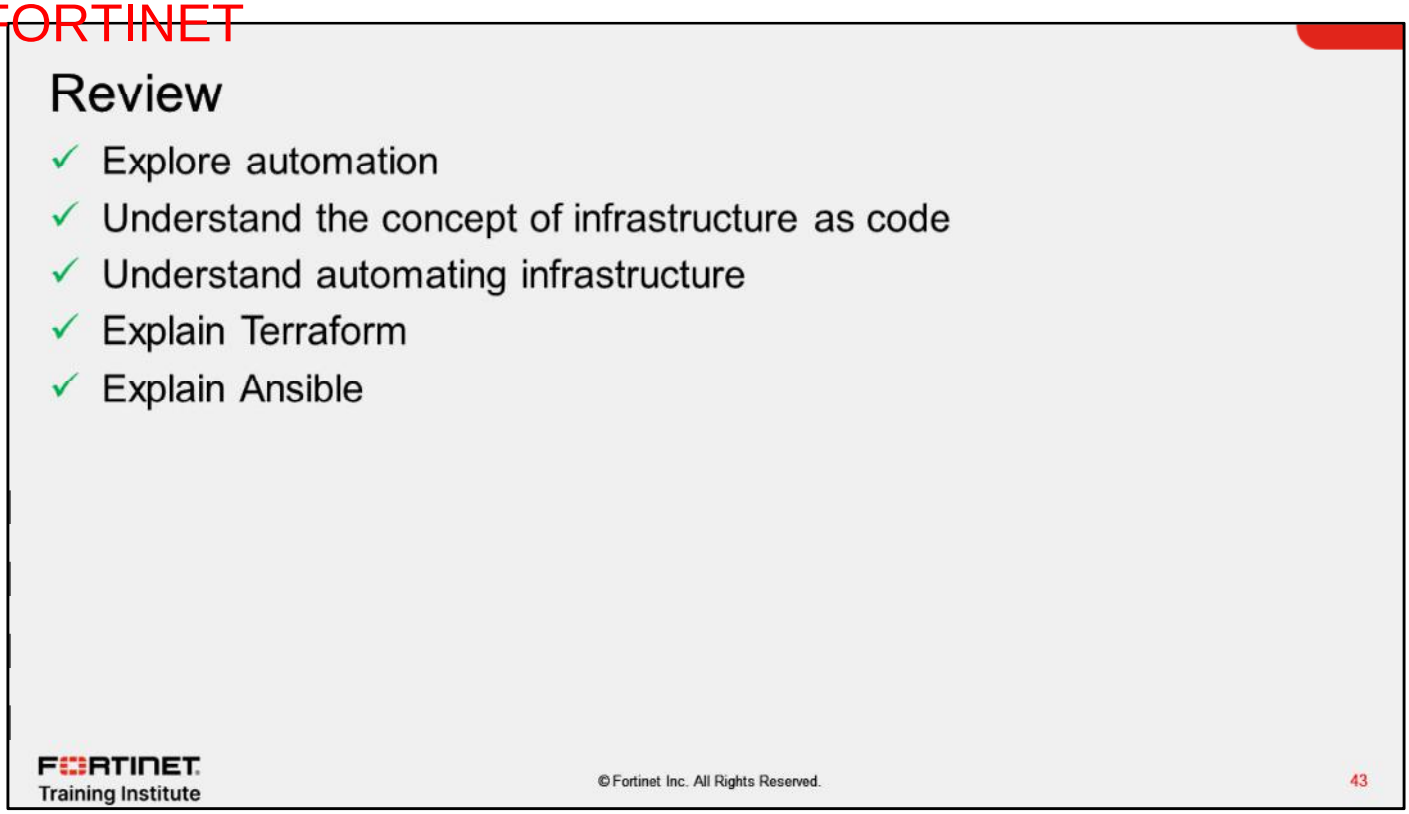
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

42

The execution of this playbook is different from the previous playbook. Besides providing the inventory file and the playbook, there are extra variables needed. This is one of several ways you can provide the variables to the Ansible playbook.

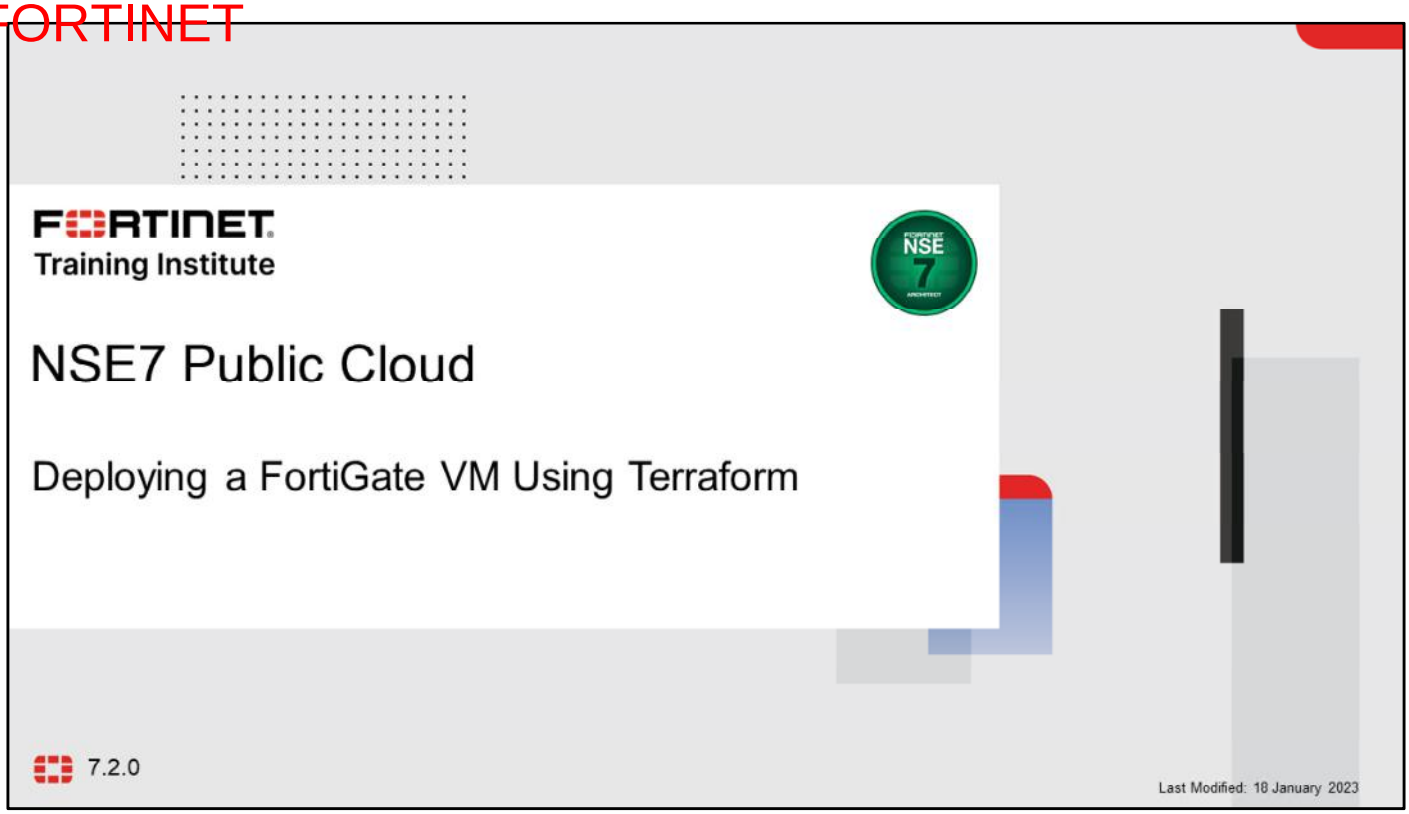
DO NOT REPRINT
© FORTINET



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

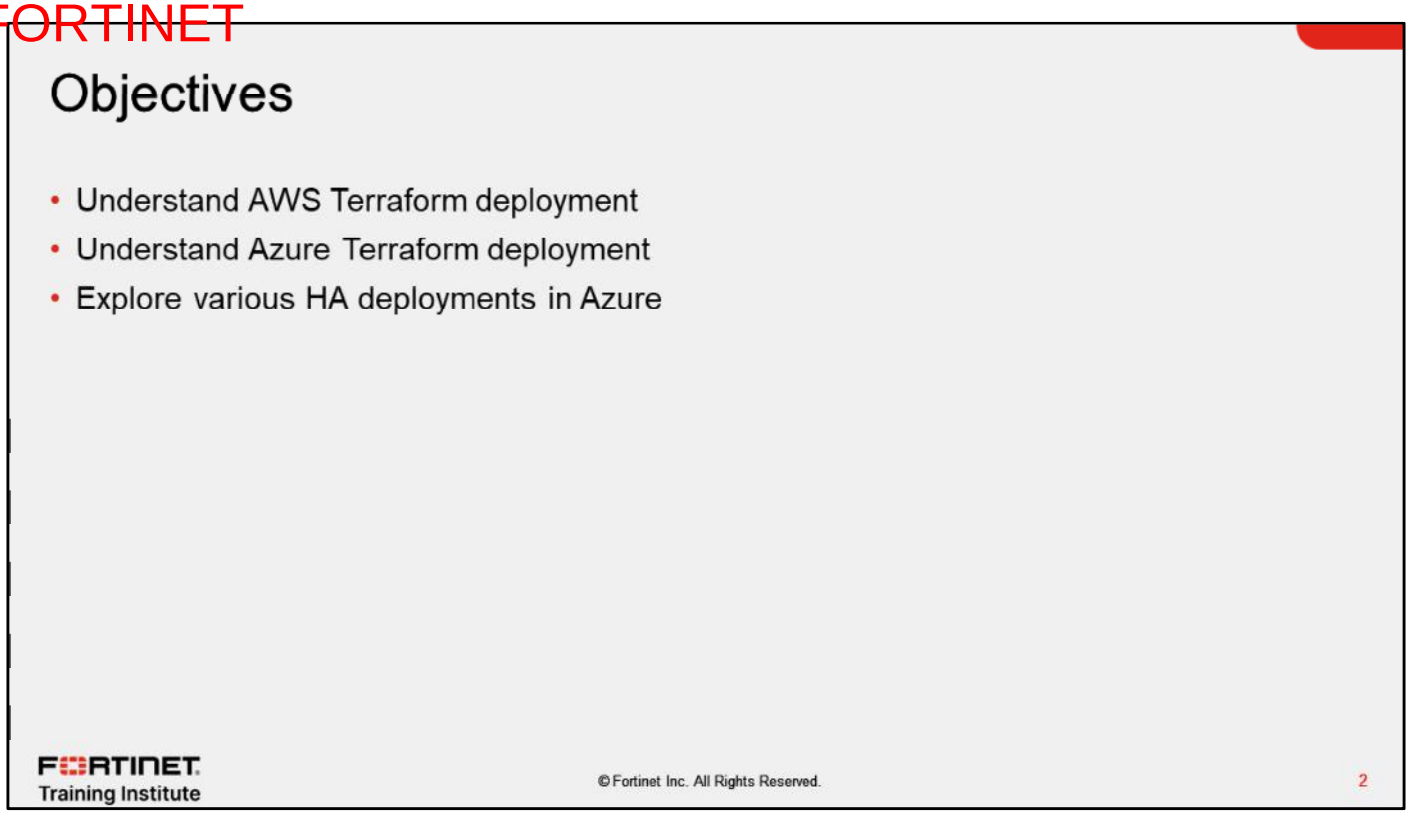
By mastering the objectives covered in this lesson, you learned about automation.

DO NOT REPRINT
© FORTINET



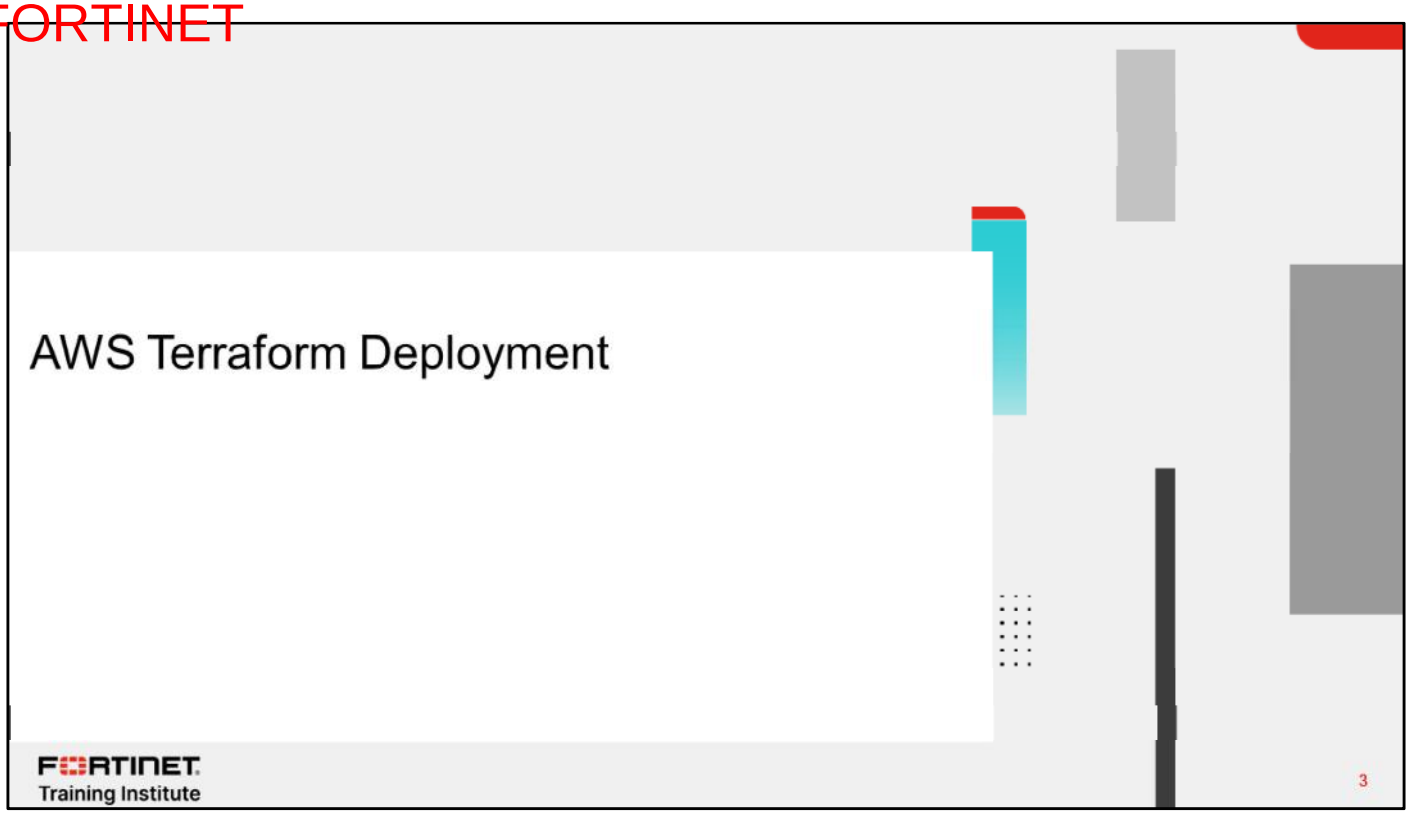
In this lesson, you will learn about deploying a FortiGate VM using Terraform.

DO NOT REPRINT
© FORTINET



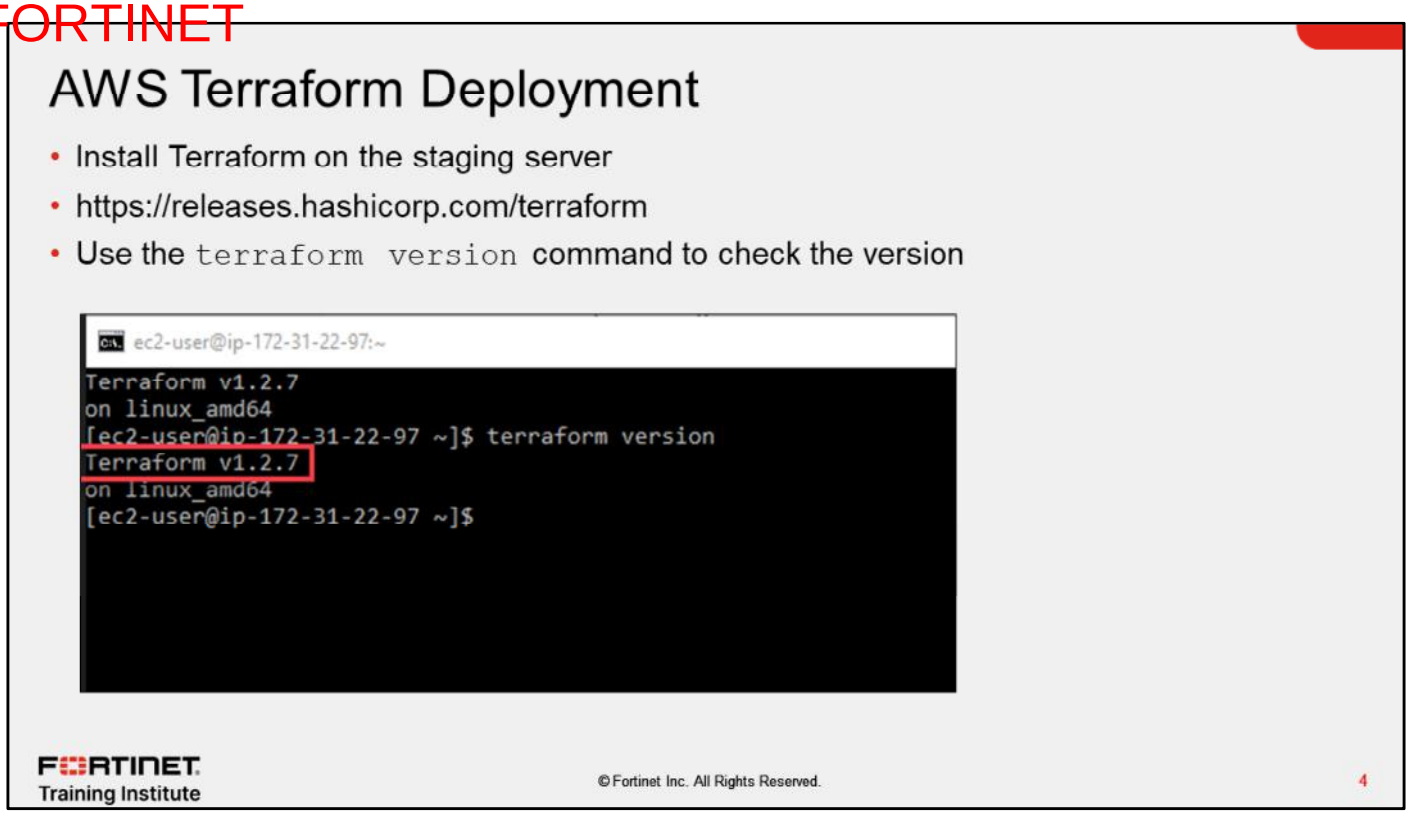
After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



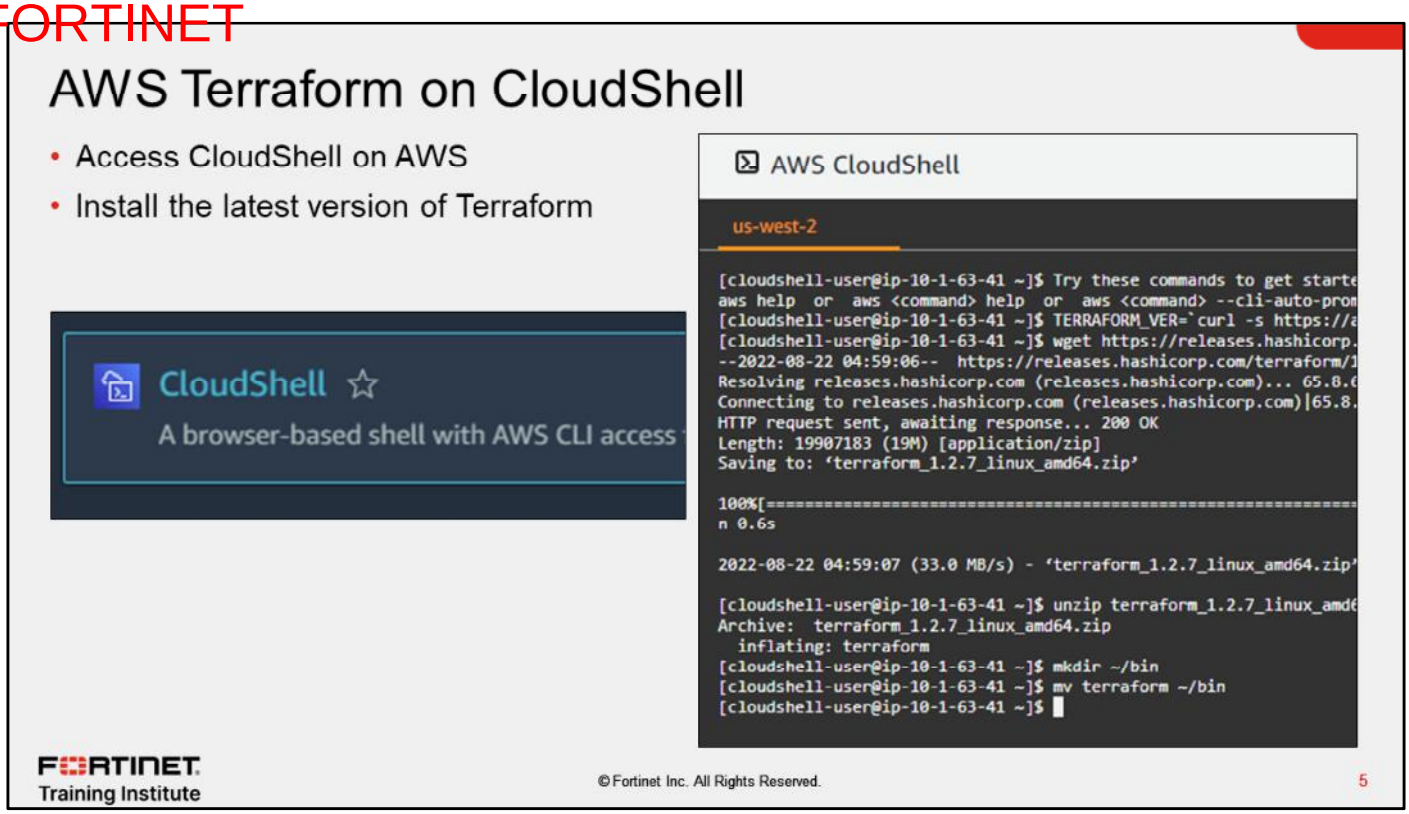
In this section, you will learn about the public cloud through a quick overview.

DO NOT REPRINT
© FORTINET



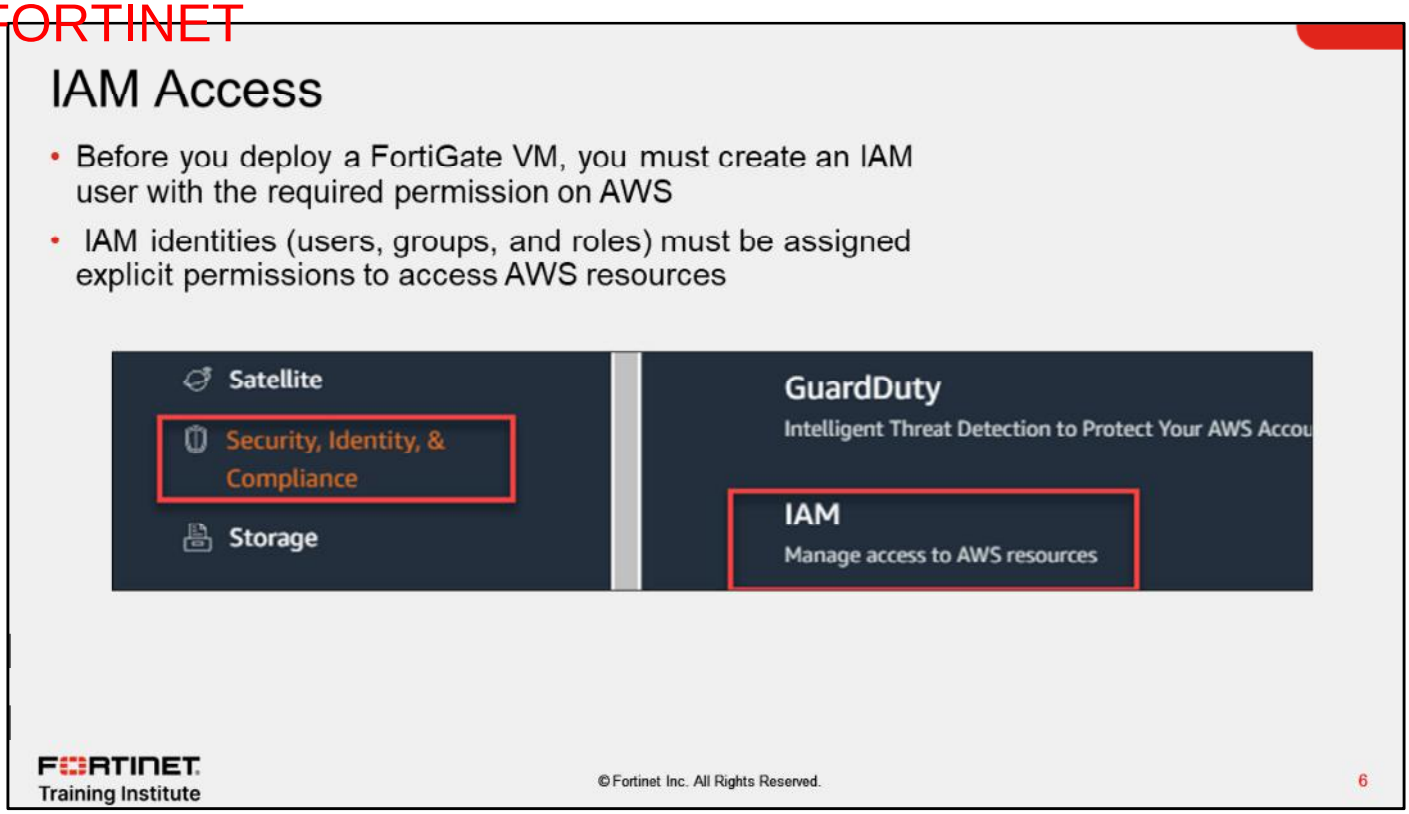
One advantage of using the staging server to perform your Terraform work is that you do not need to install products onto your local machine. You can perform many tasks without affecting the production environment. After you install Terraform on the staging server, you can run the `terraform version command` to check which version of Terraform is installed.

DO NOT REPRINT
© FORTINET



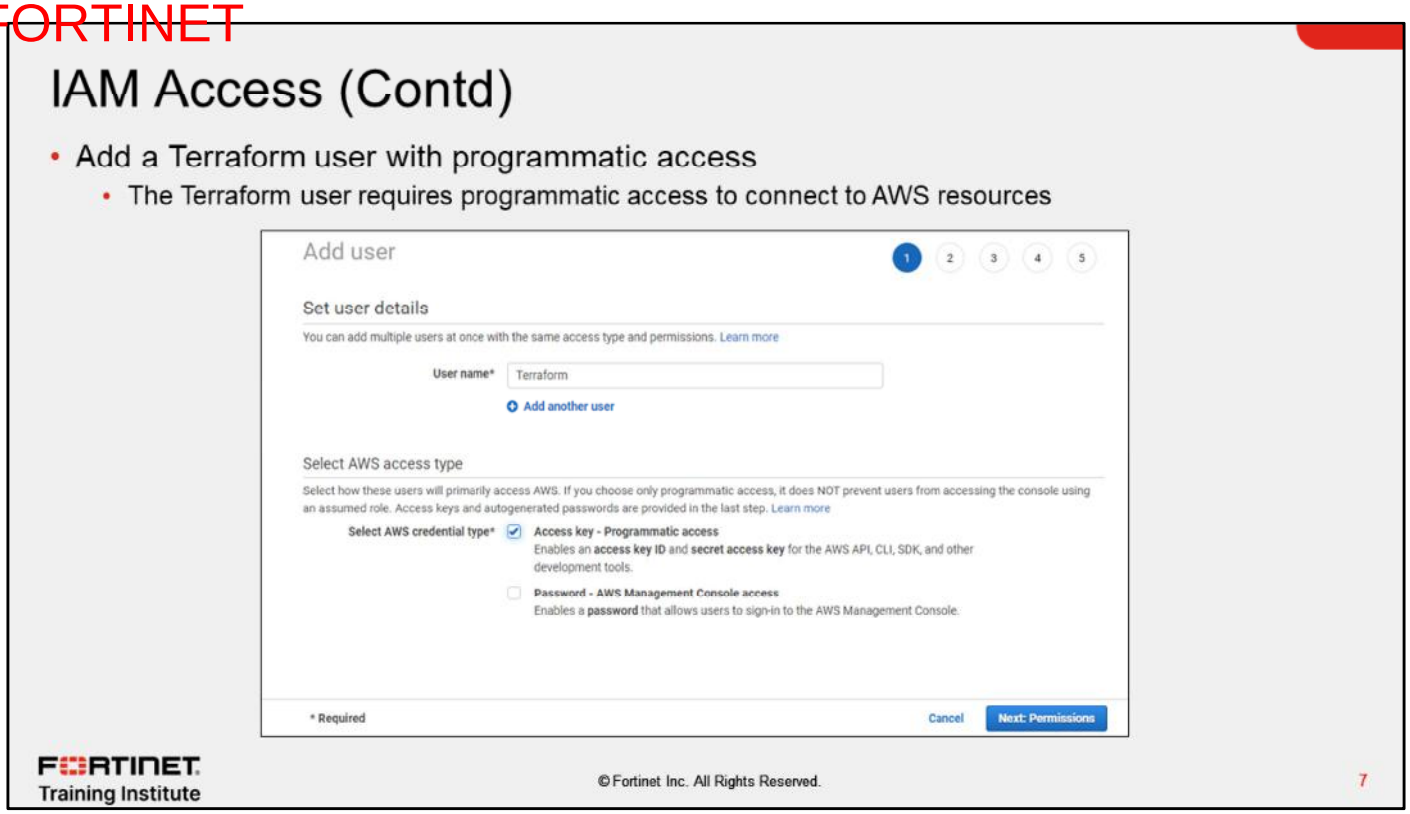
Another way of installing Terraform is to use AWS CloudShell. AWS CloudShell is included in every AWS account. Once CloudShell is running, you can install Terraform. One advantage of using CloudShell to run Terraform is easy authentication. Because you are already logged in to the AWS account and are accessing CloudShell, you do not need to authenticate, to get access to AWS resources from Terraform.

DO NOT REPRINT
© FORTINET



Before deploying a FortiGate VM from Terraform, you must create an IAM user with the required permission on AWS. IAM identities—users, groups, and roles—must be assigned explicit permissions to access AWS resources.

DO NOT REPRINT
© FORTINET

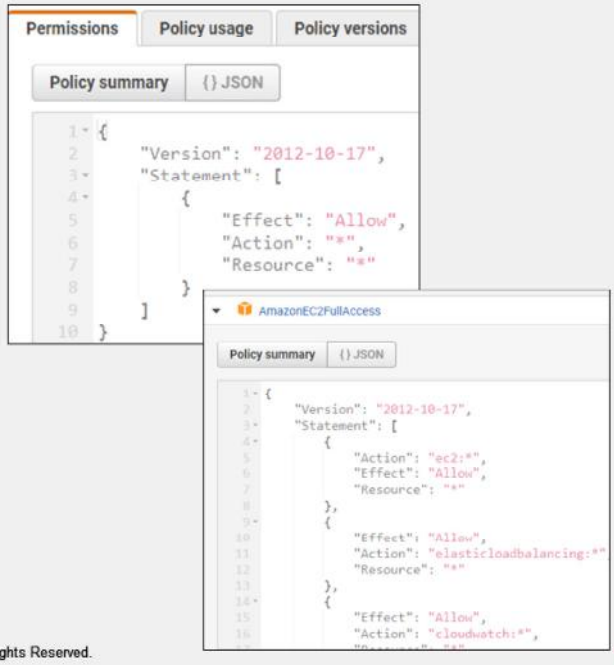


The Terraform user must have programmatic access on AWS. This ensures that Terraform can access AWS resources using APIs, without entering a password.

DO NOT REPRINT
© FORTINET

User Permission to Run Terraform

- Full administrator access
  - Be cautious when giving a full access policy
- Minimum permission to deploy an EC2 instance
  - In a production environment, apply a policy that gives permission to deploy only the required resources
  - A custom policy may be needed



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

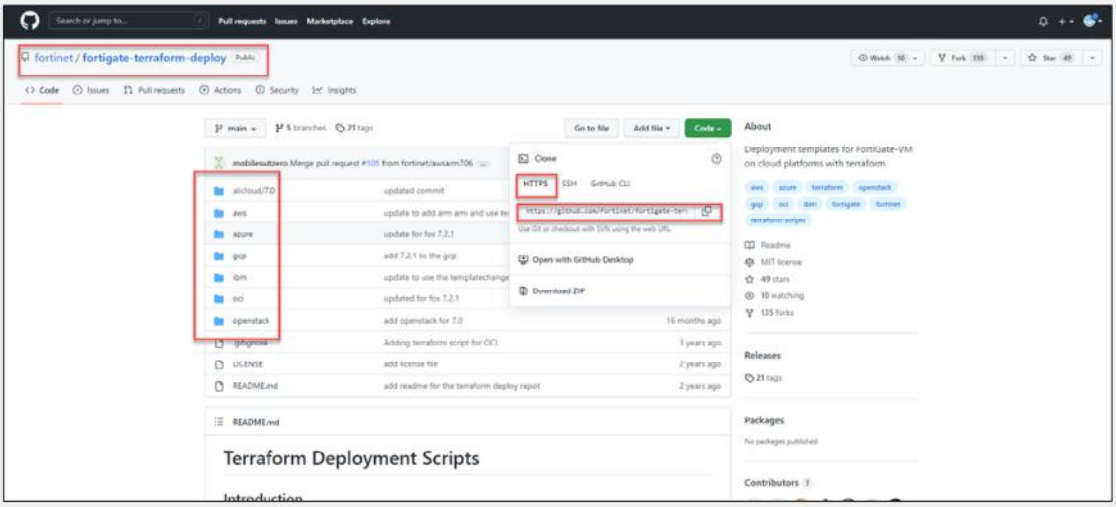
8

When you assign permissions in a production environment, it is recommended that you assign only the necessary permissions. However, during the lab exercises, you can assign full administrator access to the Terraform in order to complete the exercises. At the same time, you can manage your IAM policies in Terraform, rather than managing them manually in AWS. With Terraform, you can reuse your policy templates and ensure the principle of least privilege with resource interpolation.

DO NOT REPRINT
© FORTINET

Terraform Templates on GitHub

- Clone Terraform templates from GitHub
- There are many Fortinet templates available to choose from



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Fortinet provides many templates on GitHub. In order to deploy a specific project, you must clone the project from the GitHub.

DO NOT REPRINT
© FORTINET

Terraform Templates on GitHub (Contd)

- Use the `git clone` command to clone the Template

```
ec2-user@ip-172-31-22-97:~/NSE7/terraform/aws-terraform/single
[ec2-user@ip-172-31-22-97 ~]$ terraform version
Terraform v1.2.7
on linux_amd64
[ec2-user@ip-172-31-22-97 ~]$ git clone https://github.com/Fortinet-Courseware/NSE7.git
-bash: git: command not found
[ec2-user@ip-172-31-22-97 ~]$ git version
-bash: git: command not found
[ec2-user@ip-172-31-22-97 ~]$ sudo yum install git -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
amzn2extra-docker
```

- Use the `tree` command to check the Terraform code hierarchy

```
[ec2-user@ip-172-31-22-97 single]$ tree
.
├── fgtvm.conf
├── fgtvm.tf
├── network.tf
├── output.tf
├── provider.tf
├── README.md
├── terraform.tfvars.example
├── variables.tf
└── vpc.tf

0 directories, 9 files
[ec2-user@ip-172-31-22-97 single]$
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

After you copy the URL, use the `git clone` command to clone the environment in Terraform. After you have created the clone, you can run the Linux `tree` command to view the file structure.

DO NOT REPRINT
© FORTINET

Adding IAM Credentials to Terraform

- After cloning the Terraform template, add IAM credentials or provide credentials at the executing stage
- There are many other ways you can add credentials:
  - By default, the `terraform.tfvars.example` file is empty
  - Add the credentials and save it as `terraform.tfvars`

```
[ec2-user@ip-172-31-22-97 single]$ cat terraform.tfvars
// AWS Environment
access_key = "AKIA4JXF[redacted]SY"
secret_key = "/vUoh9M6hIB1YPdb9aZ7xoI[redacted]z"
[ec2-user@ip-172-31-22-97 single]$
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

There are several ways you can add AWS credentials. For example, you can pass the access key and secret key values as environment variables. This is the safest way to add the credentials; however, every time you open a new terminal, you have to provide the credentials again.

DO NOT REPRINT
© FORTINET

Variables File

- Know your deployment location
- Check your `variables.tf` file to verify your deployment location, license type, and so on

```
[ec2-user@ip-172-31-22-97 single]$ cat variables.tf
//AWS Configuration
variable access_key {}
variable secret_key {}

variable "region" {
  default = "us-west-1"
}

// Availability zones for the region
variable "az1" {
  default = "us-west-1a"
}

variable "vpccidr" {
```

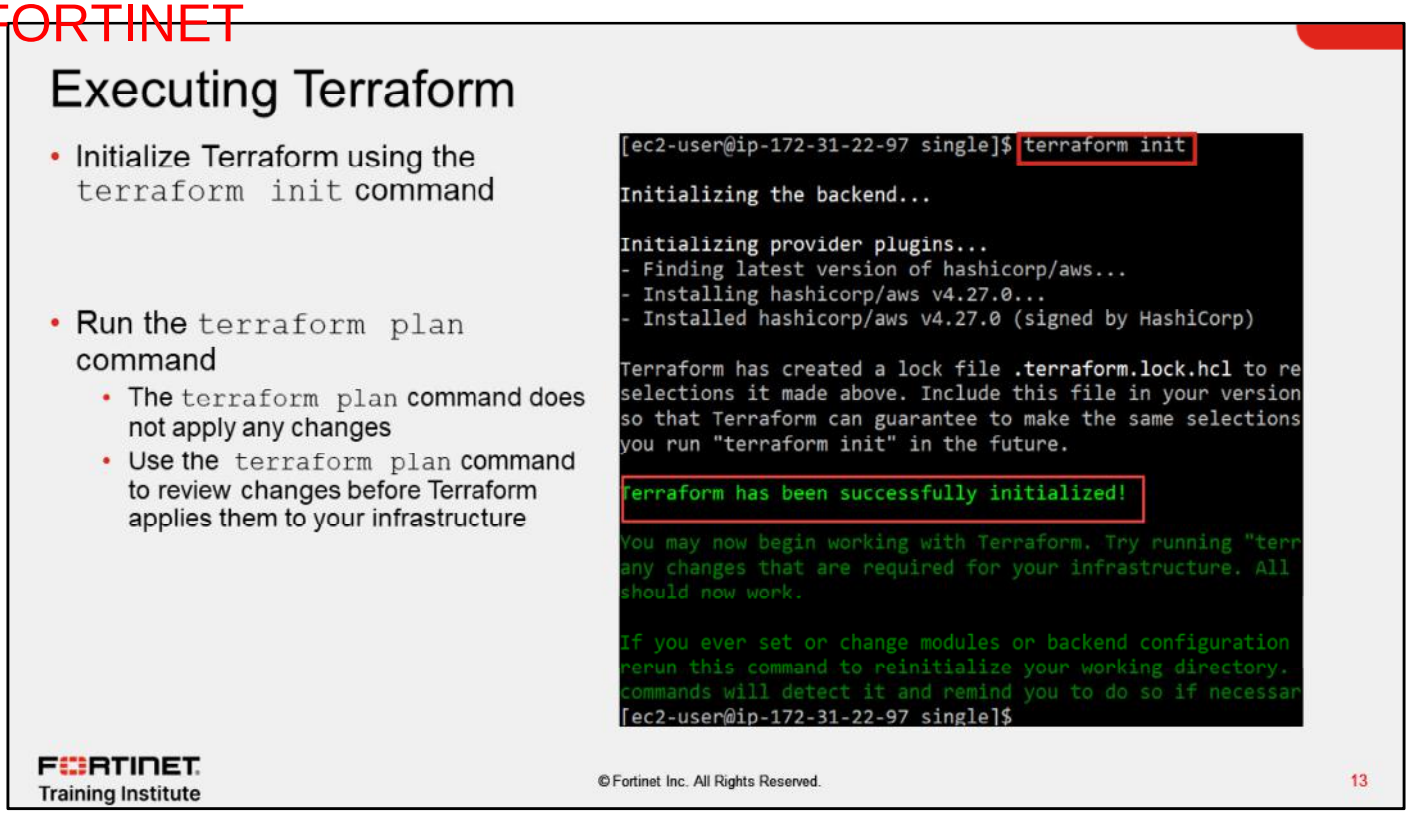
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

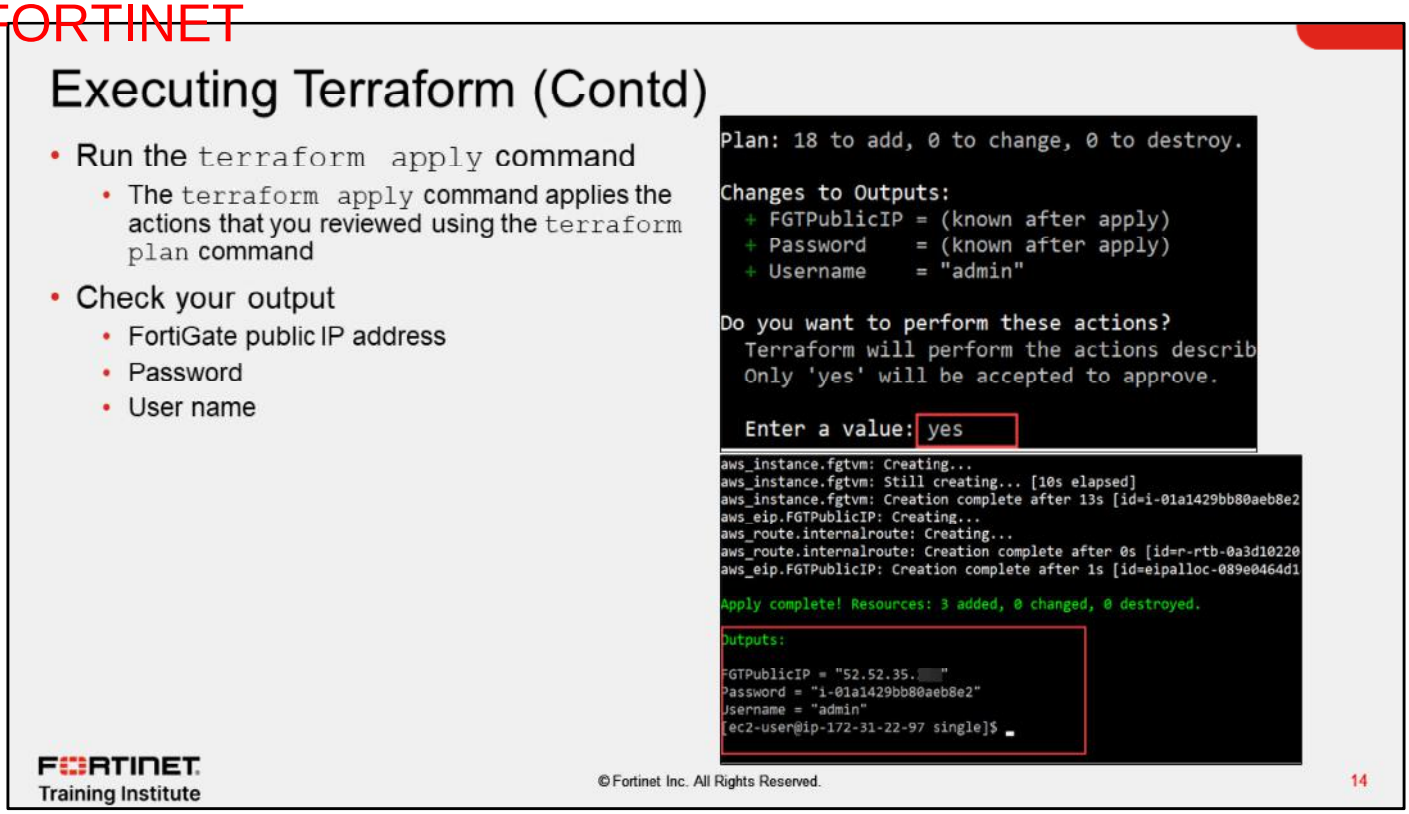
The input variables are used to define the values that configure your infrastructure. These variables can be reused multiple times. Check your `vaiables.tf` file to see all of the variables in your configuration. In the example shown on this slide, all resources will be deployed in the `us-west-1` region.

DO NOT REPRINT
© FORTINET



So, how do you start the Terraform execution? The first step is to initialize Terraform by running the `terraform init` command. After you initialize your working directory, the next step is to run the `terraform plan` command. The `terraform plan` command lets you view all the actions that Terraform will take to change your infrastructure.

DO NOT REPRINT
© FORTINET



It is very straightforward. The `terraform apply` command performs the actions proposed in a Terraform plan. The `terraform apply` command deploys your infrastructure. After you give confirmation, it will take a few minutes for the process to finish. Finally, you will see output that shows you the information that you need to access the resources.

DO NOT REPRINT
© FORTINET

Destroy Resources Using Terraform

- The `terraform destroy` command terminates resources
  - Objects are maintained in a state file and the `terraform destroy` command terminates resources in the state file
- A destroy plan is presented for review before the final confirmation

```
Terraform used the selected providers to generate the following execution plan. Resourc
  - destroy

Terraform will perform the following actions:

  # aws_eip.FGTPublicIP will be destroyed
  - resource "aws_eip" "FGTPublicIP" {
      - allocation_id        = "eipalloc-089e0464d18c2324d" -> null
      - association_id       = "eipassoc-09ed7fe277f15e617" -> null
      - domain               = "vpc" -> null
      - id                   = "eipalloc-089e0464d18c2324d" -> null
      - instance             = "i-01a1429bb80aeb8e2" -> null
      - network_border_group = "us-west-1" -> null
      - network_interface    = "eni-021f06cf6135f9e33" -> null
      - private_dns          = "ip-10-1-0-244.us-west-1.compute.internal" -> null
      - private_ip           = "10.1.0.244" -> null
      - public_dns           = "ec2-52-52-35-242.us-west-1.compute.amazonaws.com" -> nu
      - public_ip            = "52.52.35.242" -> null
      - public_ipv4_pool     = "amazon" -> null
      - tags                 = {} -> null
      - tags_all             = {} -> null
      - vpc                  = true -> null
    }

  # aws_instance.fgtvm will be destroyed
  - resource "aws_instance" "fgtvm" {
      - ami                                  = "ami-027023effe0d0cbcb" -> null
      - arn                                  = "arn:aws:ec2:us-west-1:845513257411:inst
      - associate_public_ip_address          = true -> null
      - availability_zone                    = "us-west-1a" -> null
      - cpu_core_count                       = 2 -> null
      - cpu_threads_per_core                 = 2 -> null
      - disable_api_stop                     = false -> null
      - disable_api_termination              = false -> null
```

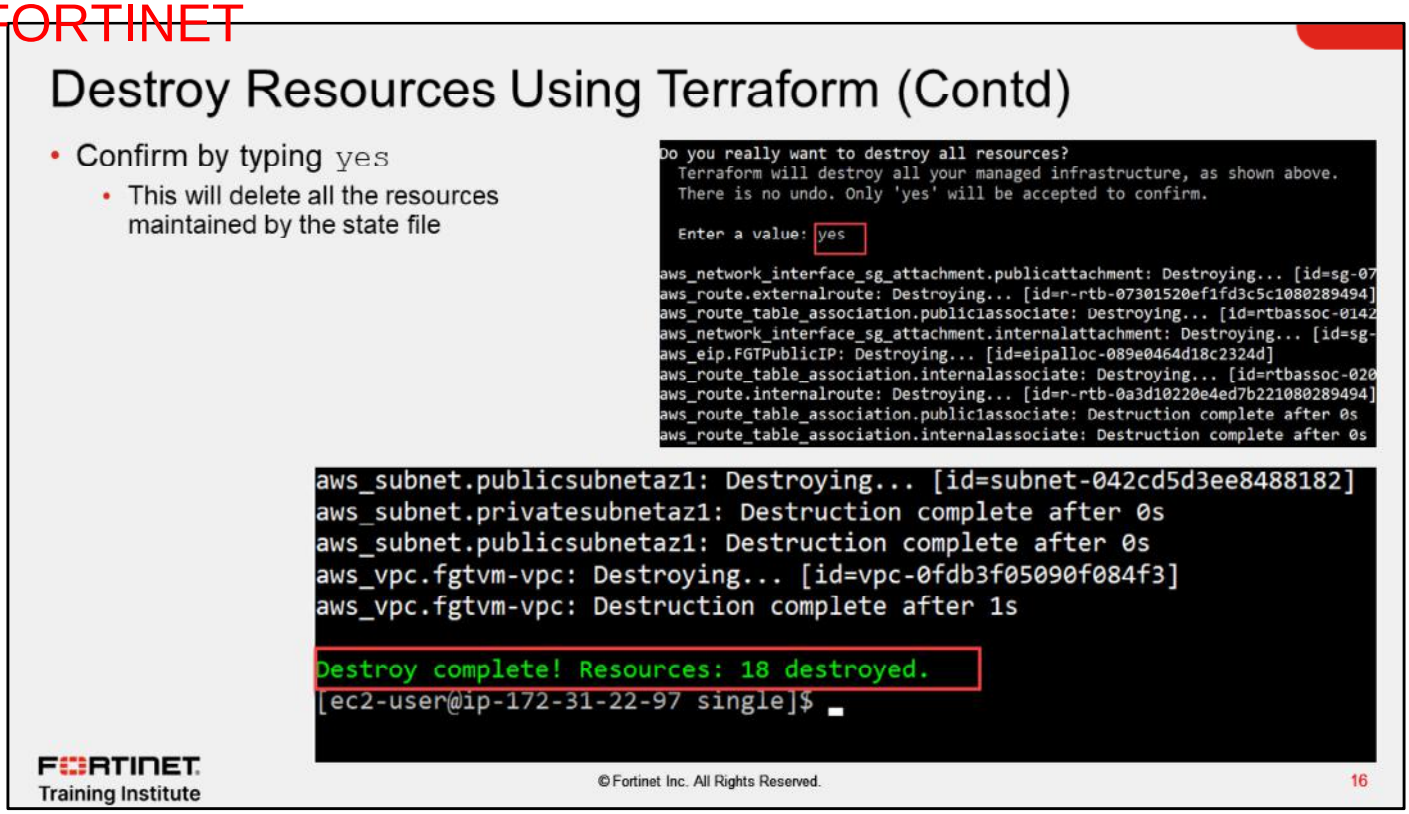
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

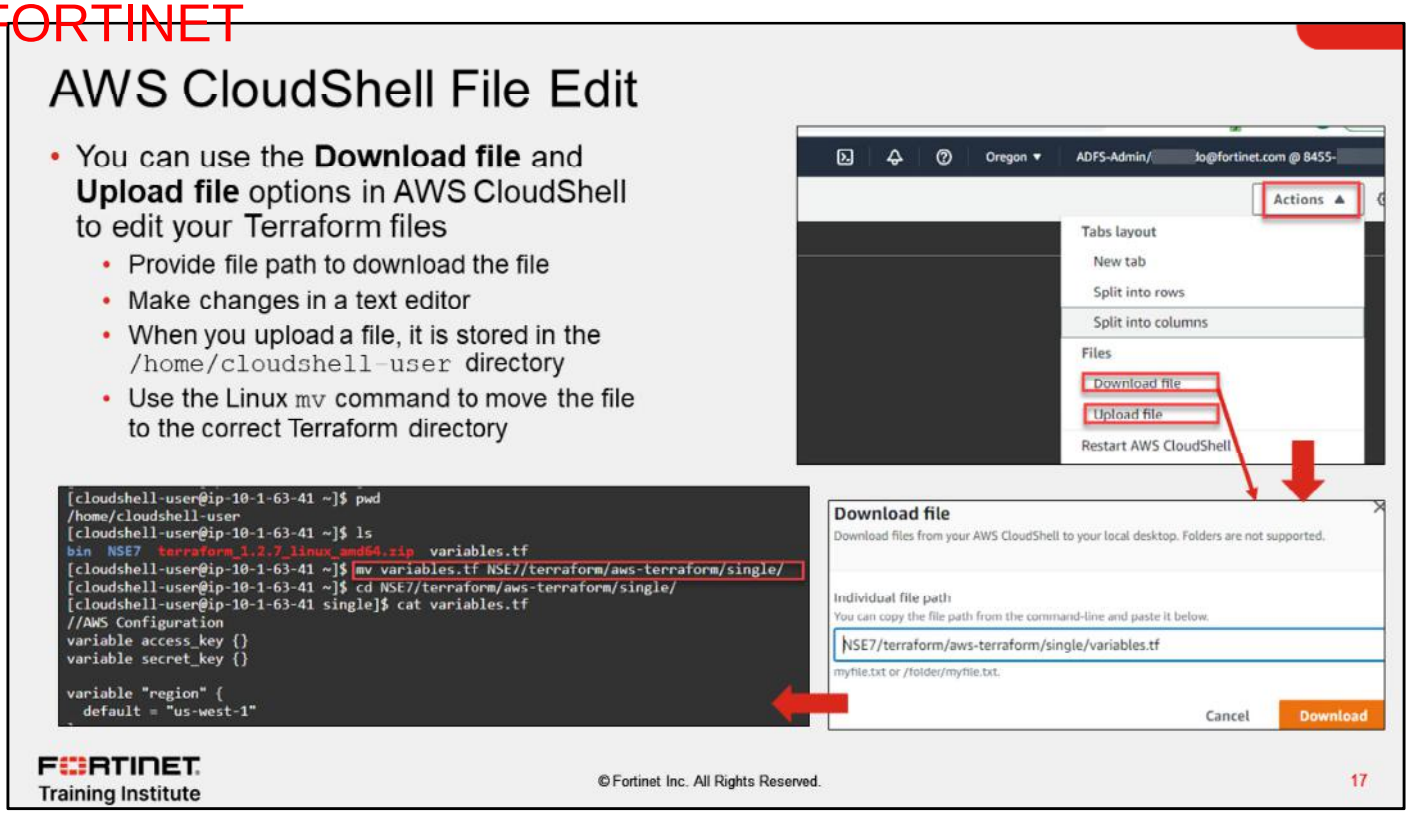
After you run the `terraform apply` command, all the objects are maintained in a state file. This is the relationship between actual infrastructure and the IaC. So, the state file plays a big role how objects are created and destroyed in Terraform. Any resources that are *not* in the state file, will not be destroyed by the `terraform destroy` command.

DO NOT REPRINT
© FORTINET



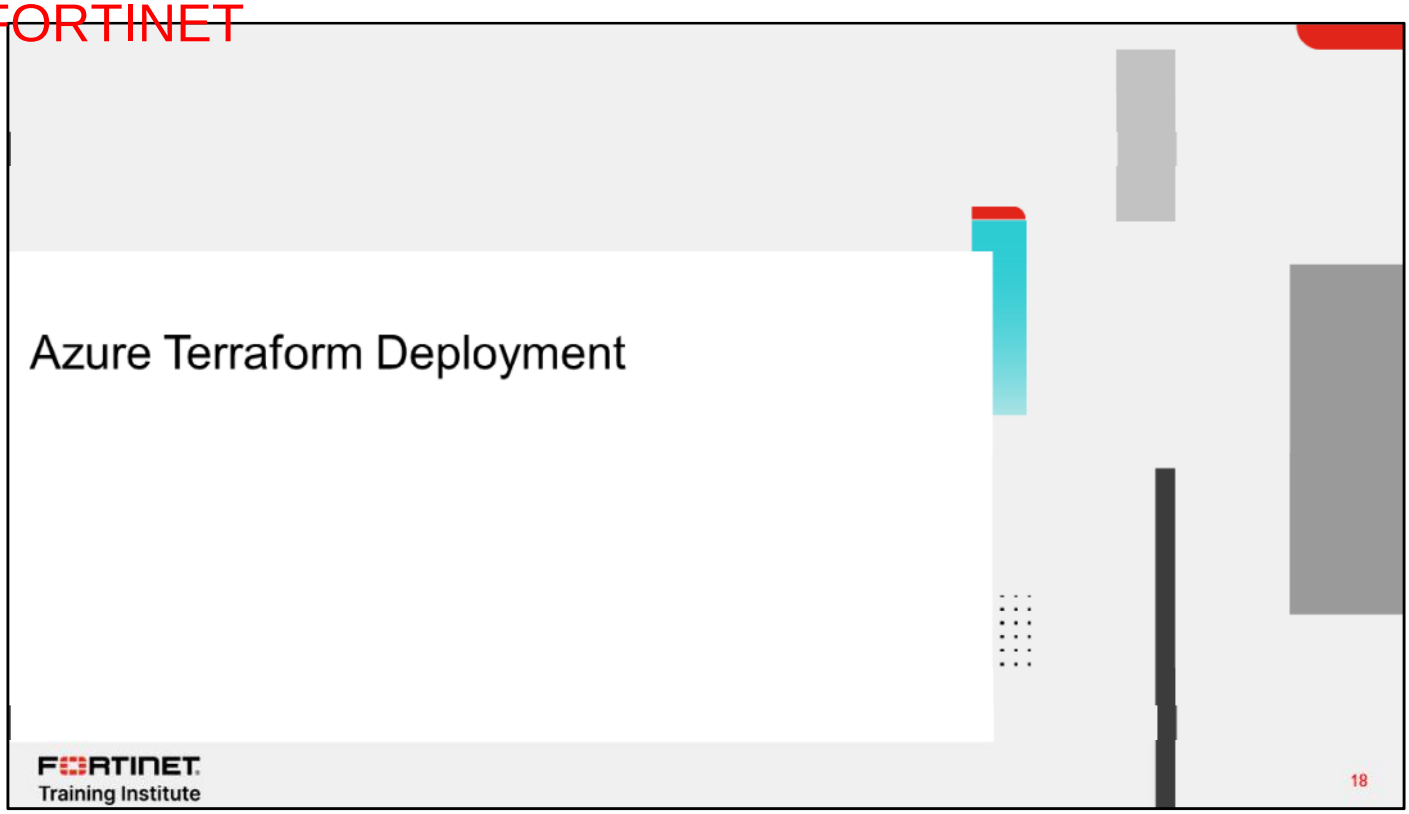
Finally, you can type `yes` to confirm the destroy action. It will take few seconds to delete all of the resources, depending on your project size. Keep in mind that the `terraform destroy` command destroys only certain items that were deployed through the Terraform code. So, make sure that you check your AWS account and manually terminate all other resources, after you complete all the labs in this course. For example, you will need to manually terminate all the Linux instances that you created separately.

DO NOT REPRINT
© FORTINET



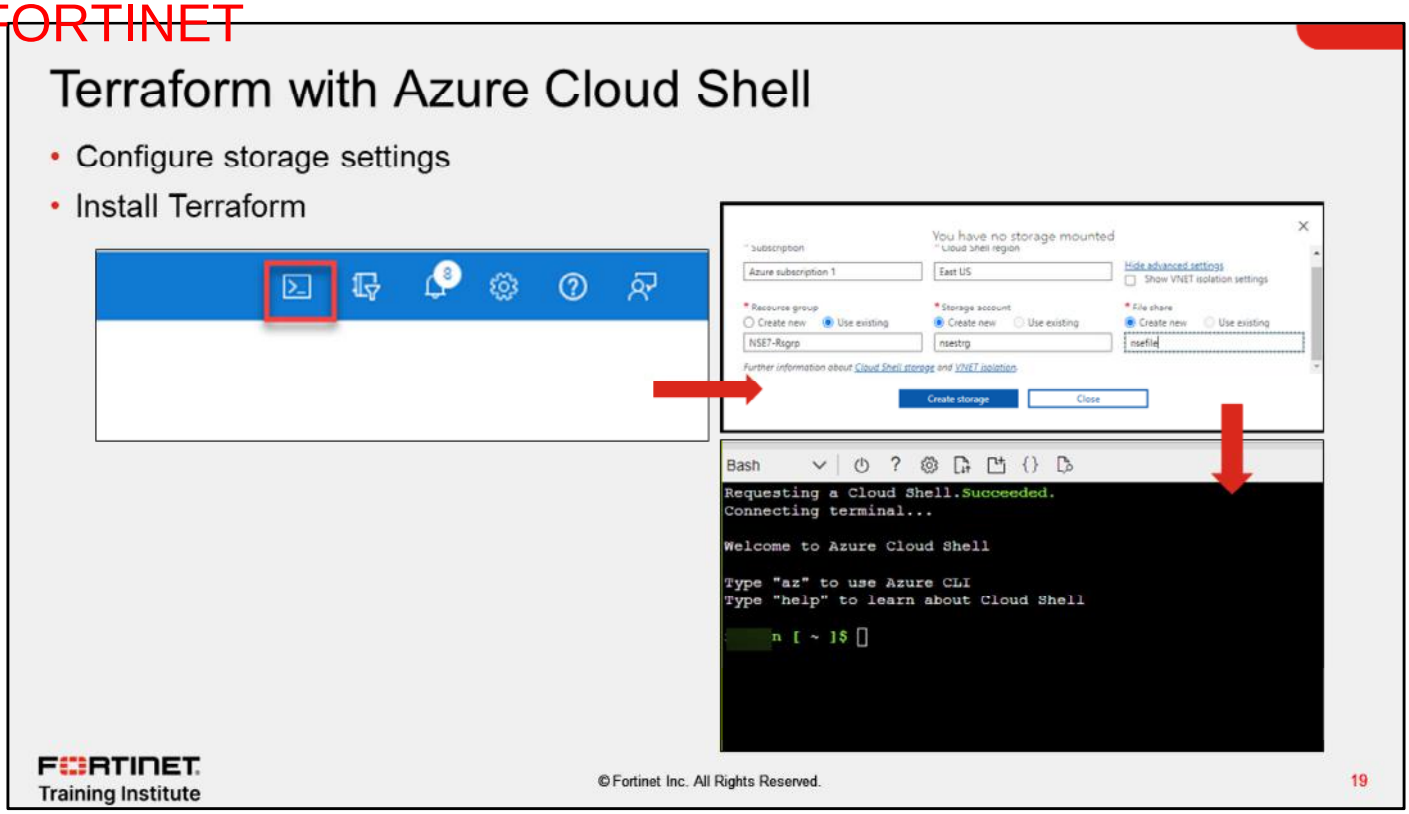
When you work with CloudShell, it is easy to use the **Upload file** and **Download file** options to update files. Also, make sure to move files from the CloudShell directory to the Terraform directory.

DO NOT REPRINT
© FORTINET



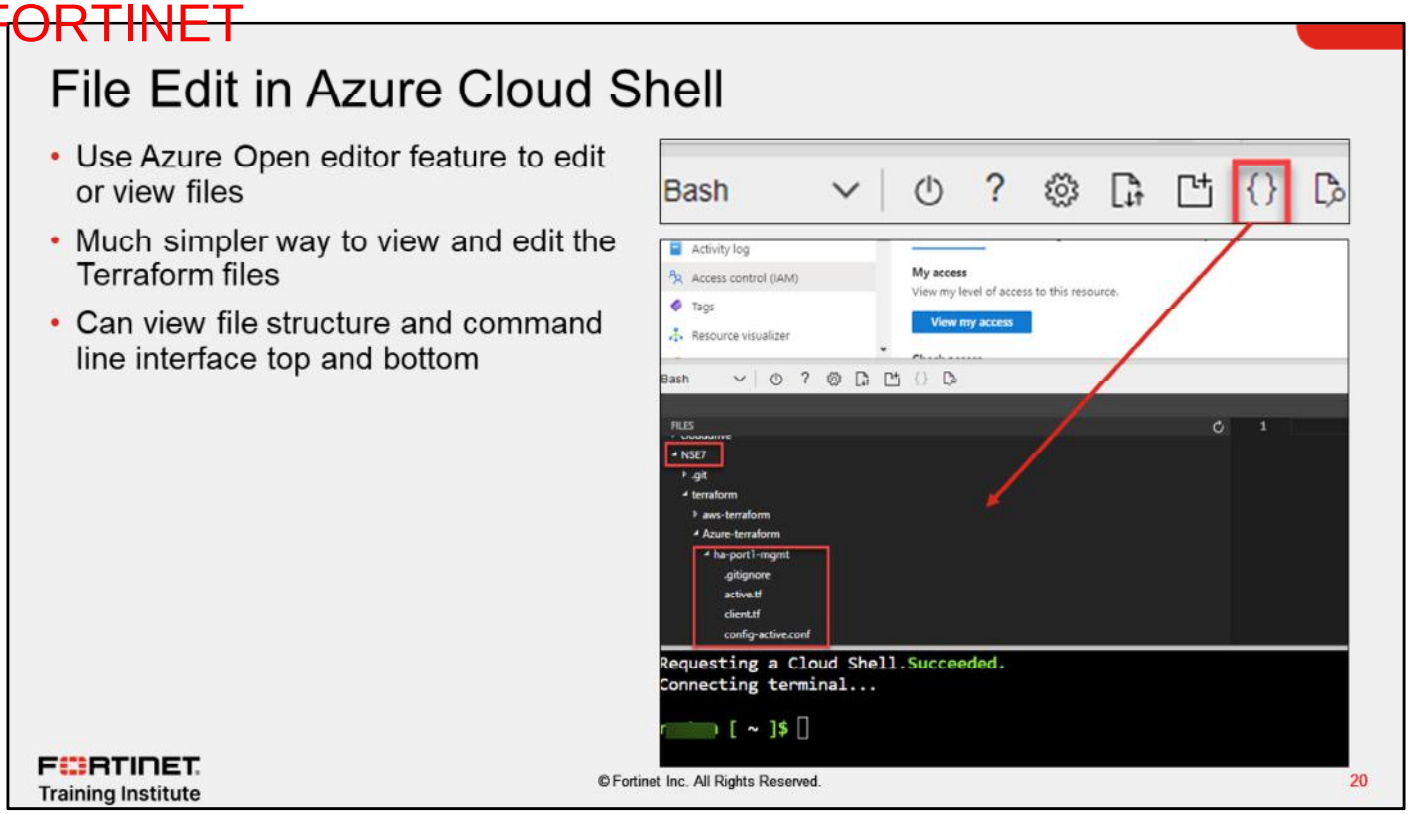
In this section, you will learn about Azure Terraform deployment.

DO NOT REPRINT
© FORTINET



Microsoft Azure Cloud Shell is another very good tool form performing your Terraform work. Every Azure account includes Azure Cloud Shell access and can be easily set up. The first time you access Azure Cloud Shell, you must configure storage settings.

DO NOT REPRINT
© FORTINET

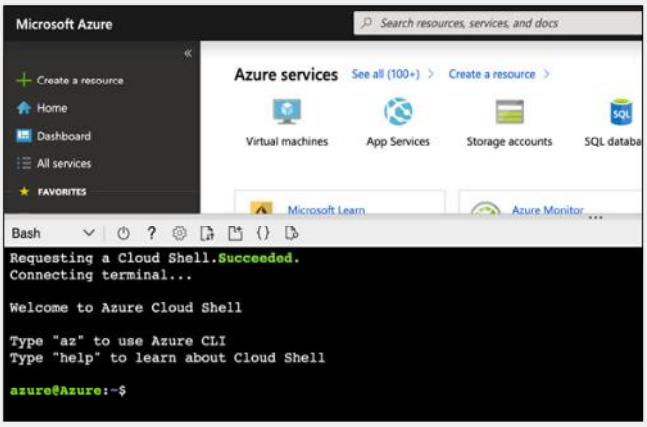


Azure **Open editor** tool is one of the convenient way to edit your Terraform files. When you working with the Azure CLI , you can also view your file structure on the top make your configuration change easy.

DO NOT REPRINT
© FORTINET

Azure License Terms Validation

- If you have never deployed a FortiGate or FortiAnalyzer in your subscription you need to accept the terms.
- Either you deploy the product in Azure through the Azure Portal or you can use the Azure Cloud Shell and run these commands:




```
$ az vm image accept-terms --publisher fortinet --offer fortinet_fortigate-vm_v5 --plan fortinet_fg-vm
$ az vm image accept-terms --publisher fortinet --offer fortinet-fortianalyzer --plan fortinet-fortianalyzer
```

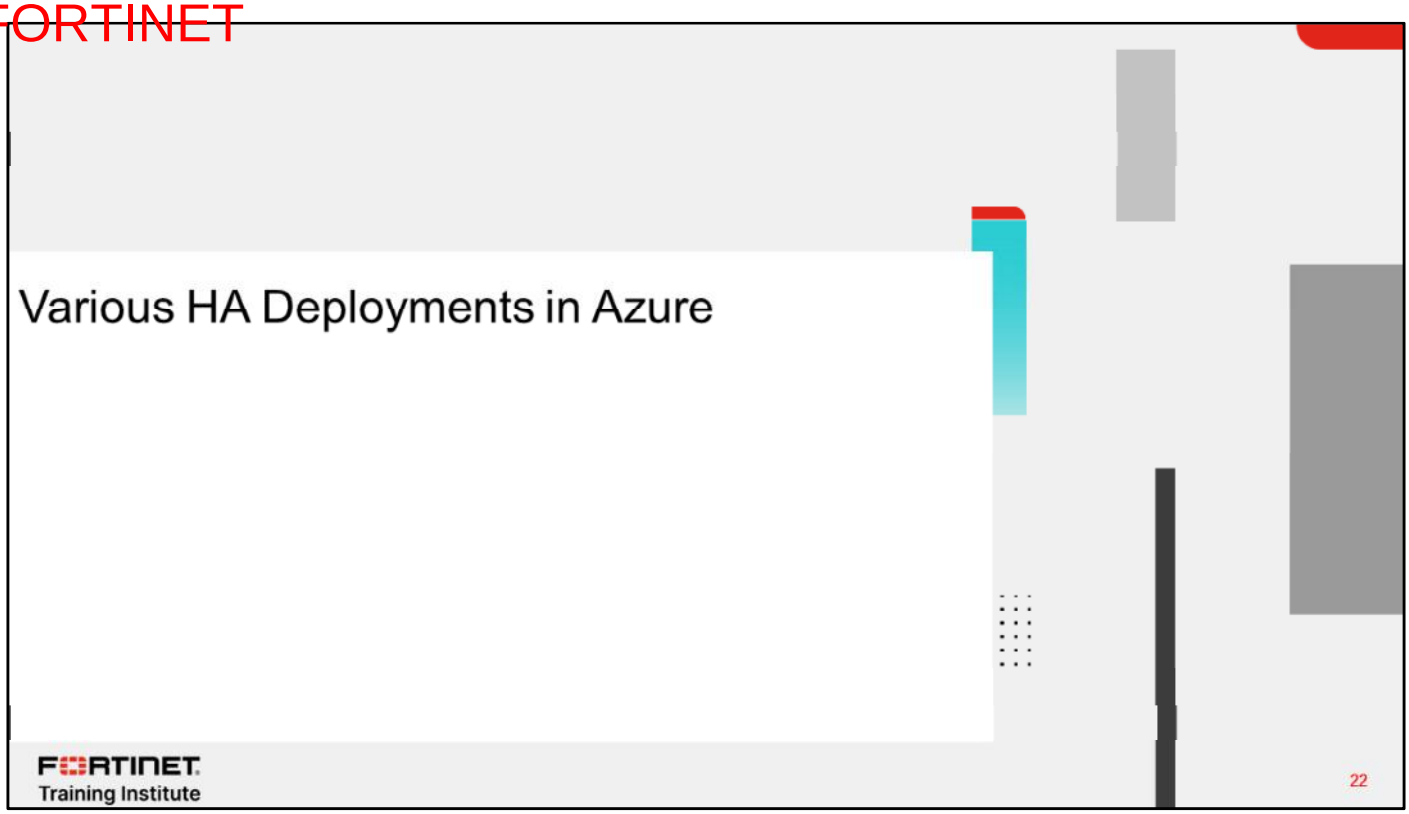
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

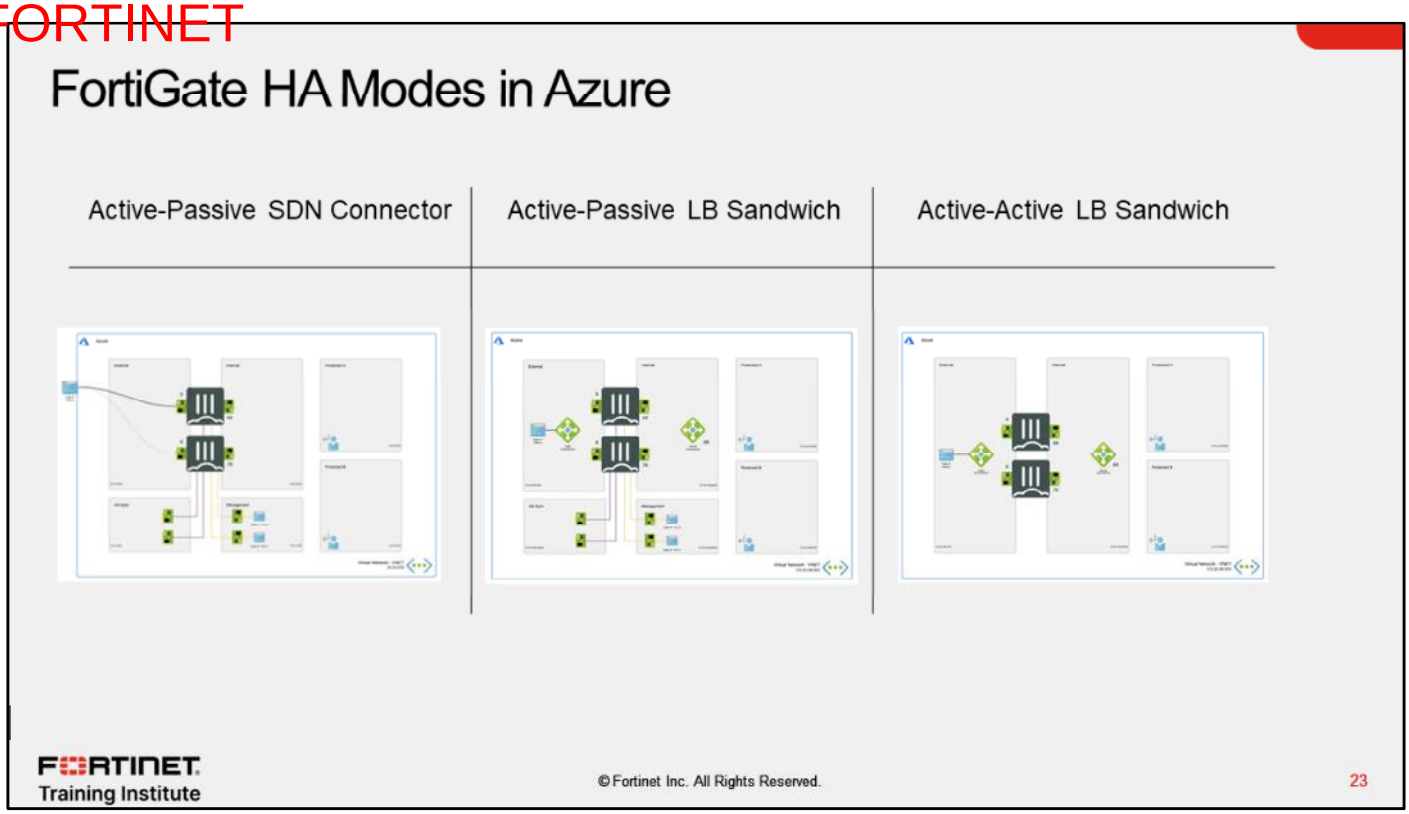
If you have never deployed any FortiGate VMs in your Azure account, you must first accept the terms for the FortiGate PAYG or BYOL image in the Azure Marketplace. Enter the command on the Azure CLI before the first deployment in a subscription or you can manually deploy the product through the Azure portal.

DO NOT REPRINT
© FORTINET



In this section, you will learn about various HA deployments in Azure.

DO NOT REPRINT
© FORTINET



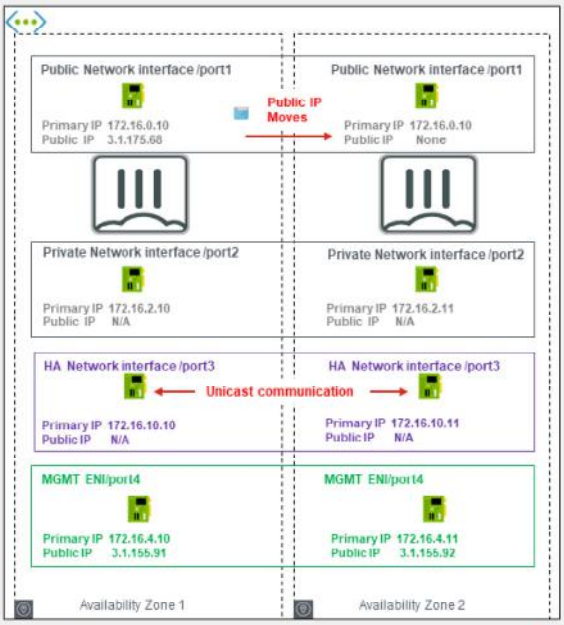
Now, you will learn the basics about FortiGate HA modes in Azure. There are three main FortiGate HA scenarios in Azure: active-passive SDN connector, active-passive load balance sandwich, and active-active load balance sandwich.

DO NOT REPRINT
© FORTINET

FortiGate HA Modes In Azure (Contd)

- Active-Passive SDN Connector
  - Two FortiGate VMs
  - HA unicast communication
  - Minimum of four network interfaces:
    - Port1: external interface
    - Port2: private interface
    - Port3: HA interface
    - Port4: dedicated management interface
  - Managed Identity / Service Principal to authenticate and make API calls to Azure

```
config system sdn-connector
  edit "azure-globalsdn-iam-ha"
    set status enable
    set type azure
    set use-metadata-iam enable
    set ha-status enable
    set subscription-id ""
    set resource-group ""
    set azure-region global
    config nic
      edit "fgta-ap-port1"
        config ip
          edit "ipconfig1"
            set public-ip "fgt-ap-cluster"
            set resource-group "fortigate-ha-training"
          next
        end
      next
    end
    config route-table
      edit "az_spoke1_useast_web"
        set subscription-id "bc0e730b-2345-4c66-9a74-afdfc1xxxxxx"
        set resource-group "fortigate-ha-training"
        config route
          edit "default_spoke1_web"
            set next-hop "10.60.5.4"
          next
          edit "az_spoke1_useast_app"
            set next-hop "10.60.5.4"
          next
        end
      next
    end
    set update-interval 40
  next
end
```



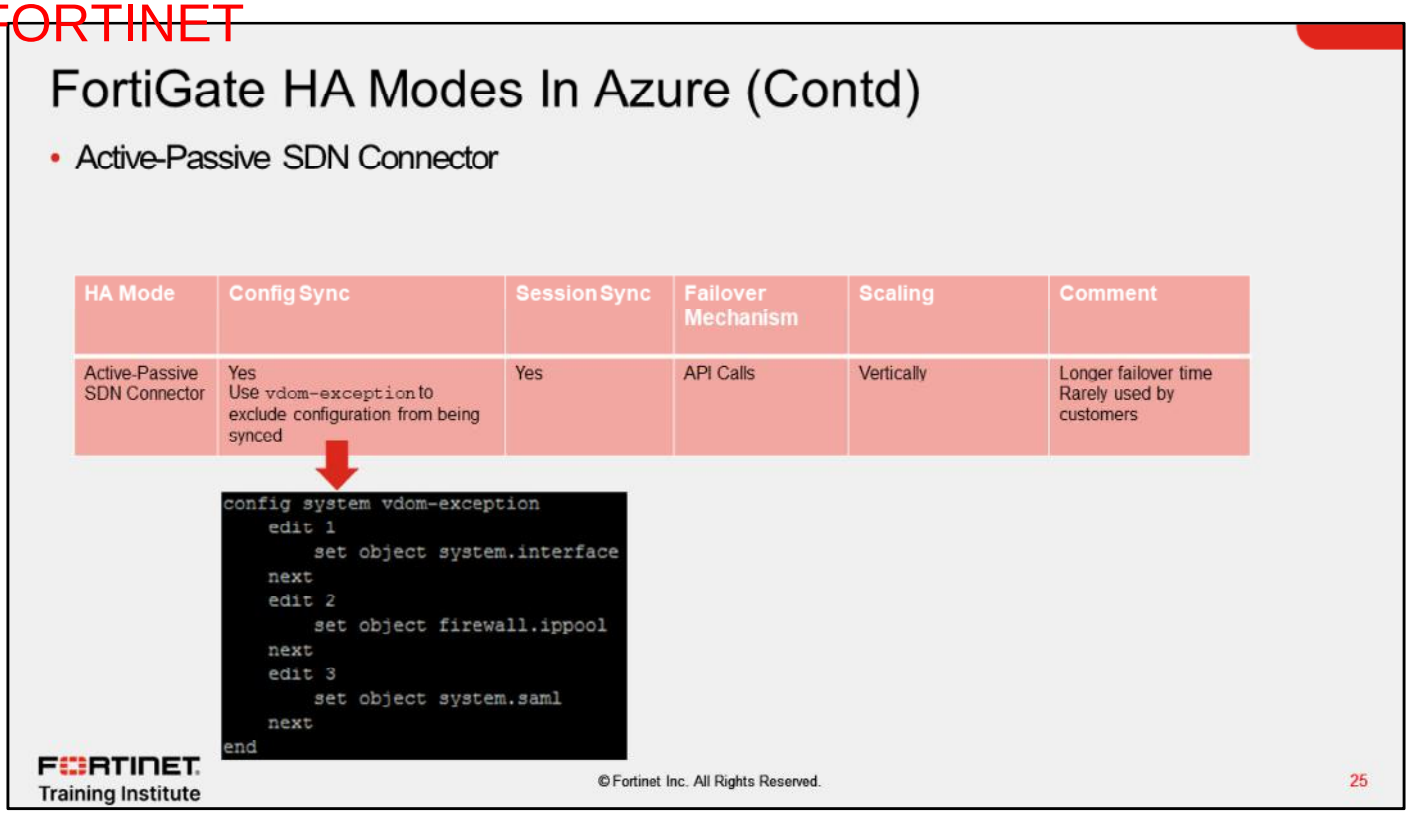
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

The active-passive SDN connector design deploys two FortiGate VMs in active-passive mode. The FortiGate VMs are connected using the unicast FGCP HA protocol. This protocol synchronizes the configuration. On failover, the passive FortiGate takes control. The passive FortiGate then issues API calls to Azure asking it to shift the public IP address and update the internal, user-defined routing to itself. Shifting the public IP address and gateway IP addresses of the routes takes time for Azure to complete, especially if environment is larger and there are multiple Public IPs to be shifted and multiple routes to be changed. The failover time is variable depending on the platform.

DO NOT REPRINT
© FORTINET

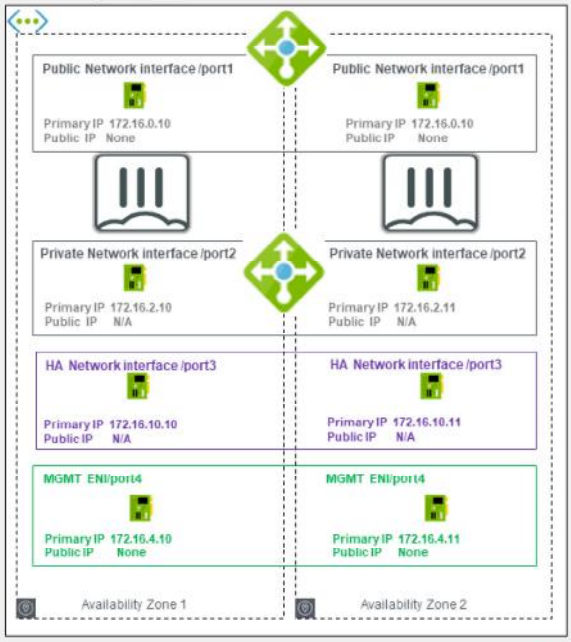


The table on this slide provides a summary of various settings in an active-passive HA with SDN connector scenario. Two key points to note are that you must use `vdom-exception` to exclude the configuration from being synchronized, and that the failover time is longer.

DO NOT REPRINT
© FORTINET

FortiGate HA Modes In Azure (Contd)

- Active-Passive Load Balance Sandwich
  - Two FortiGate VMs
  - HA unicast communication
  - Minimum of four network interfaces:
    - Port1: external interface
    - Port2: private interface
    - Port3: HA interface
    - Port4: dedicated management interface



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

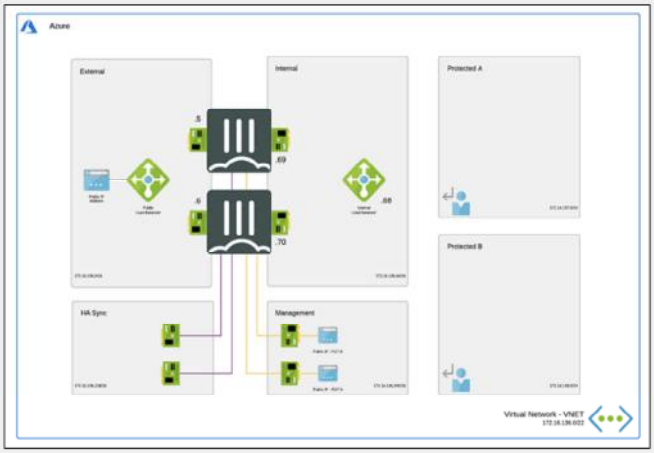
26

This slide shows an example FortiGate active-passive load balance sandwich scenario. An active-passive load balance sandwich design deploys two FortiGate VMs in active-passive mode, connected using unicast FortiGate clustering protocol (FGCP) HA protocol. In this setup, the Azure load balancer handles traffic failover using a health probe directed towards the FortiGate VMs. The failover times are based on the health probe of the Azure load balancer; two failed attempts per five seconds in a maximum of 15 seconds. The public IP addresses are configured on the Azure load balancer and provide ingress and egress flows with inspection from FortiGate.

DO NOT REPRINT
© FORTINET

FortiGate HA Modes In Azure (Contd)

- Active-Passive Load Balance Sandwich
  - External load balancer to attach public IP
    - Load balancing rules
  - Internal load balancer listener to be used as the next-hop for outgoing traffic
    - HA ports load balancing rule



Name	Type
fgt-InternalLoadBalancer	Load balancer
fgt-publicLoadBalancer	Load balancer

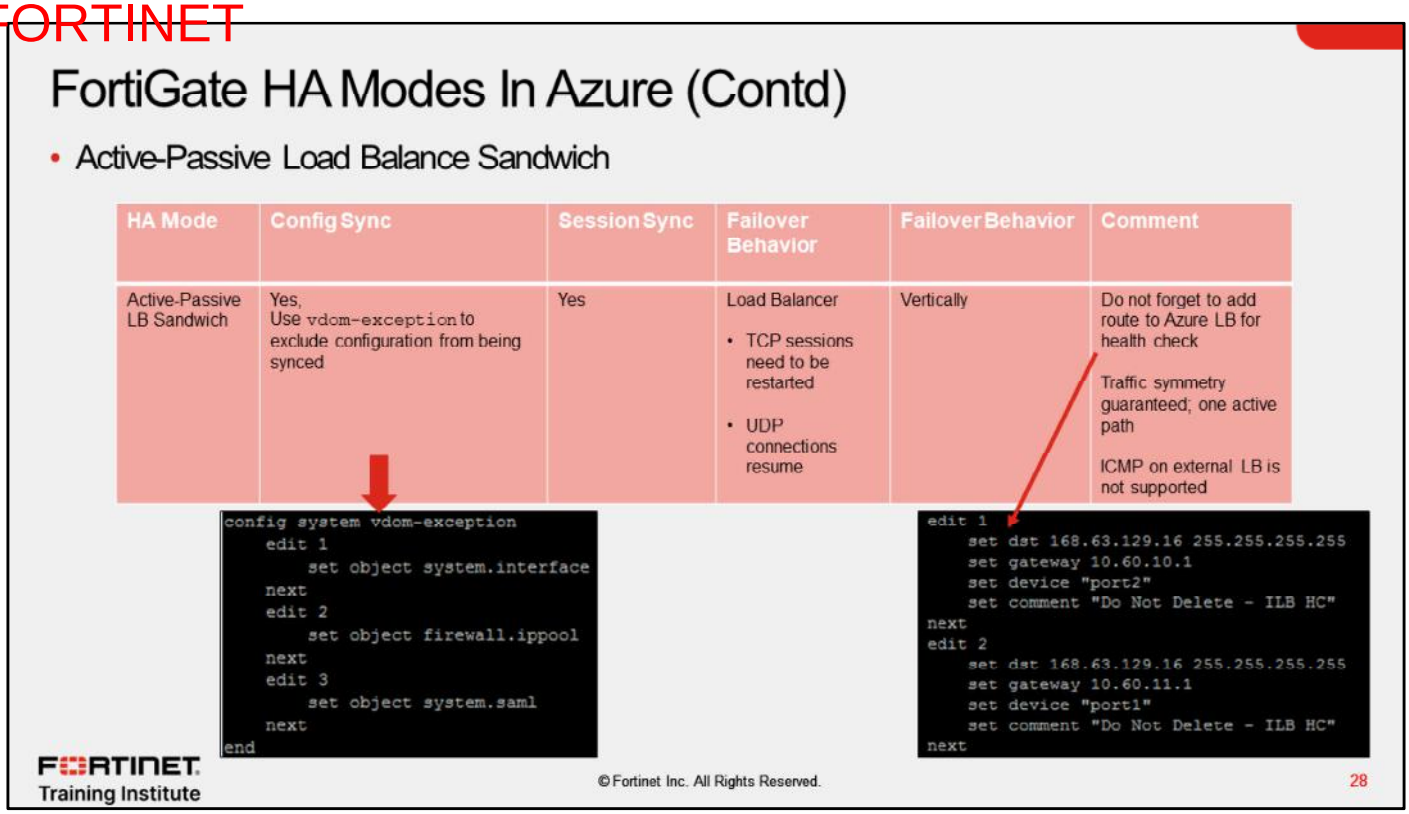
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

In this FortiGate active-passive load balance sandwich scenario, the external load balancer has the public IP address with load balancing rules. The internal load balancer receives all internal traffic and forwards it to the Azure gateways connecting ExpressRoute or Azure VPNs. HA ports are a type of load balancing rule that provides an easy way to load balance all flows that arrive on all ports of an internal standard load balancer. The load balancing decision is made per flow.

DO NOT REPRINT
© FORTINET



The table on this slide provides a summary of various settings in HA active-passive load balance sandwich. Two important points to note are that you must use `vdom-exception` to exclude the configuration from being synchronized and that you must add a route to the Azure load balancer for the health check.

DO NOT REPRINT
© FORTINET

FortiGate HA Modes In Azure (Contd)

- HA with three NICs (FortiOS 7.0.1 or later)
  - Two FortiGate VMs
  - HA unicast communication
  - Minimum of three network interfaces:
    - Port1: external interface
    - Port2: private interface
    - Port3: HA interface and dedicated management interface

```
config system ha
    set group-name "az-fgtha-3nic"
    set mode a-p
    set password ENC zURWvRR91vKMNyappSMJA2GnpBYCnh2dDUq/2+krMsqLv
yh8jzzBN1FagIe0lcfUEEhZDXggY54qWnlm86Ev5H6NicDgg==
    set hbdev "port3" 50
    set session-pickup enable
    set uninterruptible-upgrade disable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port3"
            set gateway 10.60.7.1
        next
    end
    set override disable
    set priority 100
    set unicast-hb enable
    set unicast-hb-peerip 10.60.7.7
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

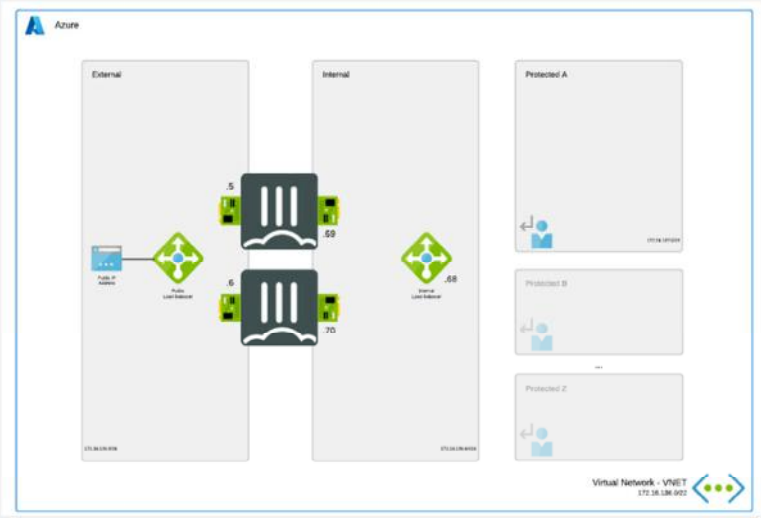
29

This slide shows an example of FortiGate HA in Azure with only three ports. The main difference between this scenario and other HA scenarios, is that port3 is used for both the HA interface and the dedicated management interface.

DO NOT REPRINT
© FORTINET

FortiGate HA Modes In Azure (Contd)

- Active-Active Load Balance Sandwich
  - Two or more FortiGate VMs
  - Minimum of two network interfaces
    - » Port1: external interface
    - » Port2: private interface



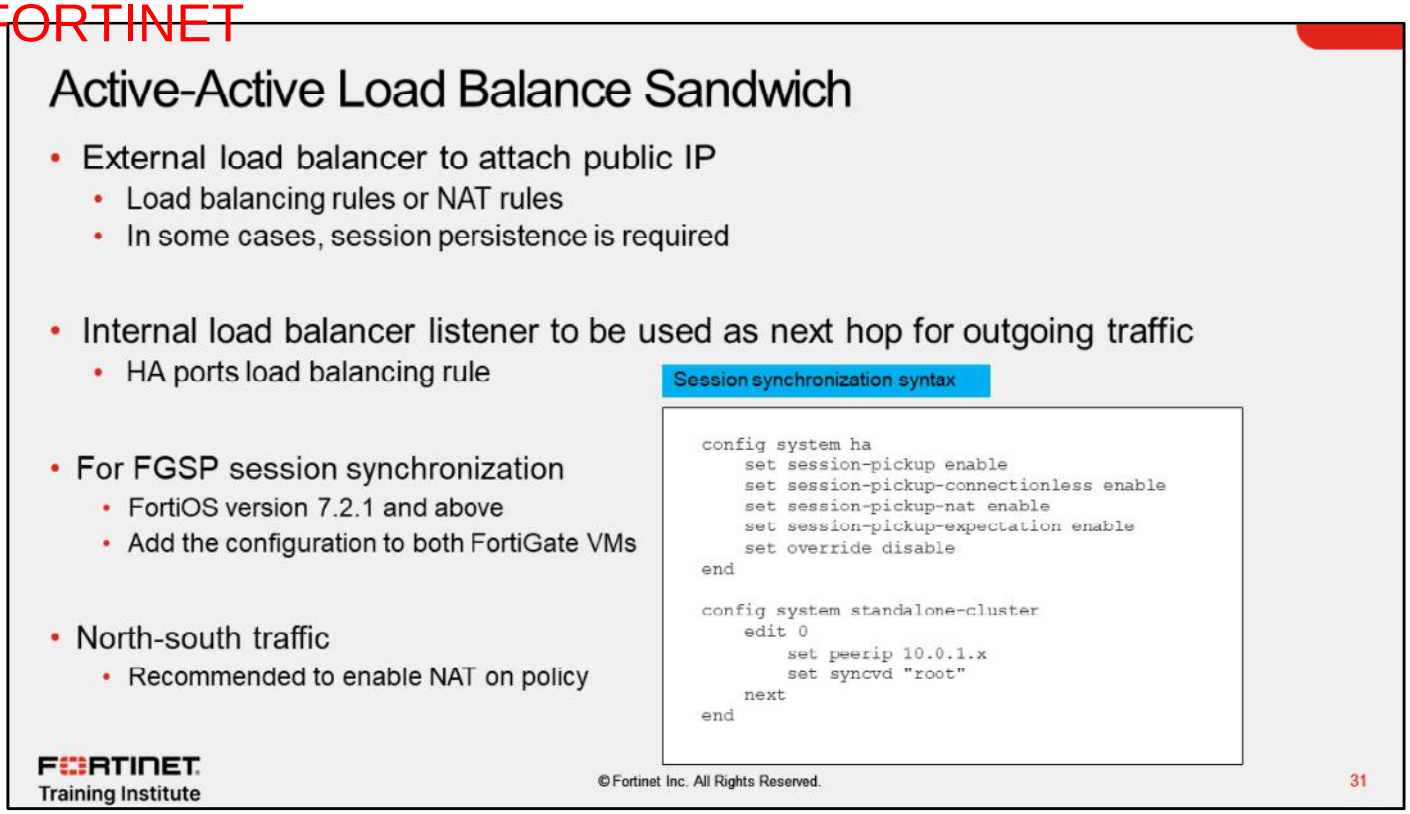
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

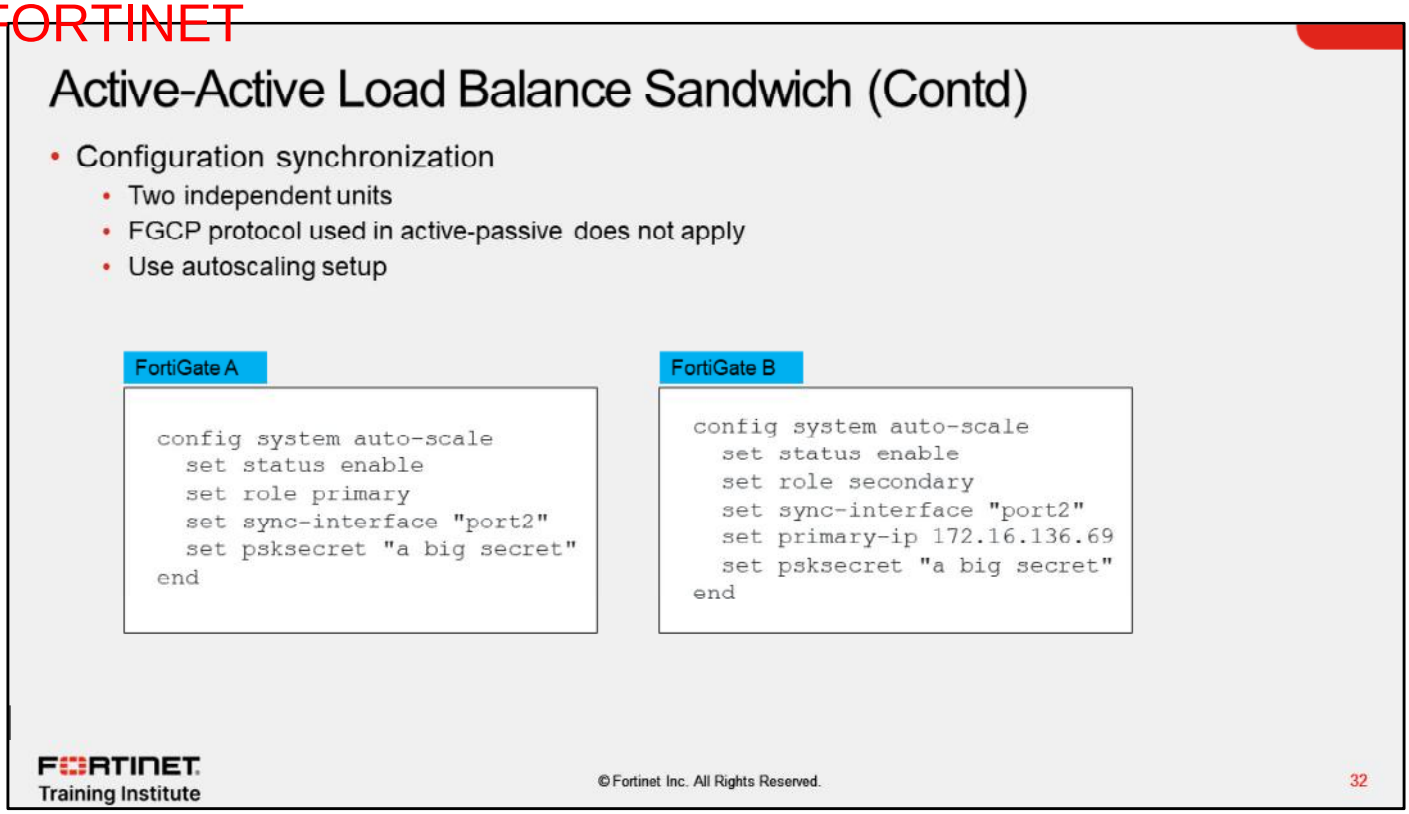
This is an example of an active-active load balance sandwich. The FortiGate VMs are, in this active-active setup, independent devices. In this setup, the Azure load balancer handles traffic failover using a health probe directed towards the FortiGate VMs. The public IP addresses are configured on the Azure load balancer, and provide ingress and egress flows with inspection from FortiGate. You can use FortiManager or local replication to synchronize configuration in this setup.

DO NOT REPRINT
© FORTINET



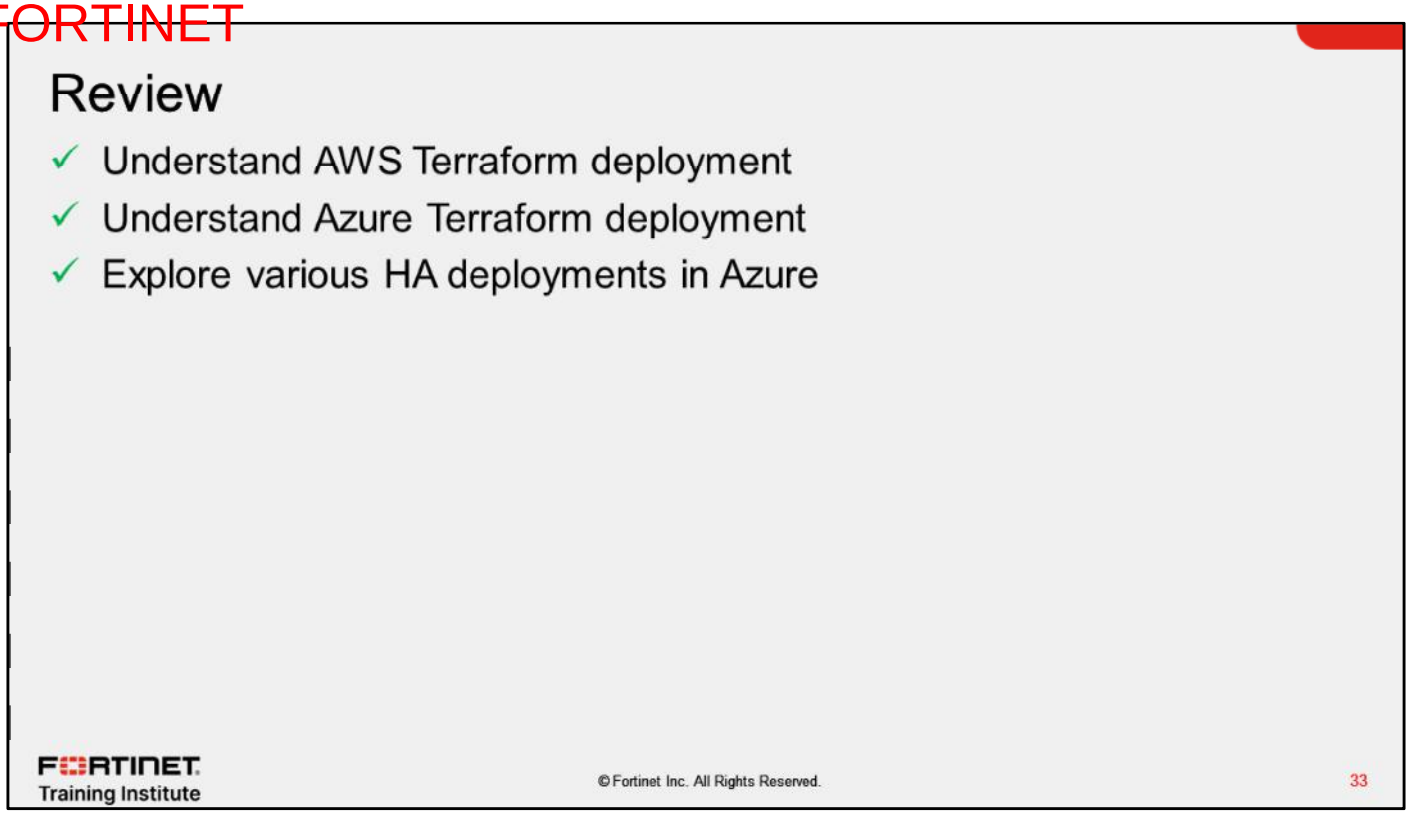
In the FortiGate active-active load balance sandwich scenario, the external load balancer has the public IP address with load balancing rules. The internal load balancer receives all internal traffic and forwards it to Azure gateways connecting ExpressRoute or Azure VPNs. When configuring the policies on the FortiGate devices to allow and forward traffic to internal hosts, it is recommended that you enable NAT. This will SNAT the packets to the IP address of port2) and enforce symmetric return. If you prefer to use FGSP for session synchronization, add the recommended configuration syntax shown on this slide to both FortiGate VMs. Note that the IP address `10.0.1.x` is the IP address of port 1 of the opposite FortiGate VM.

DO NOT REPRINT
© FORTINET



The FortiGate VMs in this active-active setup are independent devices. The FGCP protocol, used in the active-passive setup to sync the configuration, is not applicable here. You can use the autoscaling set up to enable configuration synchronization between both devices. This will sync all configurations except for the specific configuration item proper to the specific VM like hostname, routing and others. In order to enable the configuration sync use the commands shown on this example on both FortiGate VMs.

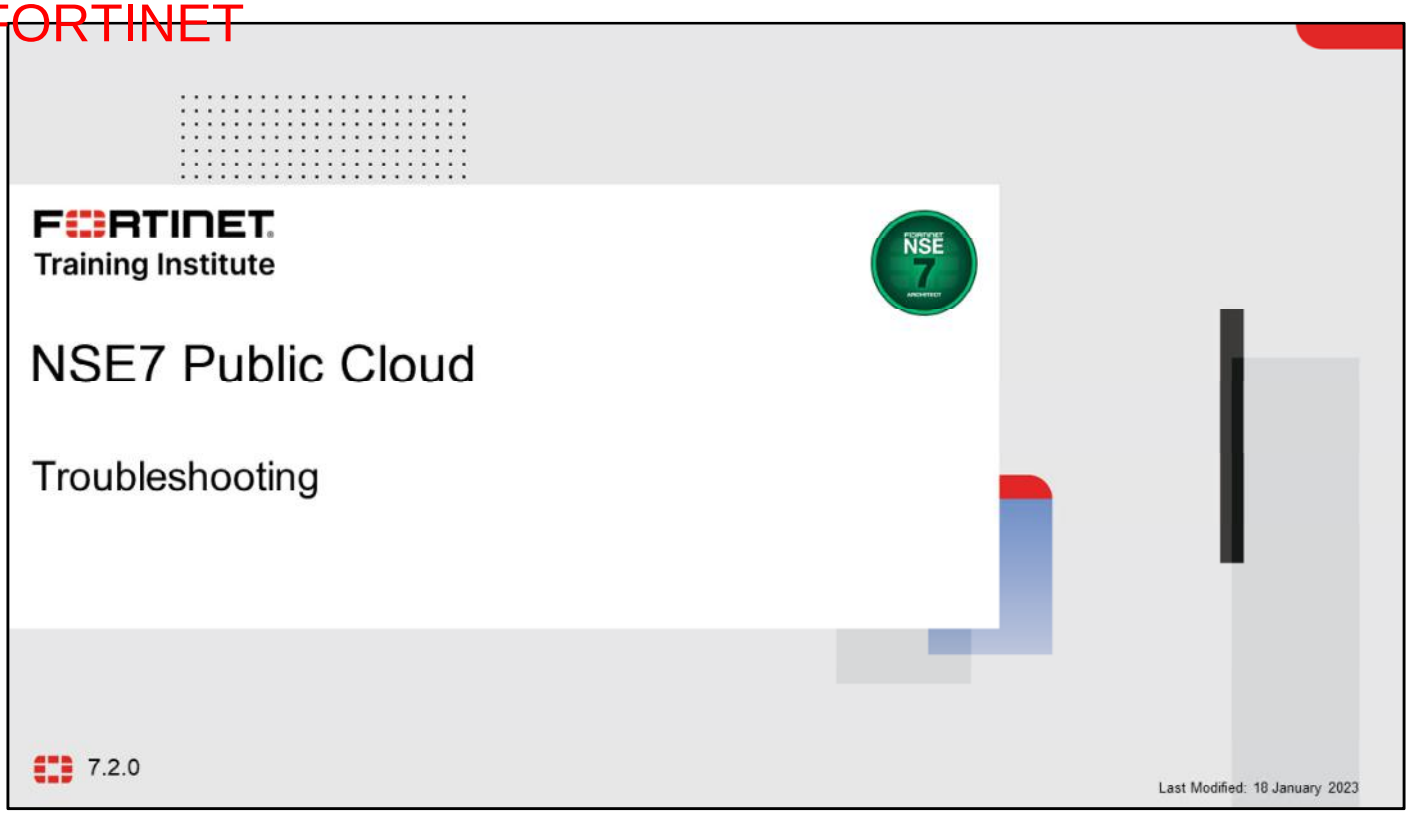
DO NOT REPRINT
© FORTINET



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

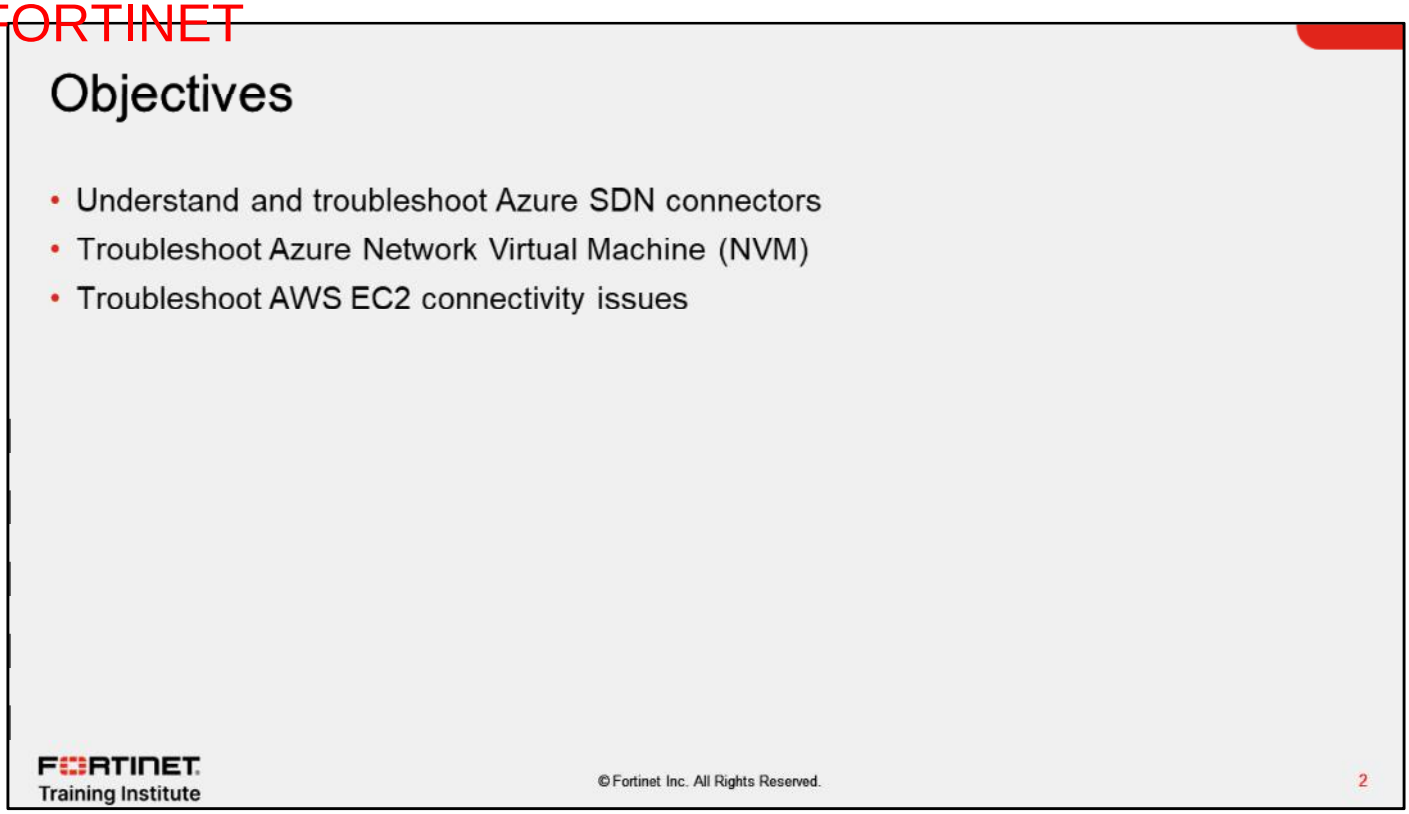
By mastering the objectives covered in this lesson, you learned about FortiGate deployment with Terraform.

DO NOT REPRINT
© FORTINET



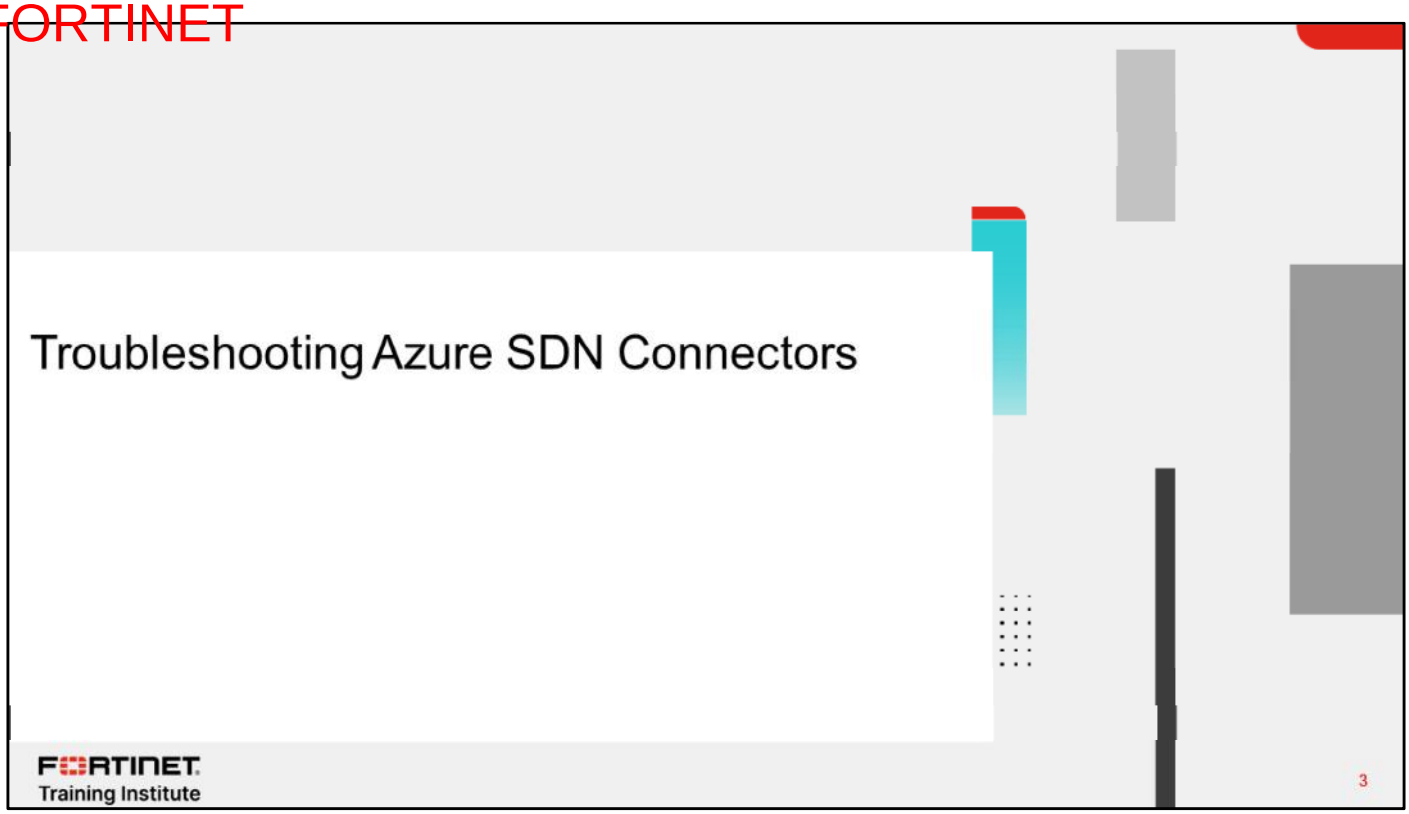
In this lesson, you will learn about public cloud troubleshooting.

DO NOT REPRINT
© FORTINET



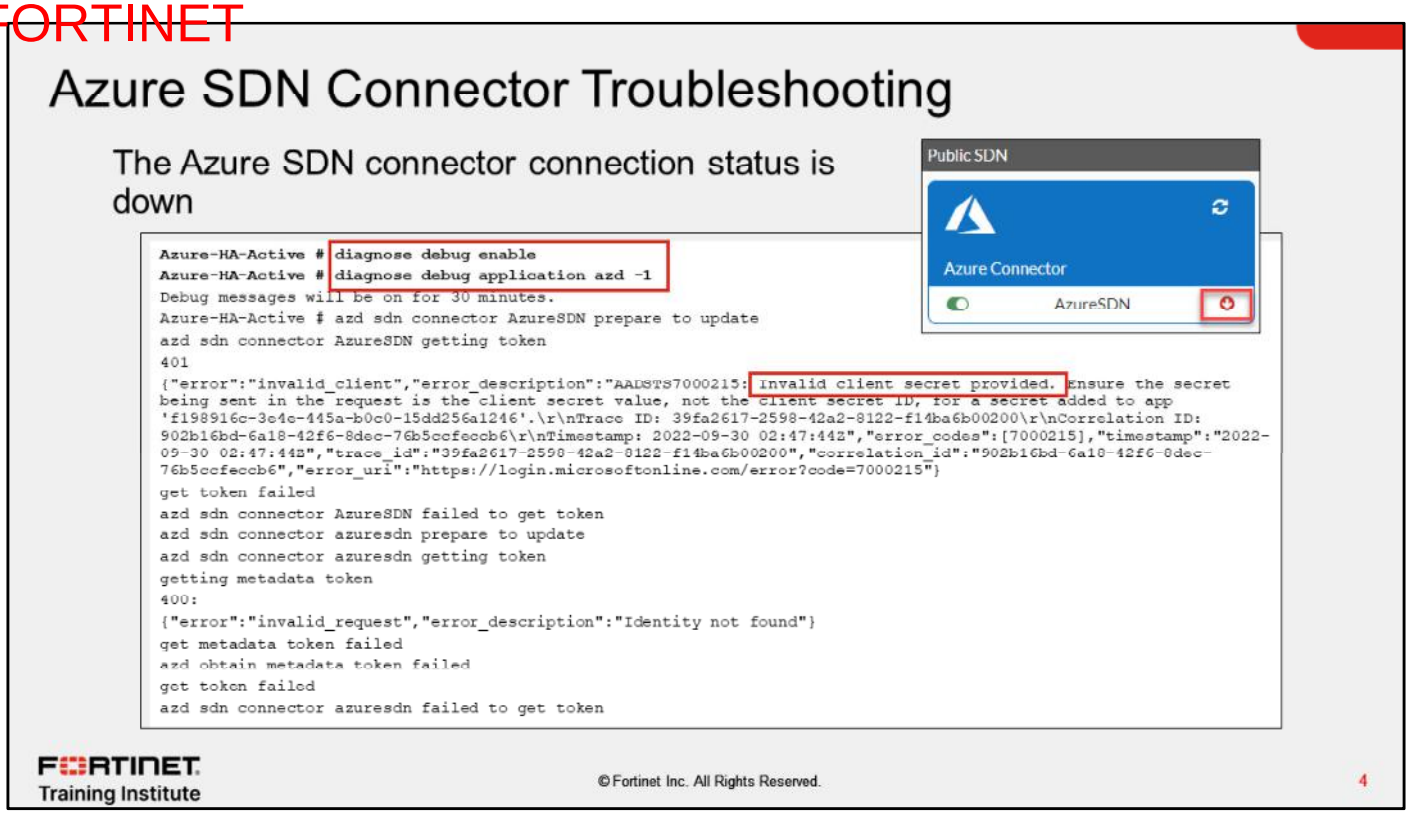
After completing this section, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn how to troubleshoot Azure SDN connectors.

DO NOT REPRINT
© FORTINET



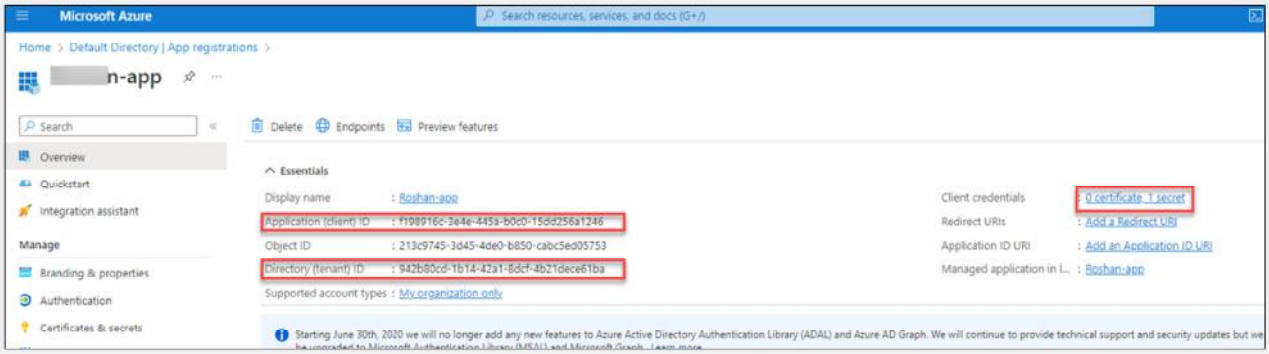
SDN connectors integrate and orchestrate Fortinet products with key SDN solutions. The Fortinet Security Fabric provides visibility into your security posture across multiple cloud networks, spanning private, public, and software-as-a-service (SaaS) clouds. In SDNs like Azure, dynamic objects and resources can be cumbersome to secure using traditional firewall policies. Using the fabric connector with Azure infrastructure-as-a-service (IaaS), FortiOS can update changes to attributes in the Azure environment, in the Security Fabric. This helps integrate and orchestrate FortiOS IPv4 policies going forward.

The example on this slide shows that the FortiGate Azure SDN Fabric Connector is not able to connect to Azure. The example shows that the Azure status is down. To troubleshoot SDN connector issues, the AZD debug command is used to troubleshoot the SDN connector issues and shows an invalid client secret was provided on the FortiGate SDN connector.

DO NOT REPRINT
© FORTINET

Azure SDN Connector Troubleshooting (Contd)

- Azure client secret must be obtained during the initial creation
- If not, create a new client secret, then use the new secret for configuration
- Does the registered app have access to the resource group?



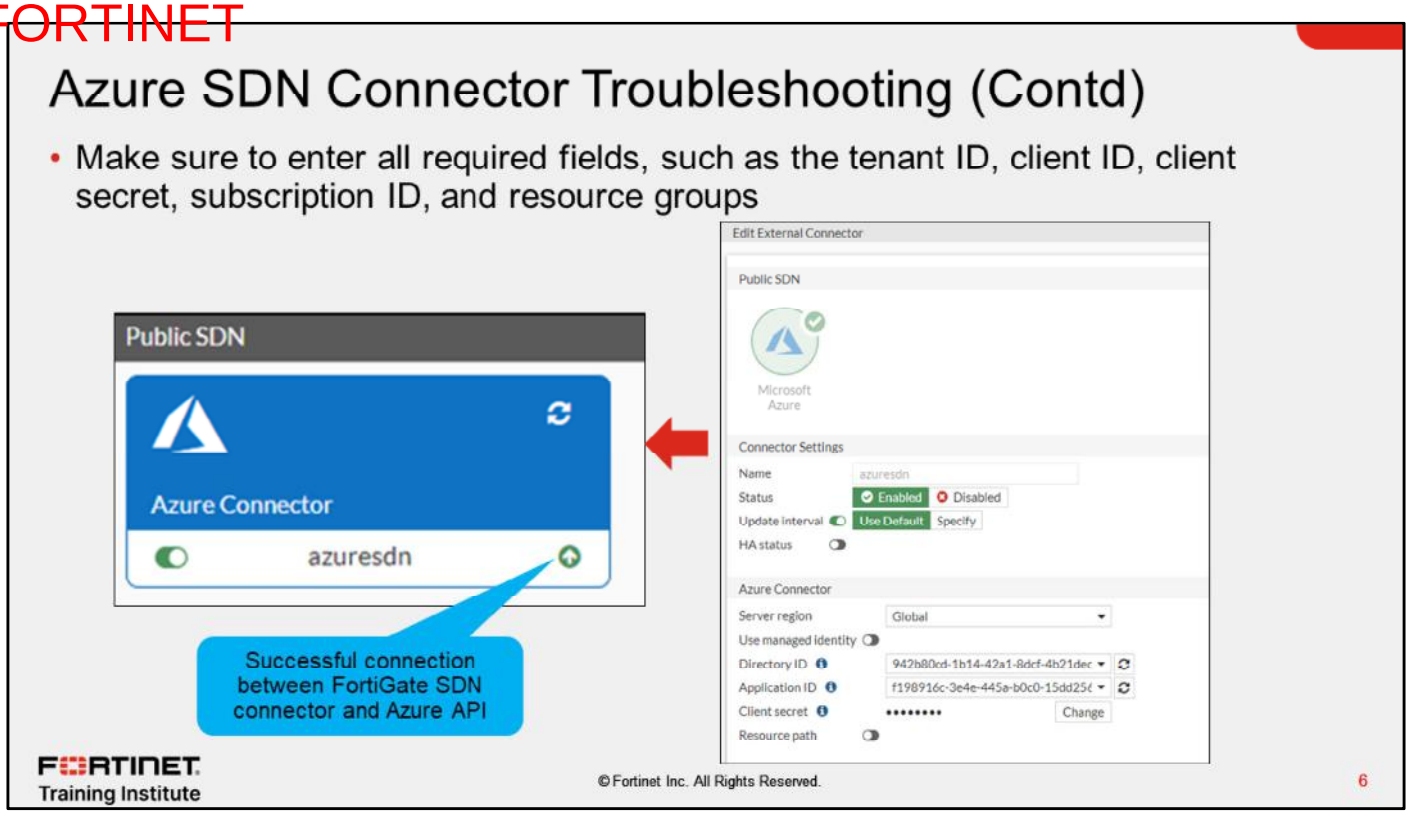
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

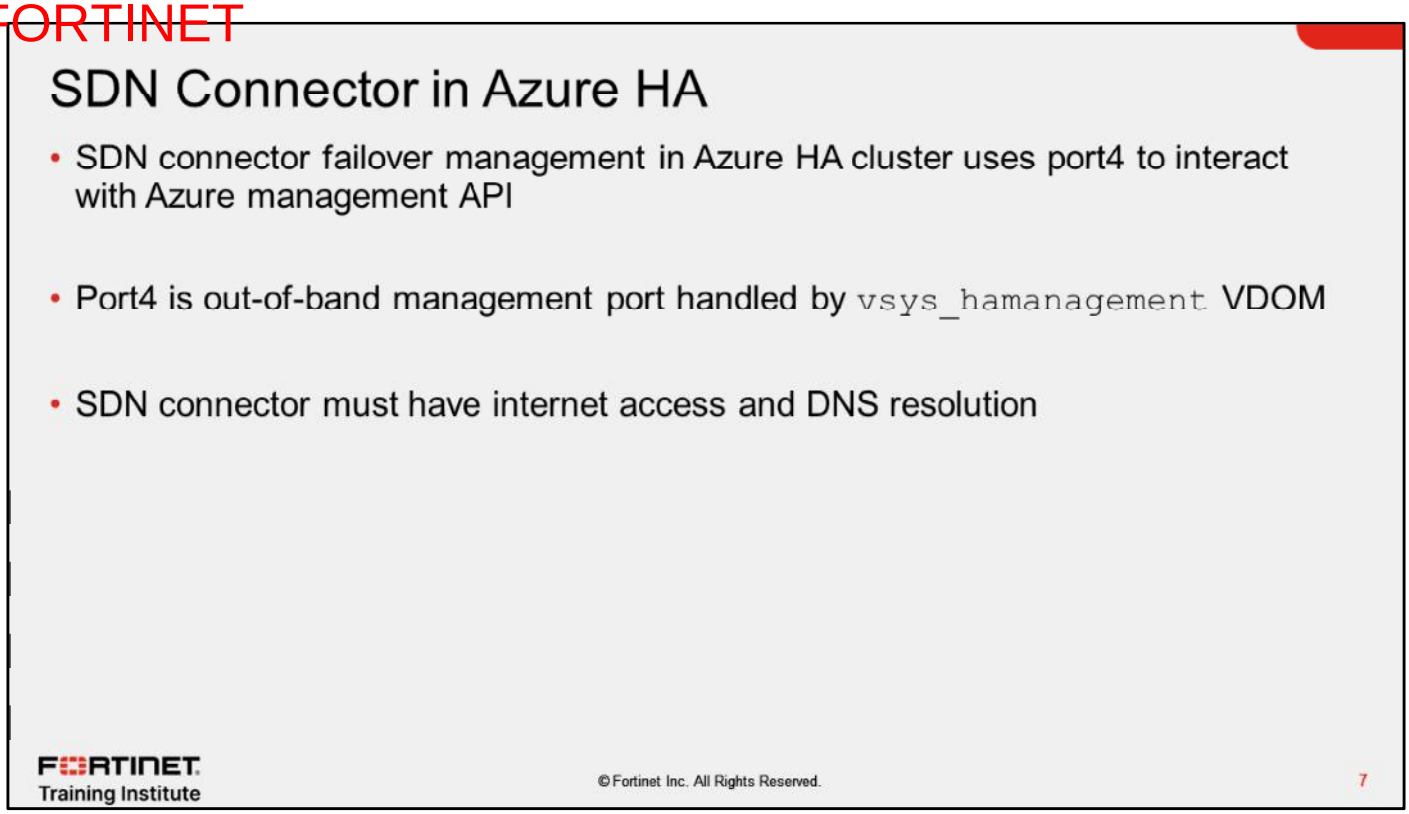
The client secret from the Azure portal is needed during the FortiGate SDN connector configuration. It is important to note the client secret during the initial stage of creating the secret. The old secret will not be visible at a later time, so you must create a new secret to replace the old one. Also, you must ensure that registered applications have access to the resource group. The steps shown in this example are very important to create a successful connection between FortiGate SDN connector and Azure API management components.

DO NOT REPRINT
© FORTINET



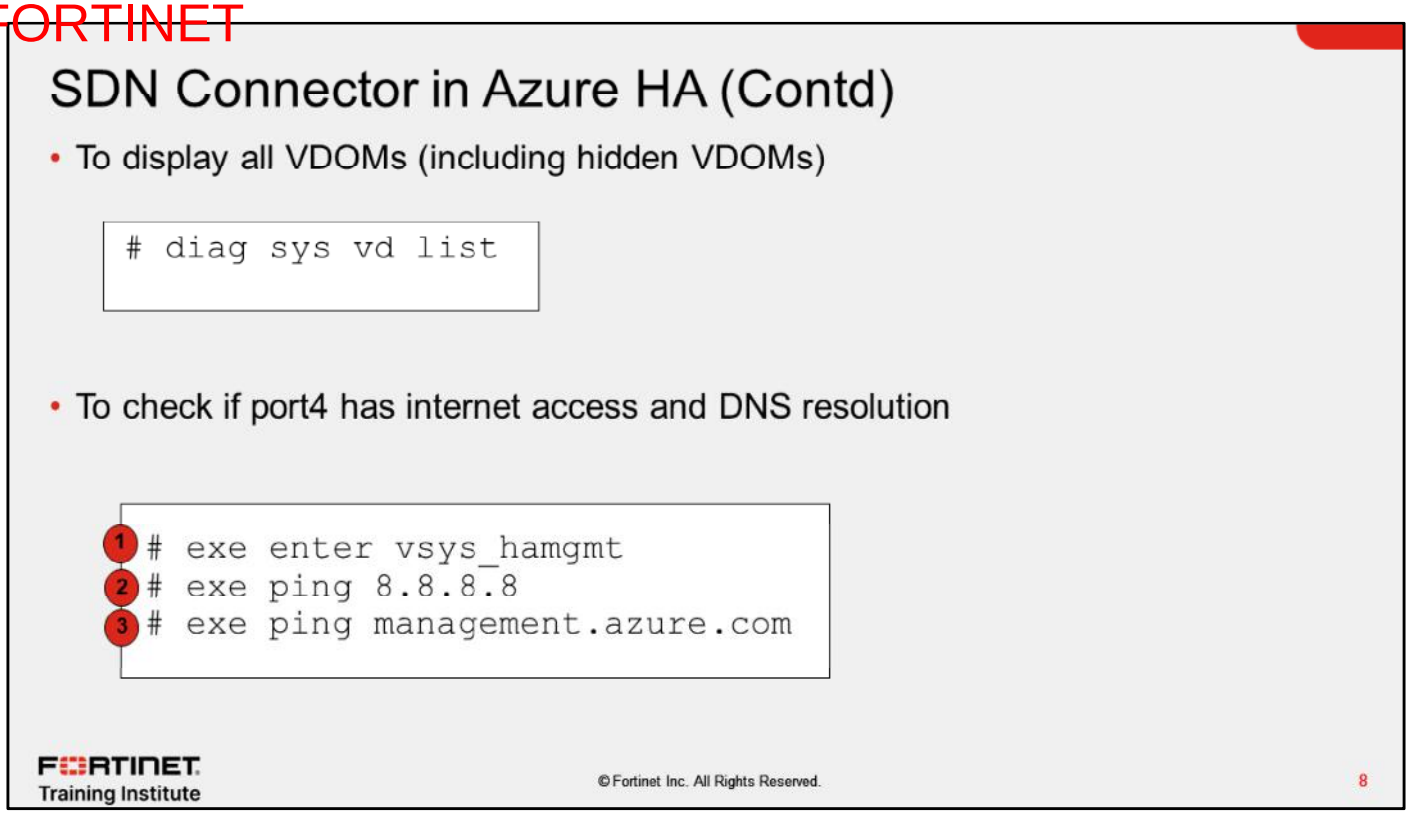
After you have successfully configured the fabric connector, the indicator turns green and the CLI output no longer shows an error when enabling and disabling the fabric connector.

DO NOT REPRINT
© FORTINET



When you do the SDN troubleshooting, it is important to understand how the FortiGate SDN fabric connector initiates a connection to the Azure management API. The SDN connector failover management in the Azure HA cluster is using `port4 to` interact with the Azure Management API. In the SDN connector in the Azure HA cluster, port4 is set to an out-of-band management port that is not handled by the root VDOM but by the vsys_hamgmt. Since port4 is set as an out-of-band management port, the interface cannot be used for routing or policies. You also cannot ping this interface from FortiGate.

DO NOT REPRINT
© FORTINET



During troubleshooting, you may want to see all VDOMs including the hidden VDOMs on FortiGate to make sure the correct VDOMs are assigned to the ports. Use the `diag sys vd list` command to list all the VDOMs first. Next, use the three commands shown on this slide to check if port4 has internet access and DNS resolution. During the connection between the SDN connector and Azure API management, there are many queries made by the SDN connector to the Azure API management. The first query of the SDN connector is targeted to special address `169.254.169.254` to get a token in order to interact with the Azure management API. The other queries are made to manage public IP address and route tables in case failovers are targeted to `management.azure.com` using the token from the first query.

DO NOT REPRINT
© FORTINET

Azure HA VM Floating IP Issue

- The floating IP address does not shift from the previous primary FortiGate device

```
Azure-HA-Passive # diagnose debug application azd -1
Debug messages will be on for 30 minutes.
Azure-HA-Passive # diagnose debug enable
FGT-HA-Slave # azd running in secondary mode, will notupdate
HA event
HA state: primary
azd sdn connector 'AZ-Connector' getting token
size: 1268
token expire in: 3600 seconds
AZ-Connector: resourcegroup: NSE7-HA-RG, sub: "<Removed string>"
Disable interface: port1
Disable interface: port2
get pubip FGTAPClusterPublicIP in resource group NSE7-HA-RG
azd api failed, url
=https://management.azure.com/subscriptions/<Removed String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddres
ses/FGTAPClusterPublicIP?api-version=2022-06-01, rc = 403.
{"error":{"code":"AuthorizationFailed","message":"The client '<Removed String>' with obj
ect id '<Removed String>' does not have authorization to perform action
'Microsoft.Network/publicIPAddresses/read' over scope '/subscriptions/<Removed
String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddresses/FGTAPClusterPublicIP' or the scope is
invalid. If access was recen
tly granted, please refresh your credentials."}}
```

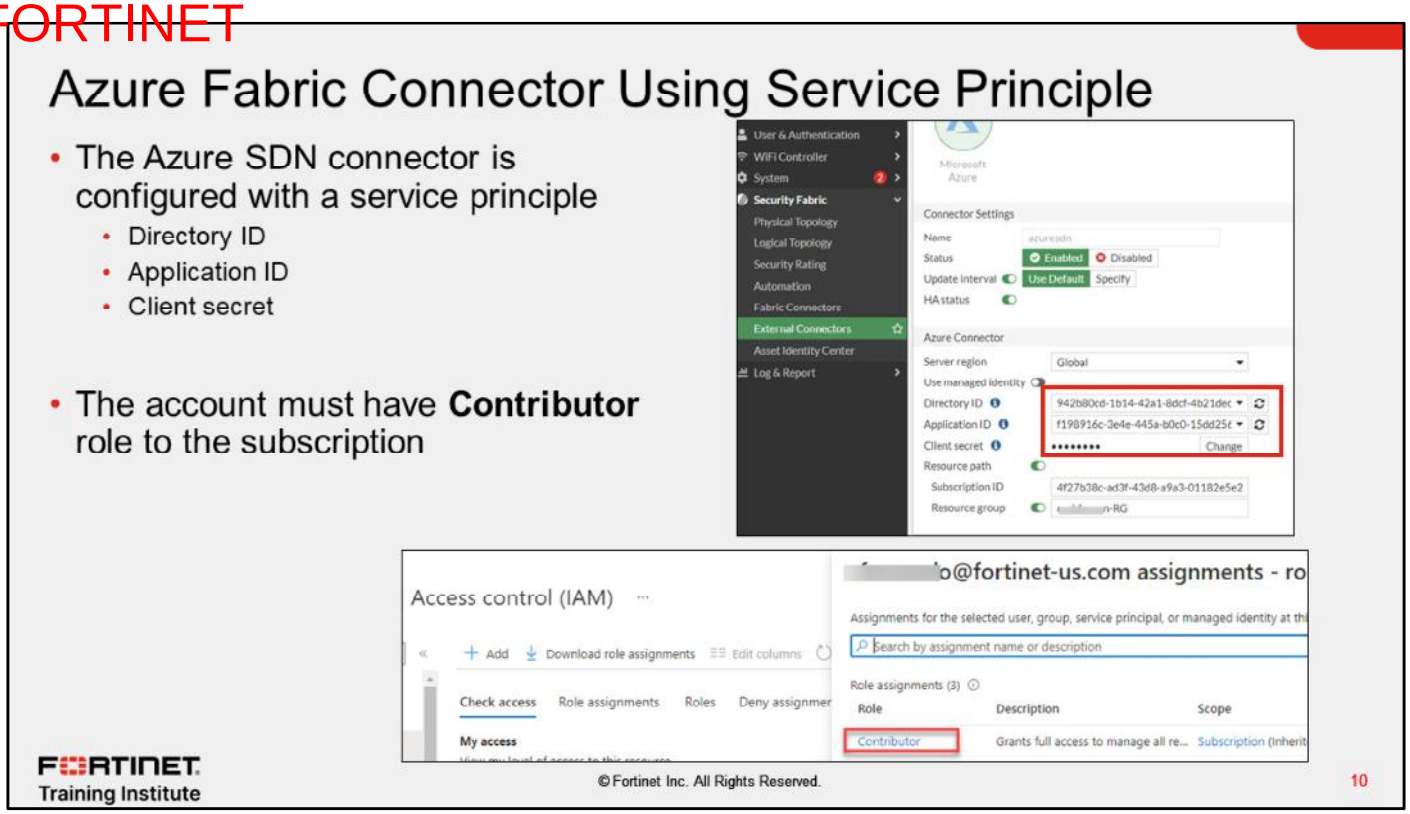
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

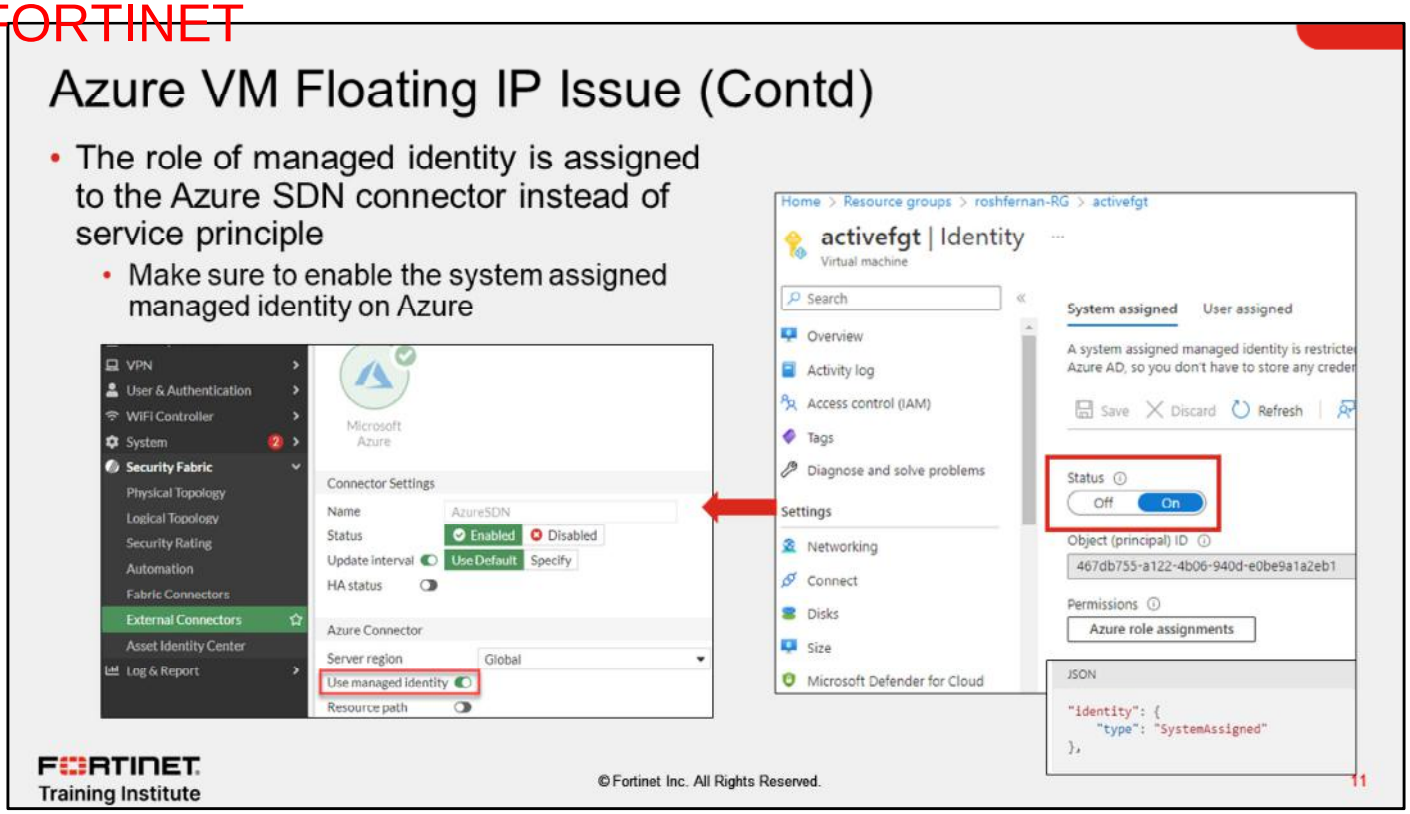
An administrator is troubleshooting an issue: the floating IP address from the previous primary device is not shifting to the secondary device during the HA failover event. So, the administrator performs the AZD debug and can see the `403 AuthorizationFailed` message error message.

DO NOT REPRINT
© FORTINET



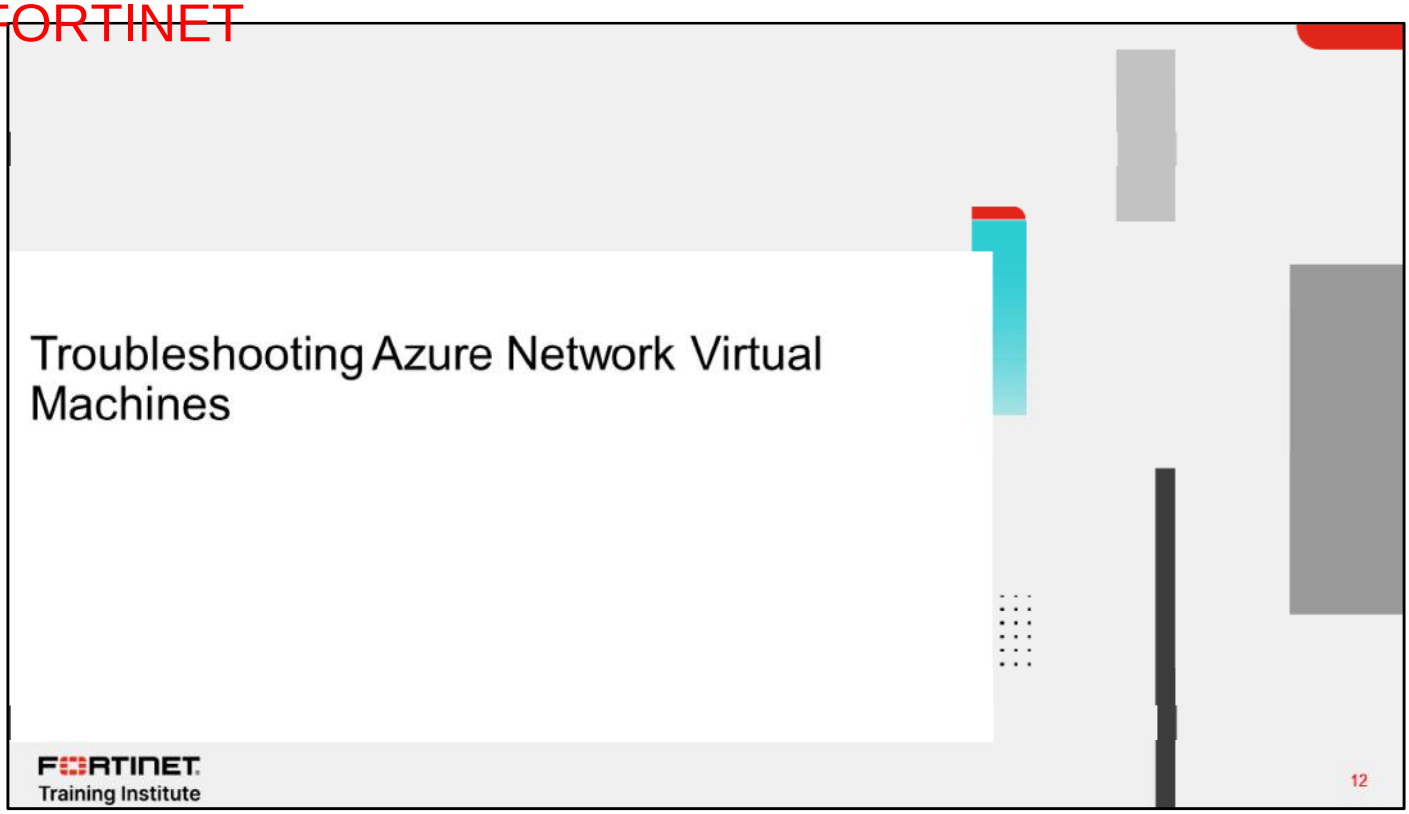
What was the issue with the floating IP not shifting from the previous primary device? In this scenario, the Azure SDN connector is configured with a service principle, however, proper permission is not assigned to the service principle account. In order to resolve the issue, you must assign the **Contributor** role to the subscription.

DO NOT REPRINT
© FORTINET



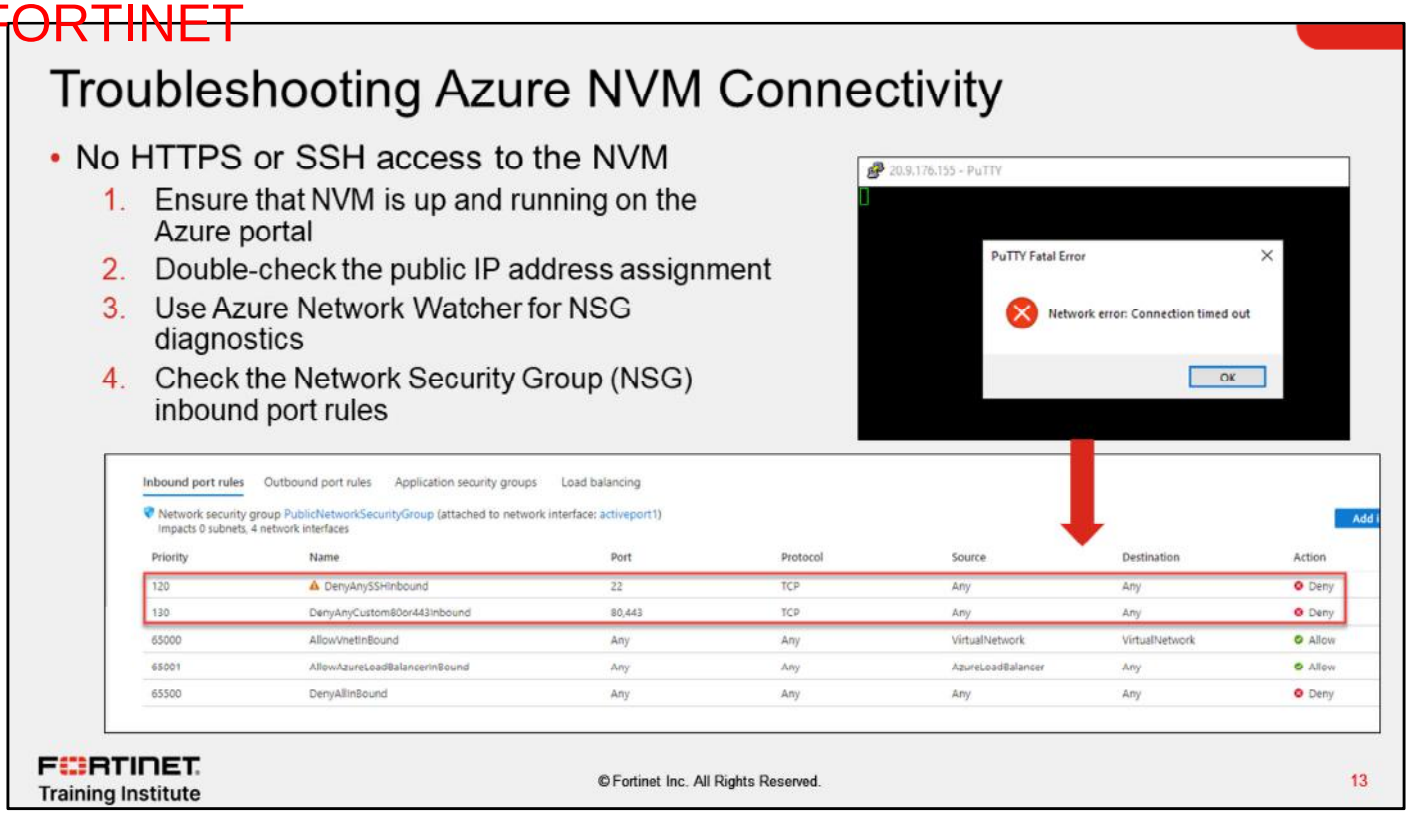
What if the Azure SDN connector is configured with the managed identity? The example on this slide shows the Azure SDN connector with the role of managed identity instead of the role of service principal. In this scenario, make sure the that system-assigned managed identity is turned on the Azure side.

DO NOT REPRINT
© FORTINET



In this section, you will learn how to troubleshoot Azure network virtual machines (NVMs).

DO NOT REPRINT
© FORTINET

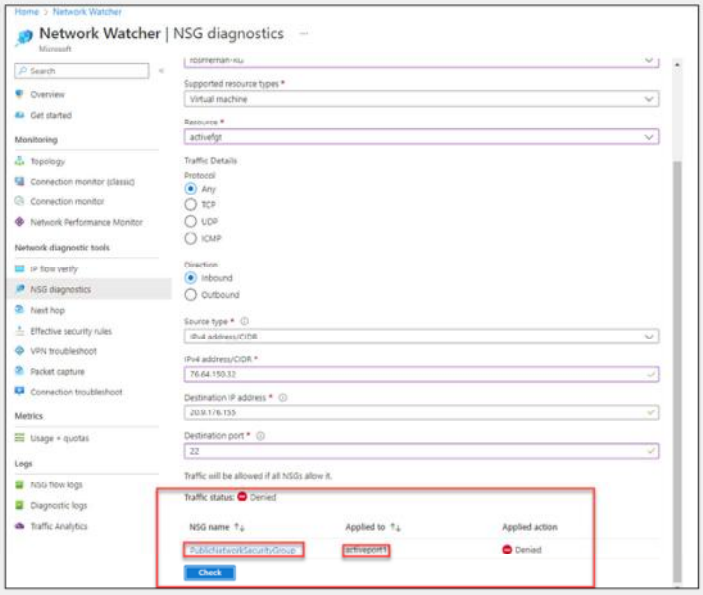


Azure NVM connectivity troubleshooting is similar to the AWS EC2 troubleshooting. As a rule of thumb, check if the NVM is up and running, and has a public IP address assigned. Next, check the NSG and make sure that the inbound port rule is not blocking any traffic.

DO NOT REPRINT
© FORTINET

Azure Network Watcher

- Use Azure Network Watcher to troubleshoot NSG issues
  - Provide the necessary details, such as resource group, source and destination IP addresses
  - Check the status and see if the traffic is denied or allowed
  - Useful when troubleshooting complex network environments



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

Azure Network Watcher can help you troubleshoot NSG issues. This tool is especially handy when you troubleshoot issues in big, complex networks. Azure Network Watcher uses your input to find issues.

DO NOT REPRINT
© FORTINET

Troubleshoot NVM

- Delete any inbound port rules that are preventing access

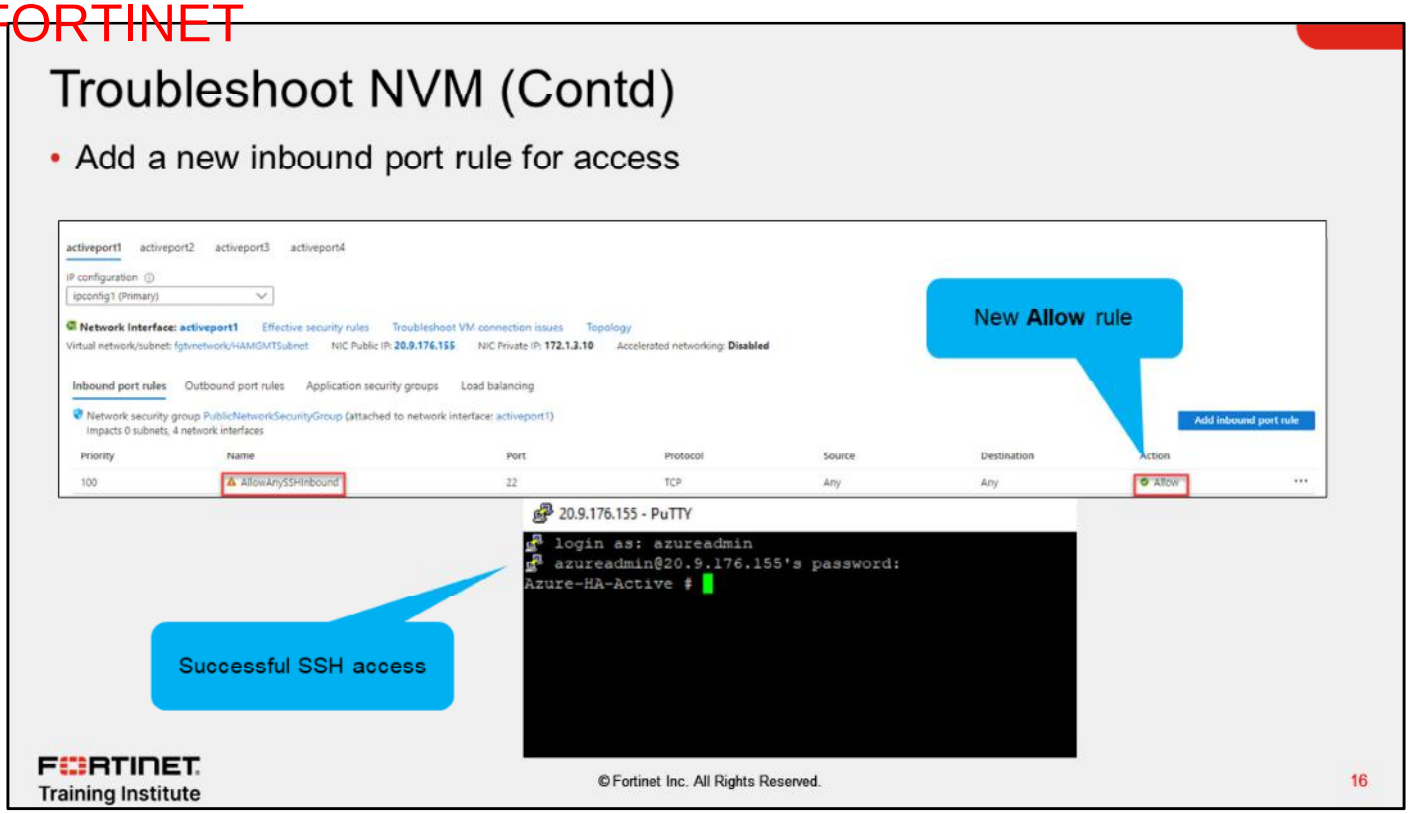
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

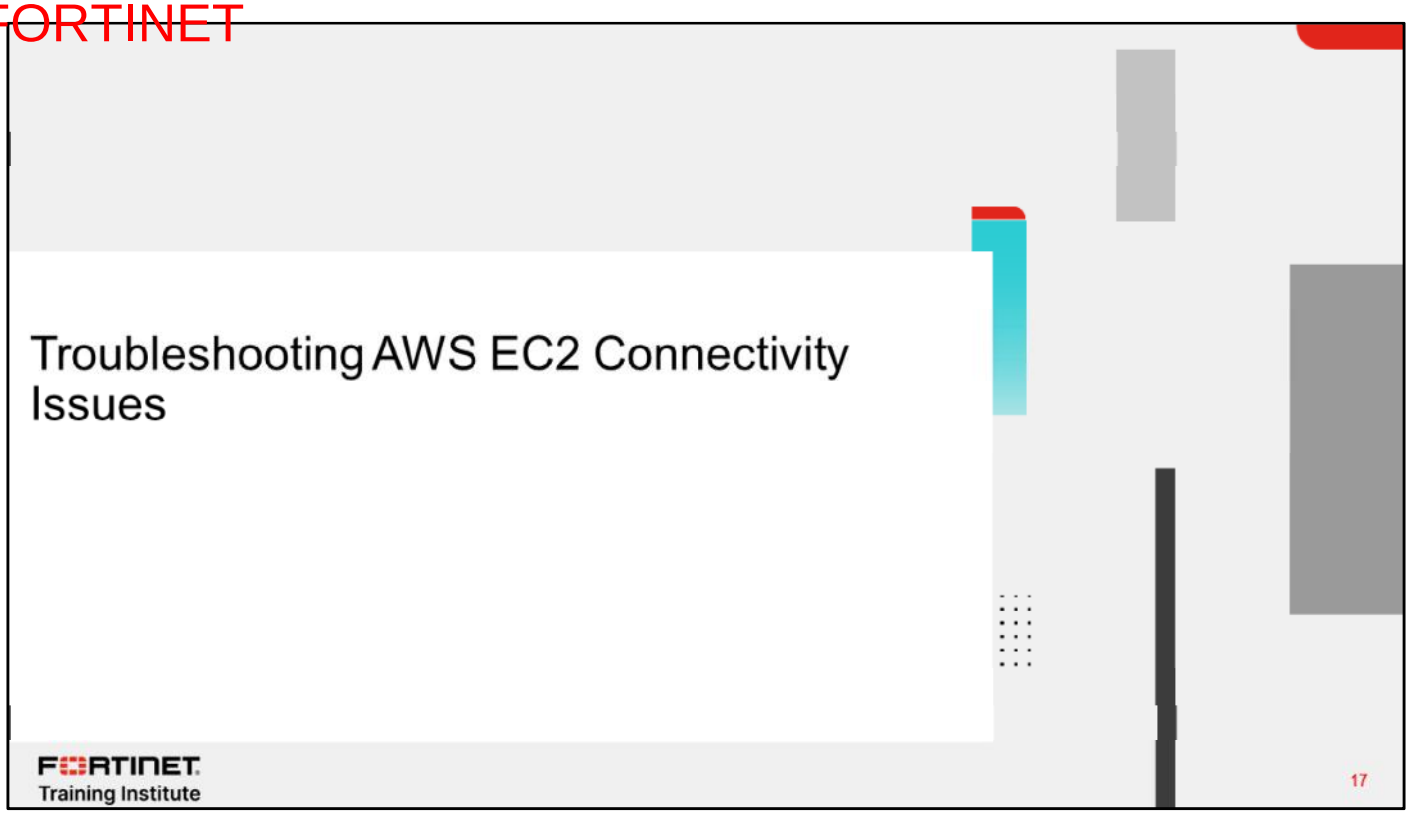
After you find the issue, you can delete the rule that was blocking access and add a new rule that will allow traffic.

DO NOT REPRINT
© FORTINET



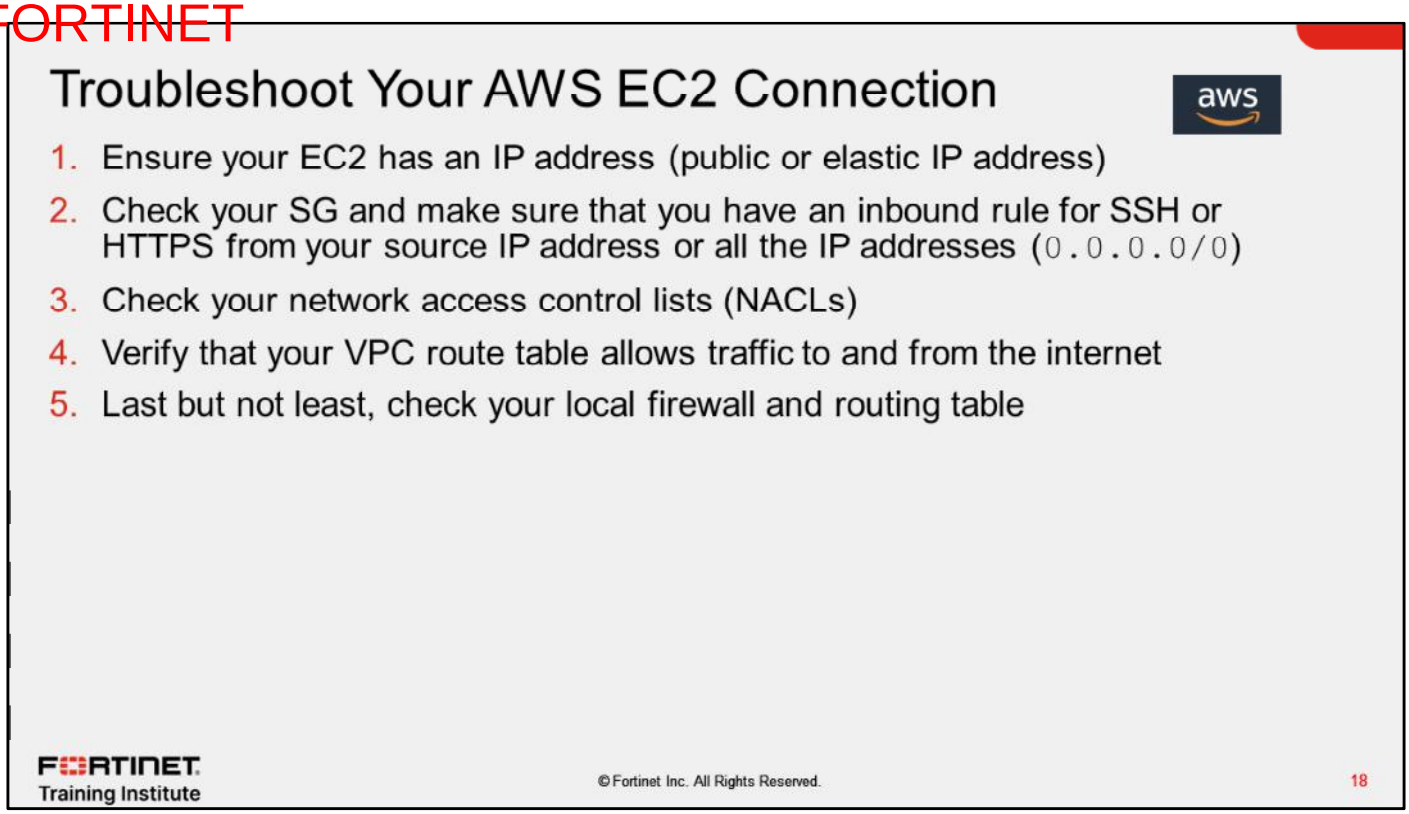
After you find the issue, you can delete the rule that was blocking access and add a new rule that will allow traffic.

DO NOT REPRINT
© FORTINET



In this section, you will learn how to troubleshoot AWS EC2 connectivity issues.

DO NOT REPRINT
© FORTINET

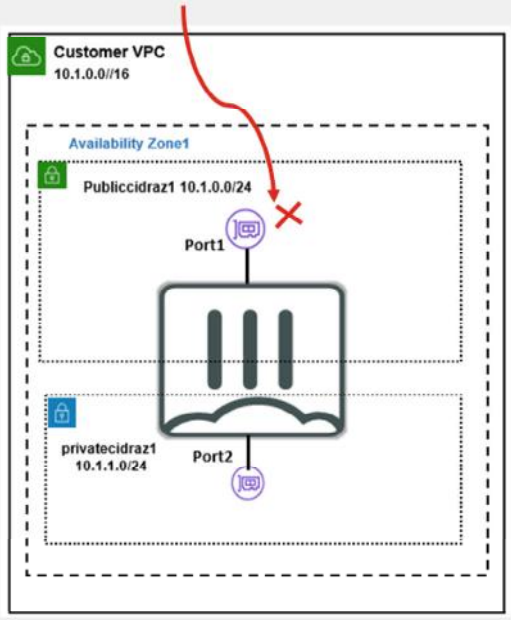


There is a checklist of items that you can go through when you are troubleshooting EC2 connectivity issues. Usually, connectivity issues occur when SG or network ACLs are blocking traffic. First, make sure that your EC2 instance has a public IP address or an elastic IP address. Check your SGs, NACLs, route tables, and local firewall and routing tables.

DO NOT REPRINT
© FORTINET

Troubleshoot EC2 Internet Connectivity

- You have deployed a FortiGate VM on a newly created VPC, however, you cannot access the VM from the internet
  - The SG has the correct inbound rule and no issues with ACL
  - The FortiGate sniffer capture shows no incoming traffic to the VM
- What could be causing the access issue?
  - The sniffer shows that no incoming traffic from your source IP address is reaching the VM, so there is no need to troubleshoot the FortiGate VM



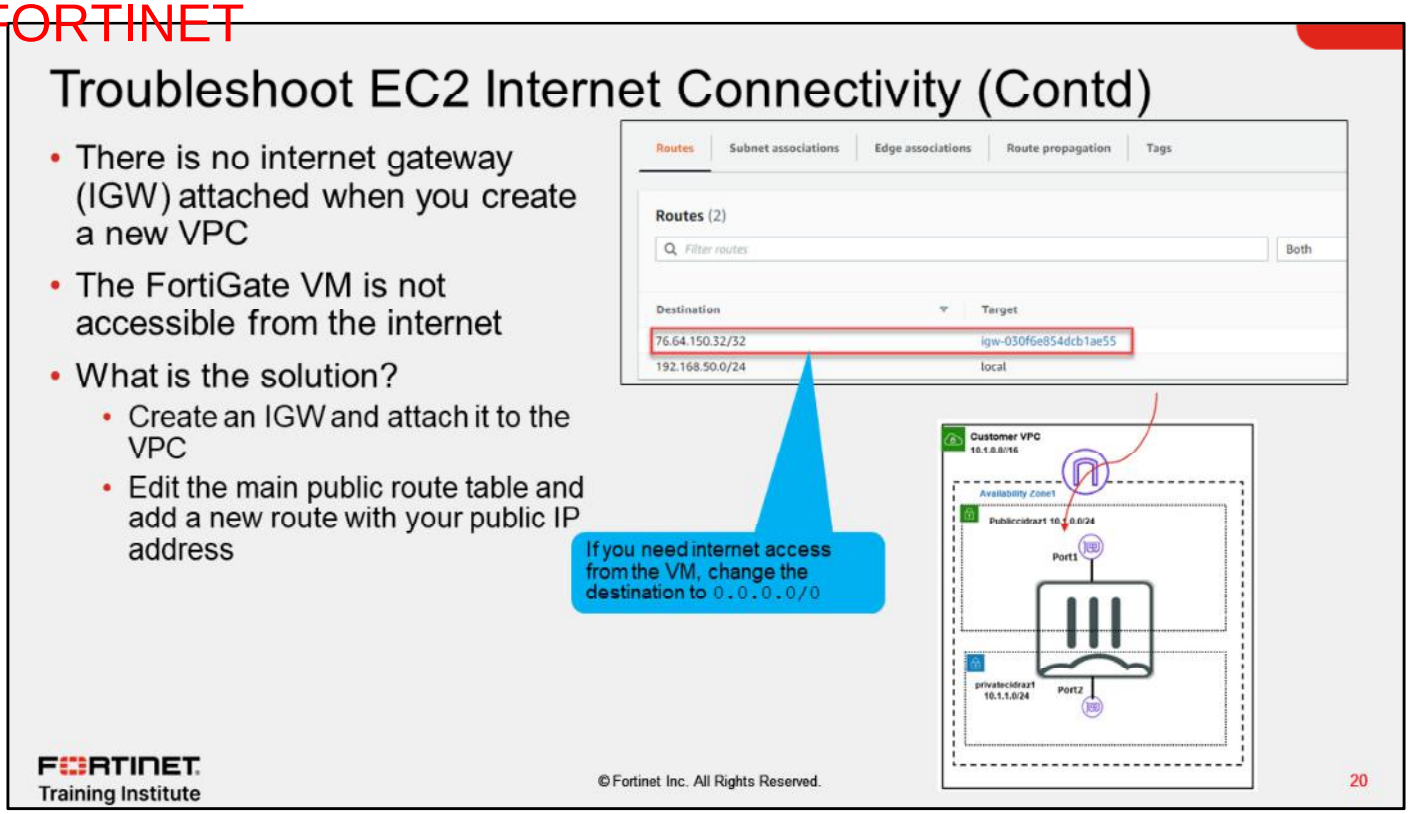
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

After deploying a FortiGate VM on a new VPC, the administrator notices that there is no `HTTPS` or `SSH` connectivity to the VM. The sniffer shows that there is no traffic FortiGate and so there is no need do further troubleshooting on the FortiGate VM. Also, there are no issues with the AWS SG.

DO NOT REPRINT
© FORTINET

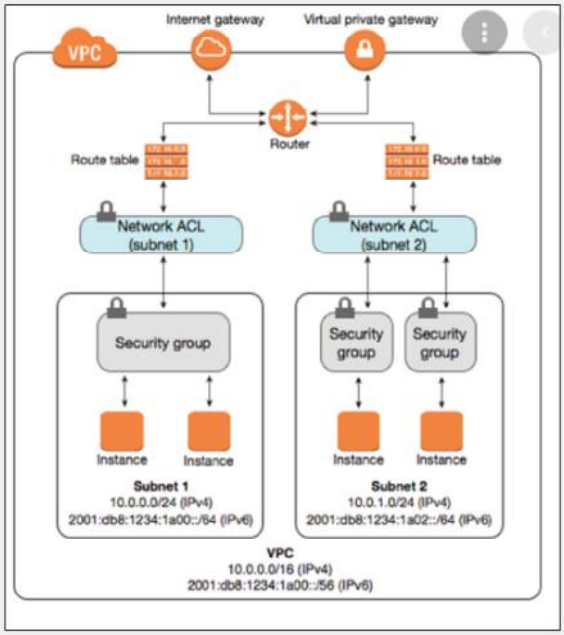


When checking the VPC, the administrator finds that there is no IGW attached to the VPC. The administrator can create a new IGW, attach it to the VPC, and then create a route with the administrator`s local public IP address and destination to the IGW. However, this issue only occurs when you create a new VPC and deploy an EC2 instance on it. The AWS default VPC has an IGW attached. So, If the administrator deploys an EC2 instance on the default VPC, the EC2 instance will have internet access automatically.

DO NOT REPRINT
© FORTINET

AWS Network Access Control Lists

- NACLs are another place to check during connectivity troubleshooting
- NACLs are applicable at the subnet level and are automatically assigned



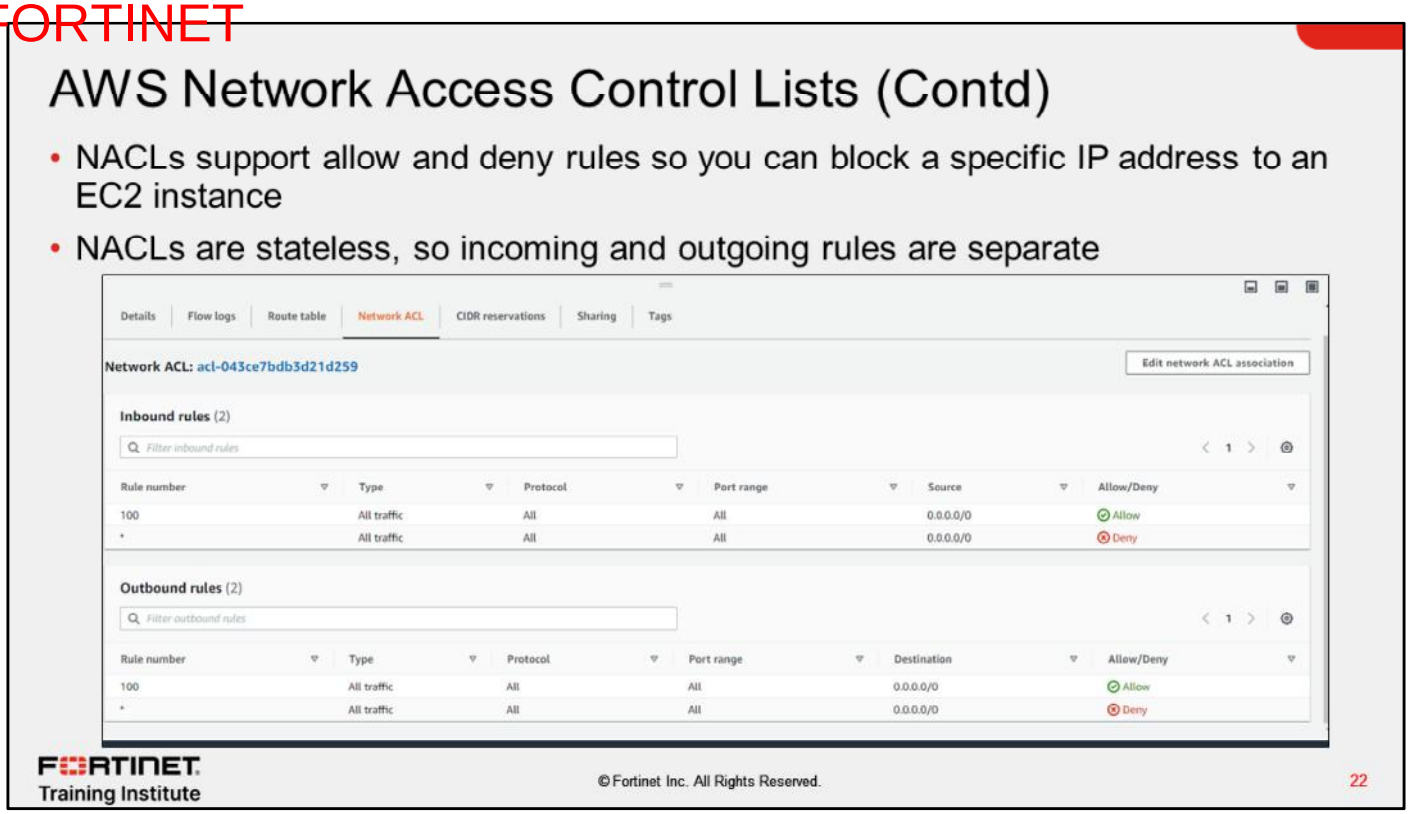
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

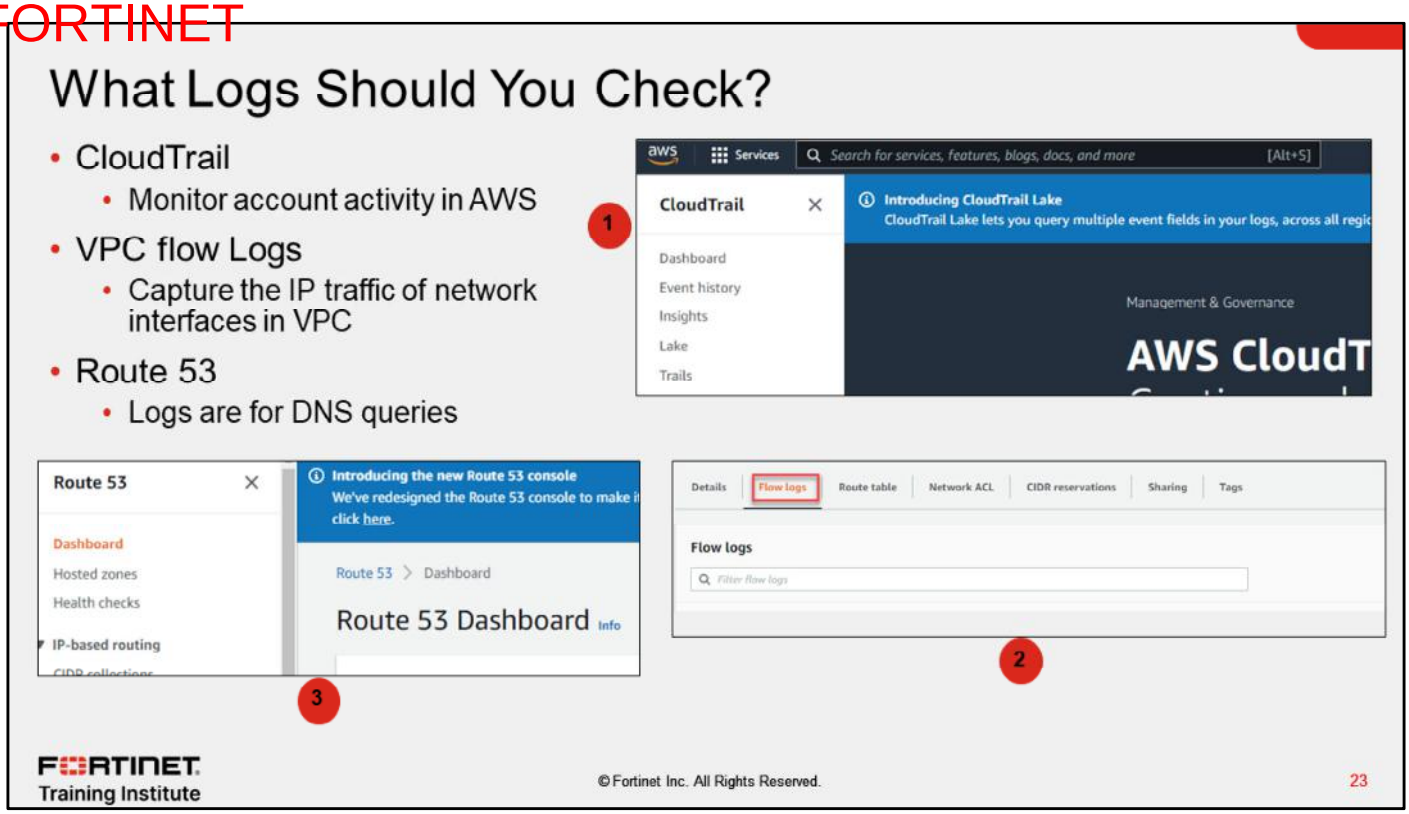
The example on this slide shows some AWS NACL details. If you are troubleshooting a connectivity issue to an instance, NACL is one of the places you should check. Any instance of a subnet with an NACL has the NACL rule applied automatically. However, in the case of a security group, the security group has to be applied to the instance.

DO NOT REPRINT
© FORTINET



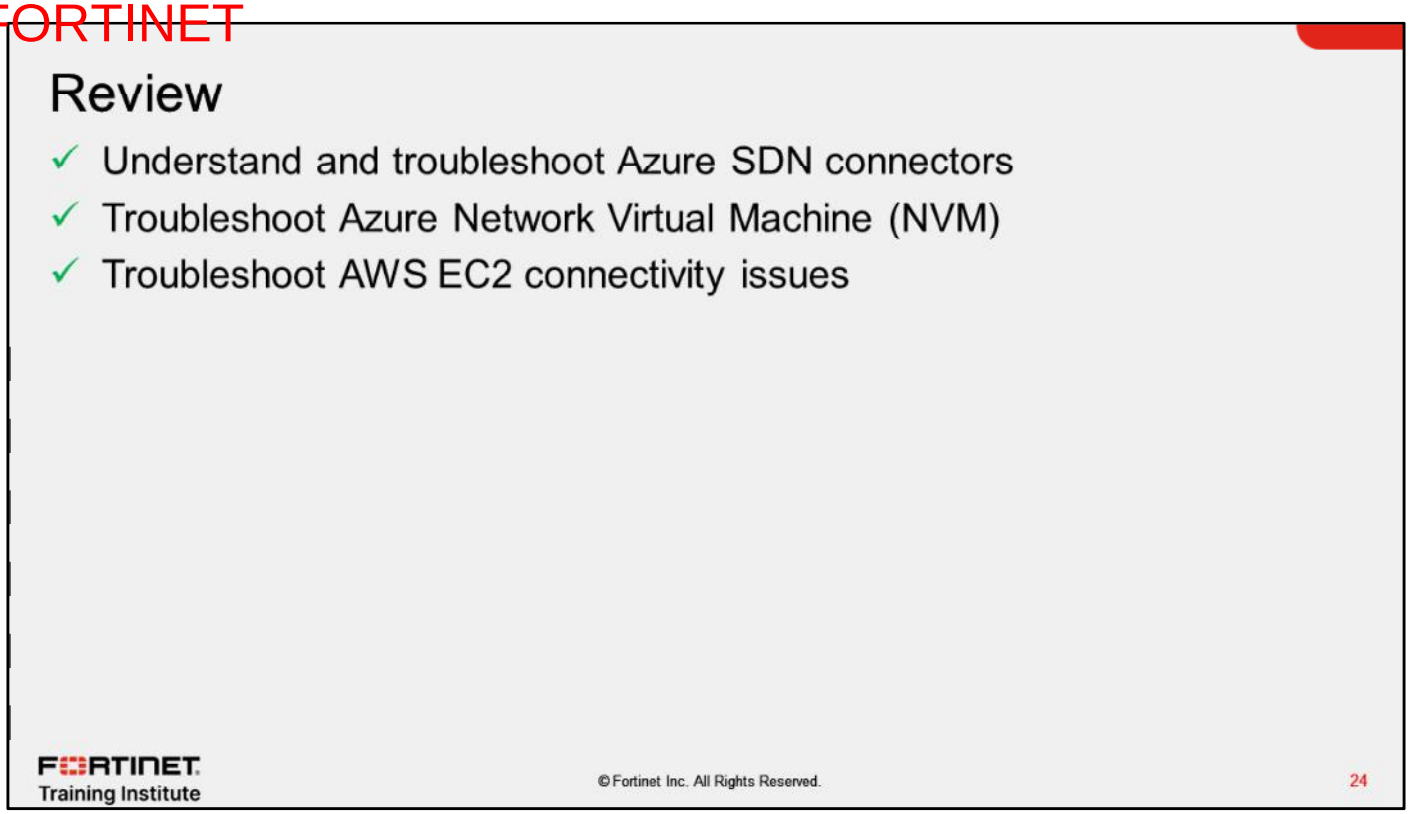
Unlike security groups, NACLs are stateless, thus, incoming and outgoing rules are separate. So any change applied to an incoming rule is not automatically applied to an outgoing rule. You can use NACLs to block a specific IP address to an EC2 instance and use it in subnet level. It is important to know some key components of NACLs. Every rule is assigned a unique number. The rules are applied in the order of their priority, where the priority is indicated by the number the rule is assigned.

DO NOT REPRINT
© FORTINET



There are few other places that you can check on AWS. The CloudTrail monitors and retains account activity related to actions in AWS. The VPC flow logs capture IP traffic going to and from your network interfaces in VPC.

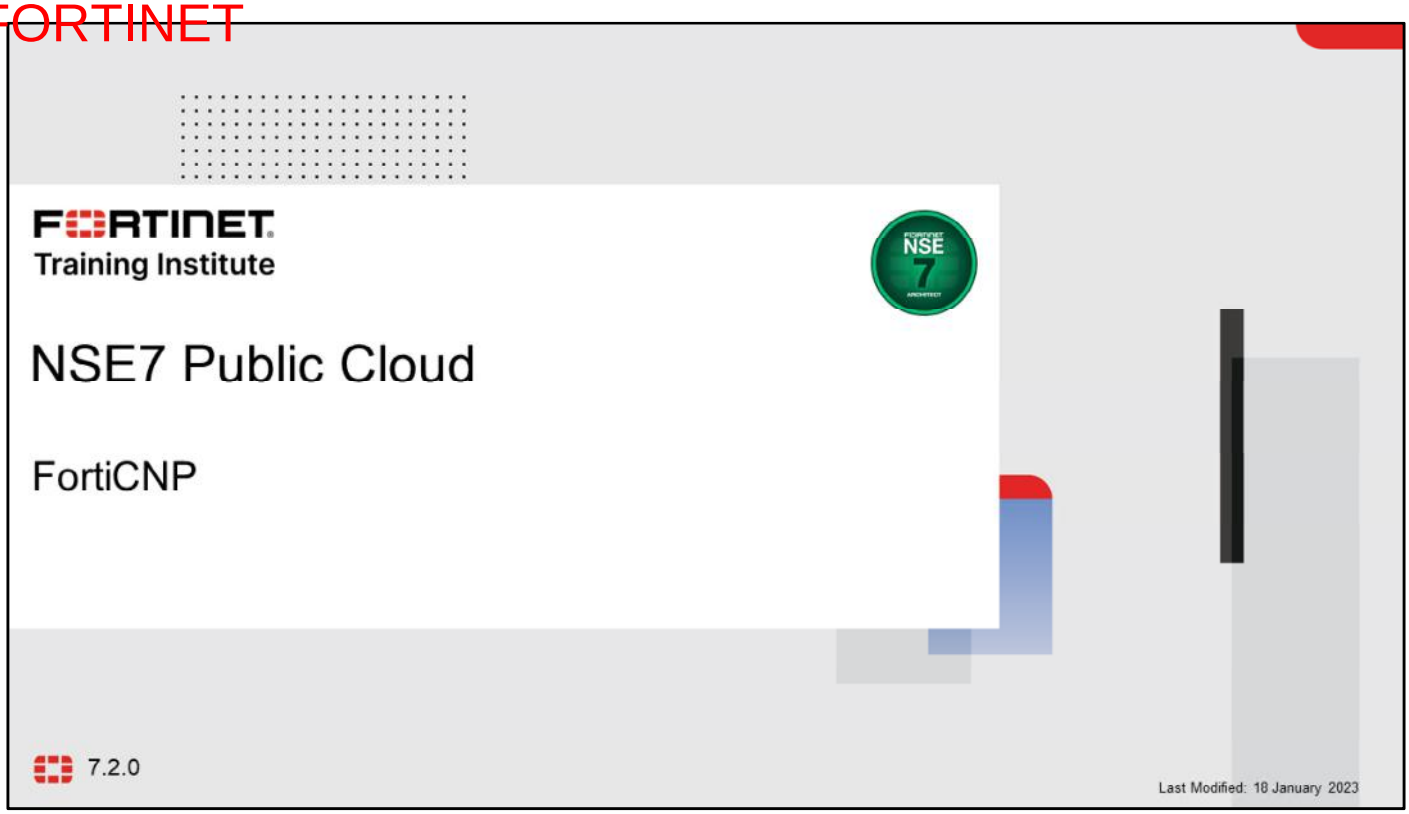
DO NOT REPRINT
© FORTINET



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

By mastering the objectives covered in this lesson, you learned how to troubleshoot public cloud connectivity issues.

DO NOT REPRINT
© FORTINET

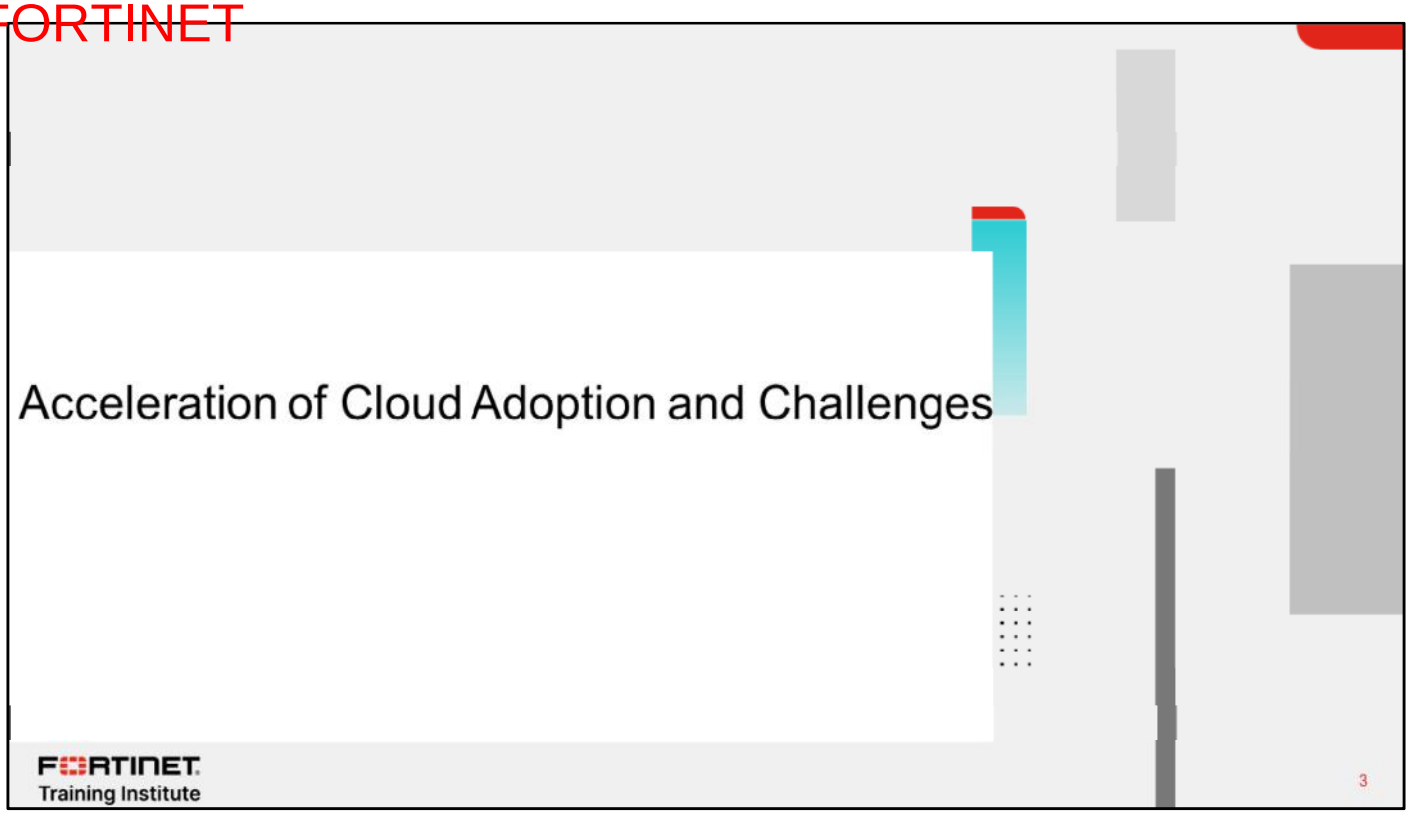


In this lesson, you will learn about Fortinet Cloud Native Protection (FortiCNP).

DO NOT REPRINT
© FORTINET

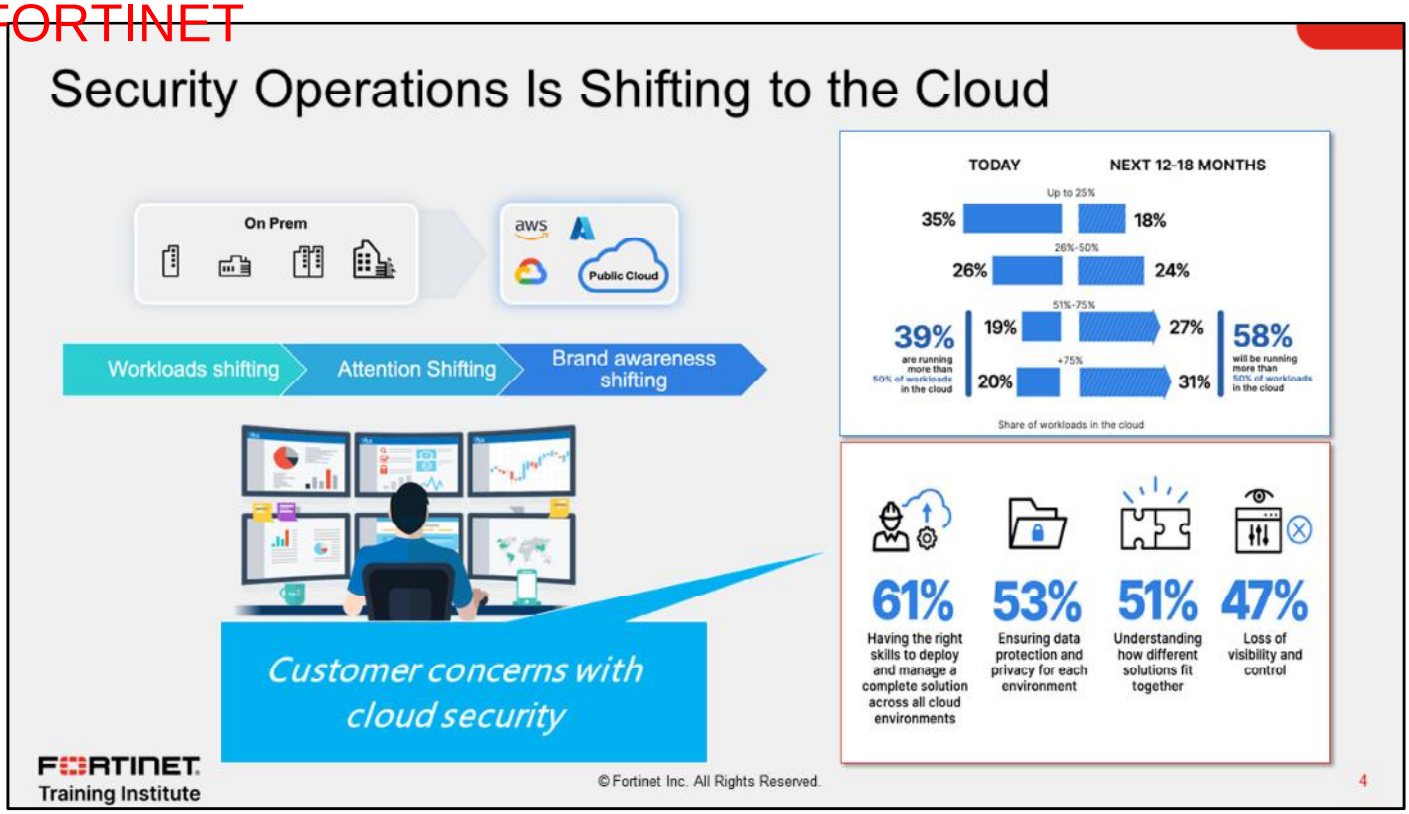
After completing this section, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



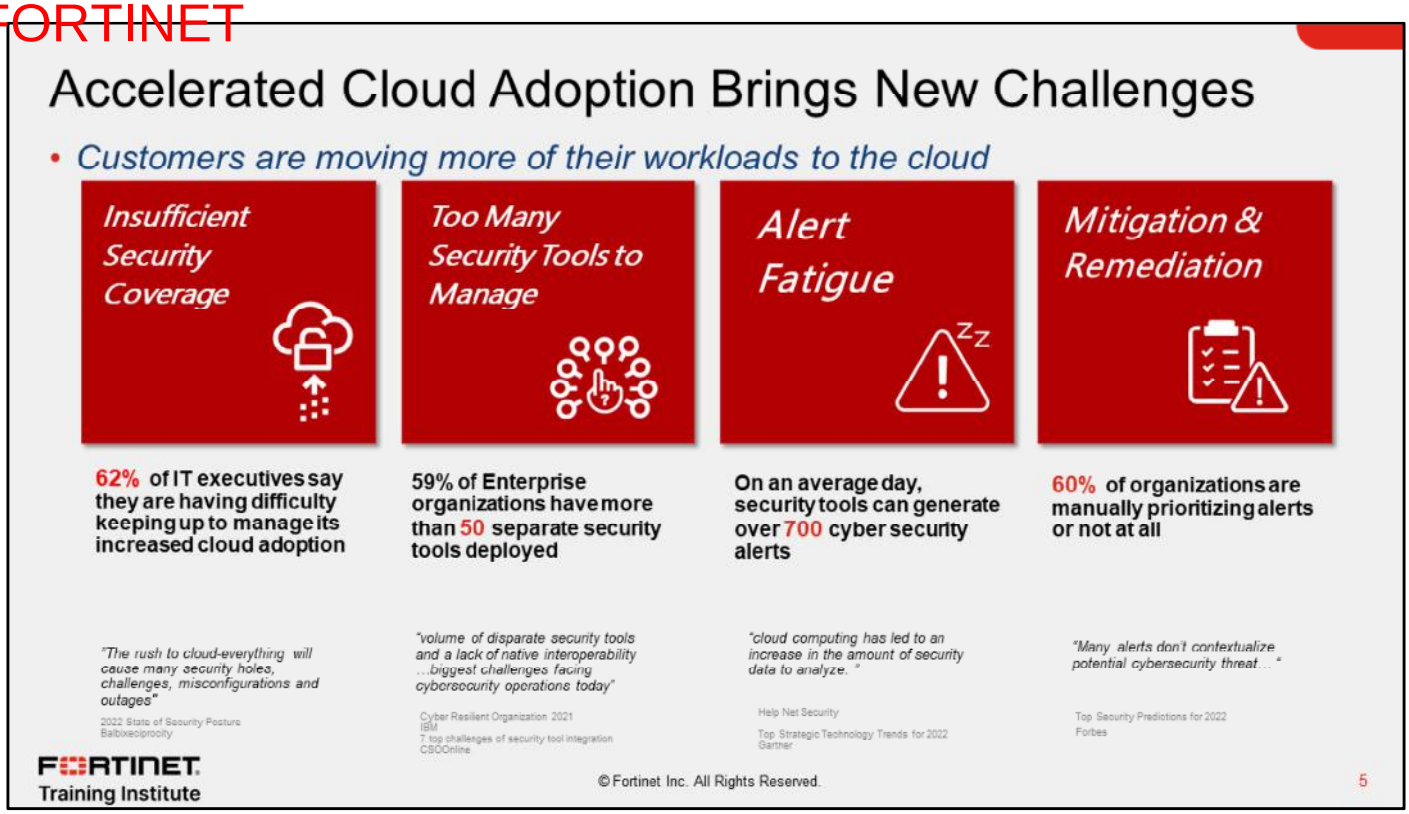
In this section, you will learn about the acceleration of cloud adoption and challenges.

DO NOT REPRINT
© FORTINET



Security operations has already been shifting its attention to the cloud. In a recent cloud security report, almost 40% of Fortinet customers have more than 50% of their workloads in the cloud. In the next 12 to 18 months, this will grow to almost 60% of those customers operating more than half of the workloads in the cloud. Using the cloud is a critical enabler to stay competitive, innovative, and deliver products and services to the market faster.

DO NOT REPRINT
© FORTINET



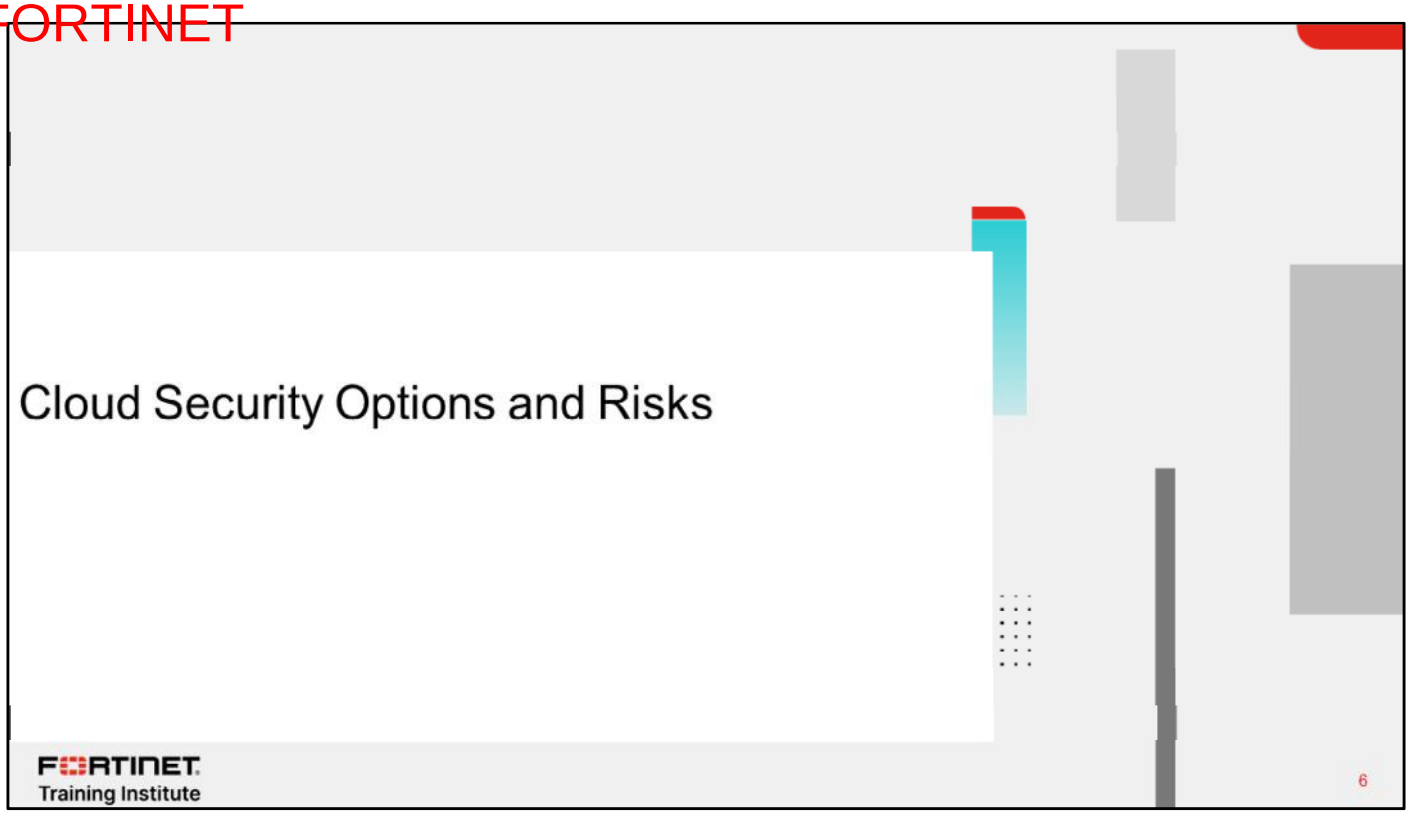
Over the last several years, many organizations have had to accelerate their digital transformation plans to modernize their interactions with customers, employees and partners. In doing so, agility and speed were prioritized over security. As customers move more and more of their workloads to the cloud, new risks have also emerged that traditional security cannot address. To avoid having insufficient security coverage, organizations tend to add new security tools that were not designed to interact. This has led to security tool sprawl, creating a complex security architecture organizations have challenges with managing.

With each of these disparate tools generating volumes of alerts, security teams can become overwhelmed, leading to alert fatigue, because they are not equipped to prioritize and investigate each of the alerts quickly enough.

This can cause critical alerts not to get addressed, putting organizations at risk. As the volume of alerts continues to increase, security teams are unable to identify critical risks to mitigate and remediate effectively, leading to decreased productivity and inconsistent workflows, creating security gaps in coverage.

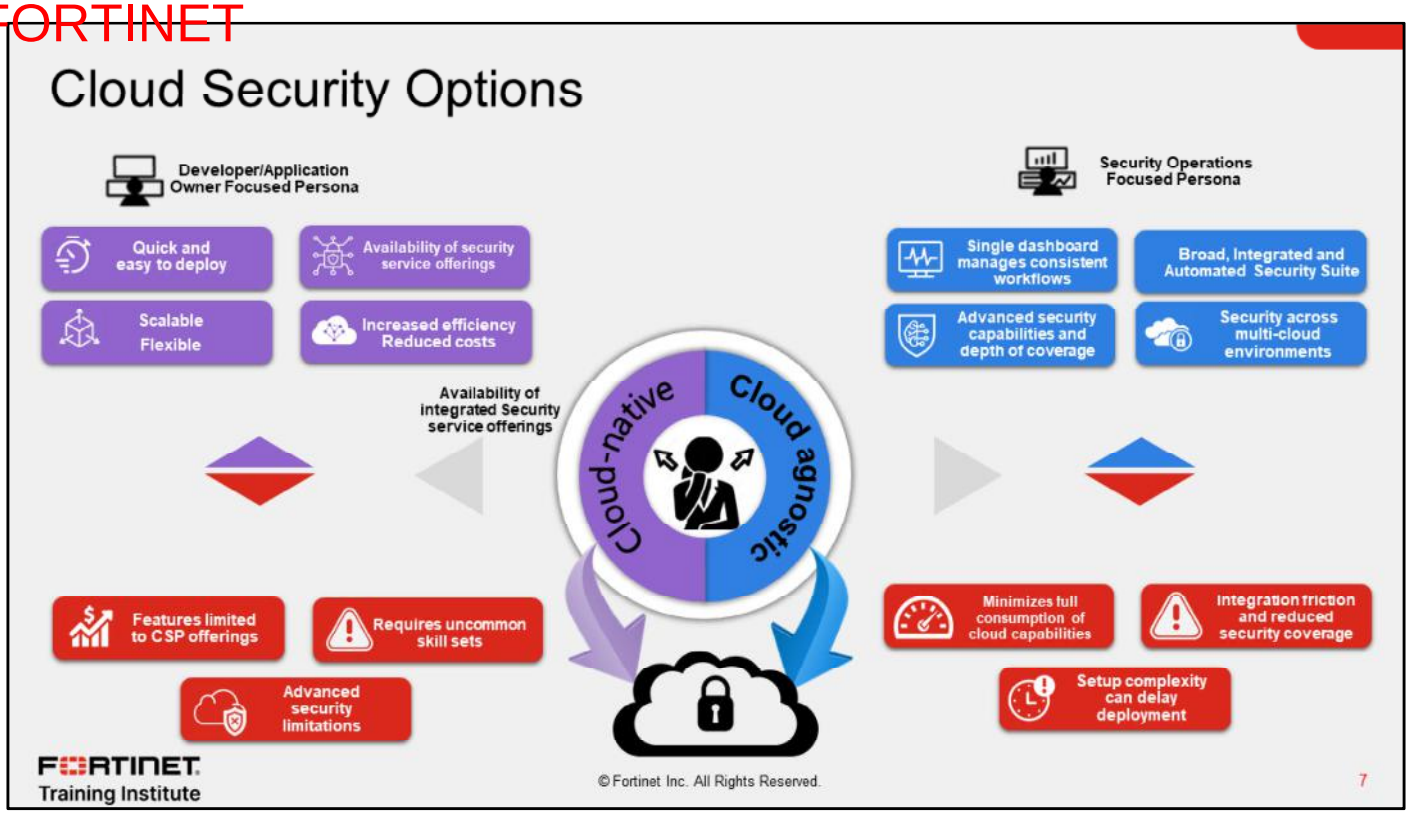
Now, security risks accumulate faster than they can be addressed, making it challenging to manage risk.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the cloud security options and risks.

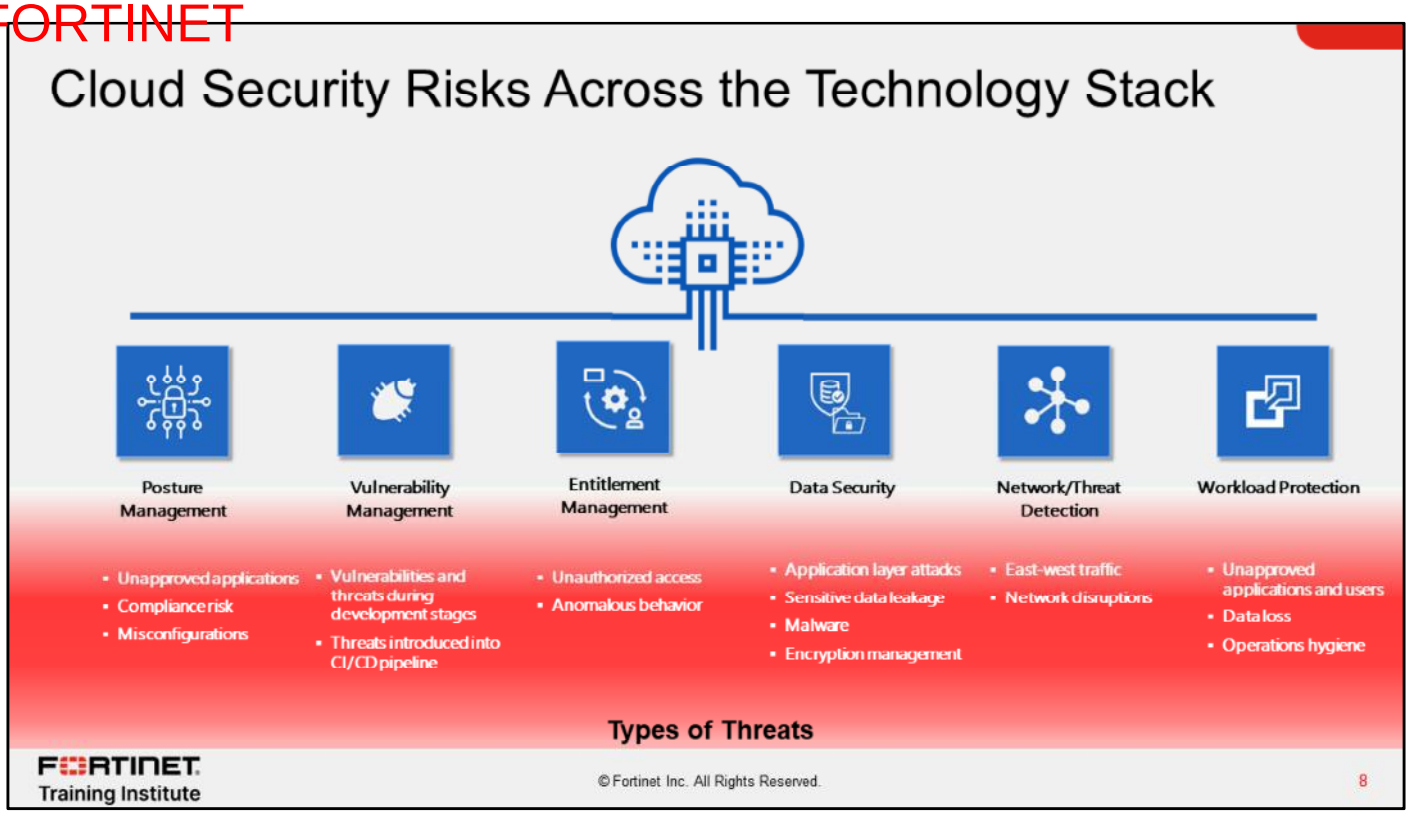
DO NOT REPRINT
© FORTINET



The cloud native security solutions are generally focused on the developer or application owner. They will likely have some expertise in the cloud environment and technologies. The benefit for the user is that these security services are easy to deploy, and have a large offering of different security services that can scale with their organization. So, having the ability to get security up and running quickly puts these services at an advantage. However, the features are limited to what the cloud service provider (CSP) offers. If advanced security requirements are needed, these services will have some limitations.

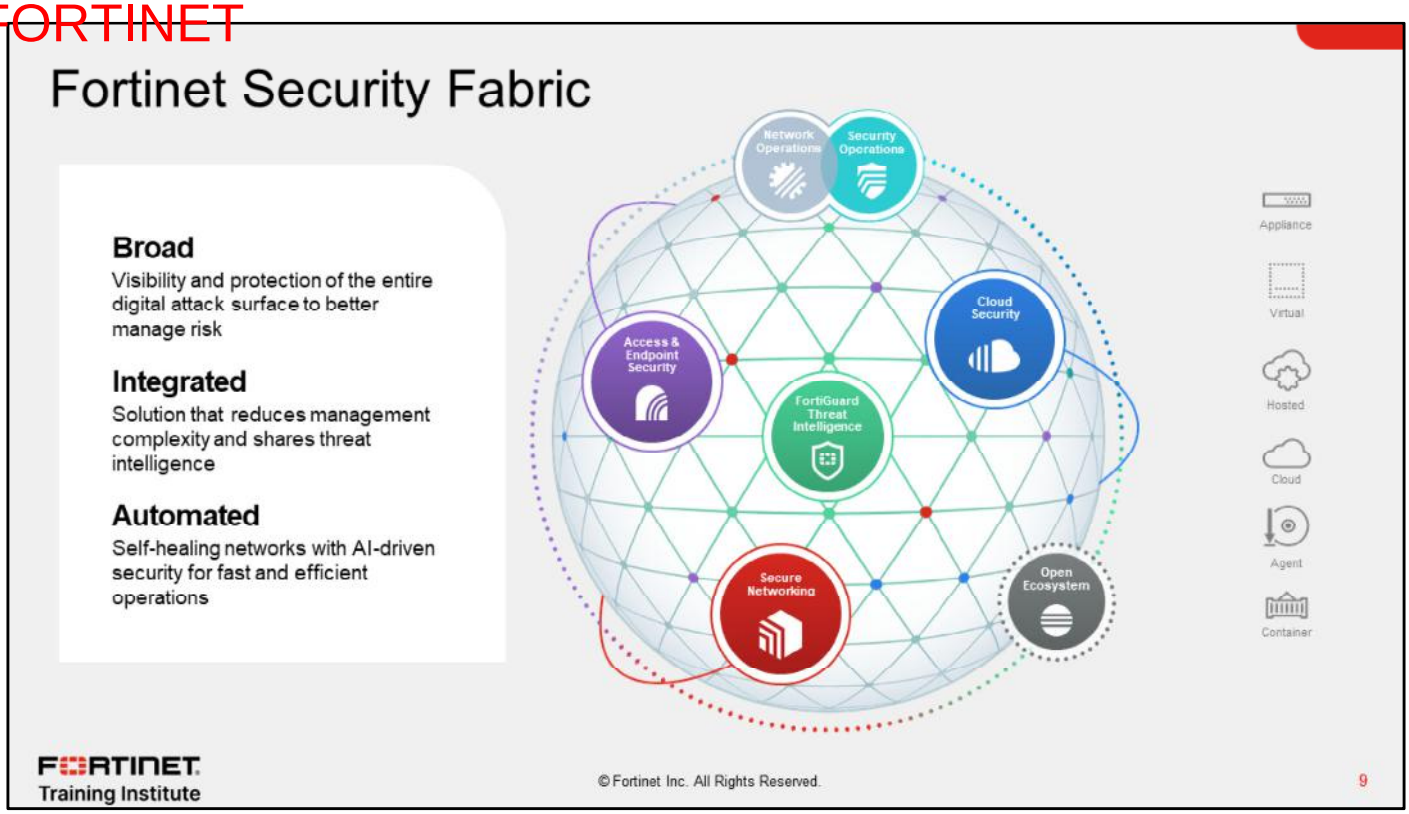
The other approach to manage risk is to leverage a third-party cloud security platform. These solutions are targeted more toward security operations personas. They are likely in multicloud environments, so these solutions can offer a single dashboard to manage consistent workflows across cloud environments. They also provide more advanced security capabilities and have a greater depth of coverage. Depending on the organization, there may be additional solutions offered in their portfolio, making it possible for organizations to expand their security footprint. But there are challenges as well. These solutions may not integrate easily with the cloud native services or other solutions, potentially creating more complexity, and inefficiencies with the use of cloud resources, preventing them from realizing the full potential of the cloud. And while these solutions may have advanced security capabilities, it may also require an expert to set up the appropriate configurations or policies, which could take time. Until it is implemented, organizations are left vulnerable without a security solution in place. So, there are benefits and challenges to either approach.
It is important to look at this from a broader perspective and know the benefits and challenges to both approaches. There is room to leverage both the strengths of a cloud native solution and a third-party solution. Each can help compensate for the challenges and each can provide strengths where the other is lacking.

DO NOT REPRINT
© FORTINET



This slide shows some of the risks across the technology stack that need to be considered.

DO NOT REPRINT
© FORTINET



The Fortinet Security Fabric is a holistic approach to security, with solutions that covers many aspects of cybersecurity. It is the same in cloud environments. It addresses the security challenges, providing broad visibility and control of an organization's entire digital attack surface to minimize risk, an integrated solution that reduces the complexity of supporting multiple point products, and automated workflow to increase the speed of operation. The Fortinet security solutions offer network security, visibility, and control in both public and private cloud deployments.

Beyond protecting against malicious content, organizations also must ensure that their cloud deployments are correctly configured. FortiCNP (Cloud-Native Protection), quickly resolves cloud security issues with actionable Resource Risk Insights (RRI). You can maximize the value of your investments in cloud provider native security services and Fortinet cloud network and application security solutions by combining security findings from all your tools into actionable insights.

DO NOT REPRINT
© FORTINET

Cloud-Native Security

- **Securing cloud-first applications and workloads**

As applications and workloads continue their journey across different clouds, it's critical to apply consistent security policies and controls across the technology stack on every cloud

Risk Management analyzes security findings generated by a cloud provider's native security services

Threat Management analyzes and continuously monitors security events for potential threats with AI/ML and automation

Data Security analyzes configurations, files, and documents in cloud storage services to detect misconfigurations, sensitive data, and malware

Container Protection provides deep visibility into the security posture of container registries and images. It monitors and protects against vulnerabilities and threats throughout the stages of the application container lifecycle

Compliance ensures compliance to regulatory standards and mandates to detect violations

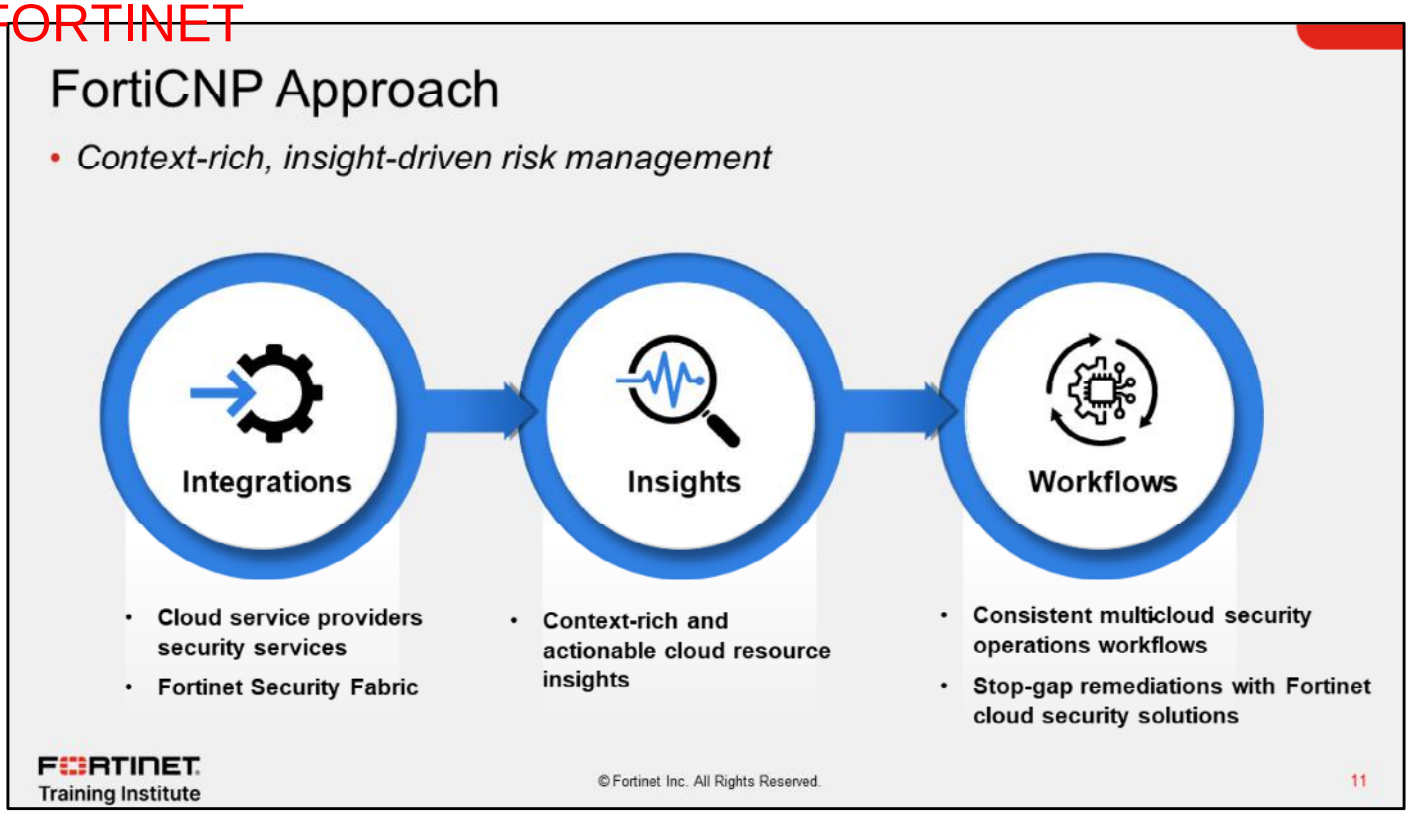
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

There are many applications and workloads spread across the multicloud environment. When you have multiple applications and workloads in different clouds, it is important to have consistent security policies and controls.

DO NOT REPRINT
© FORTINET

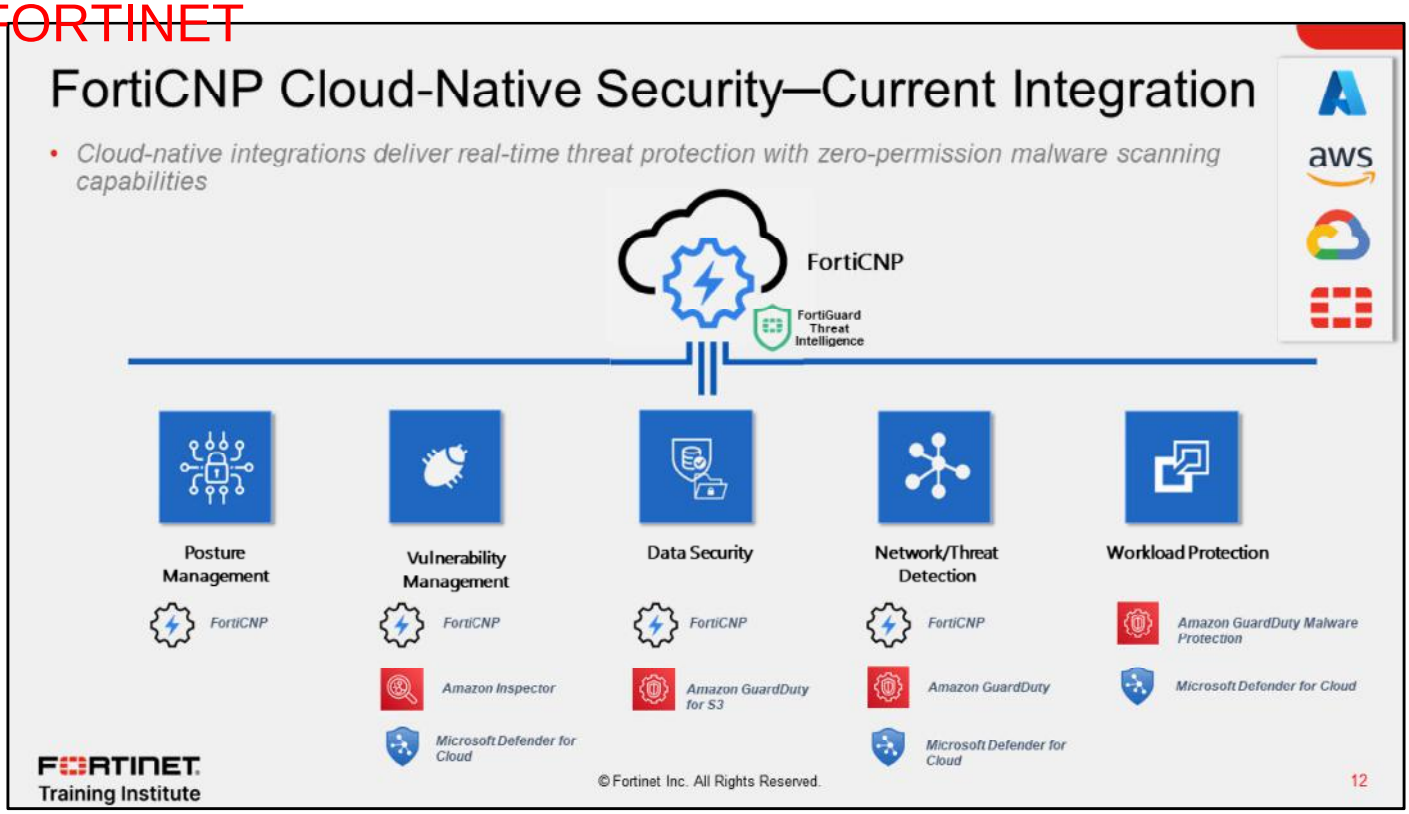


The FortiCNP approach is to support a context-rich, insight-driven risk management solution. To make that happen, FortiCNP leverages deep native integrations with CSP security services, and products and services from the Fortinet Security Fabric, to contextualize the findings.

As FortiCNP correlates and normalizes the security findings across those products and services, it provides context-rich, actionable insights that help enable consistent workflows that can be enabled across cloud environments. This also includes the stop-gap remediation that can be enabled using Fortinet cloud security solutions.

This helps security teams avoid having to manually triage and prioritize the alerts, and determine how to remediate the risk. It also relieves security teams from having to master the intricacies of each cloud platform and technology stack to remediate the risk.

DO NOT REPRINT
© FORTINET

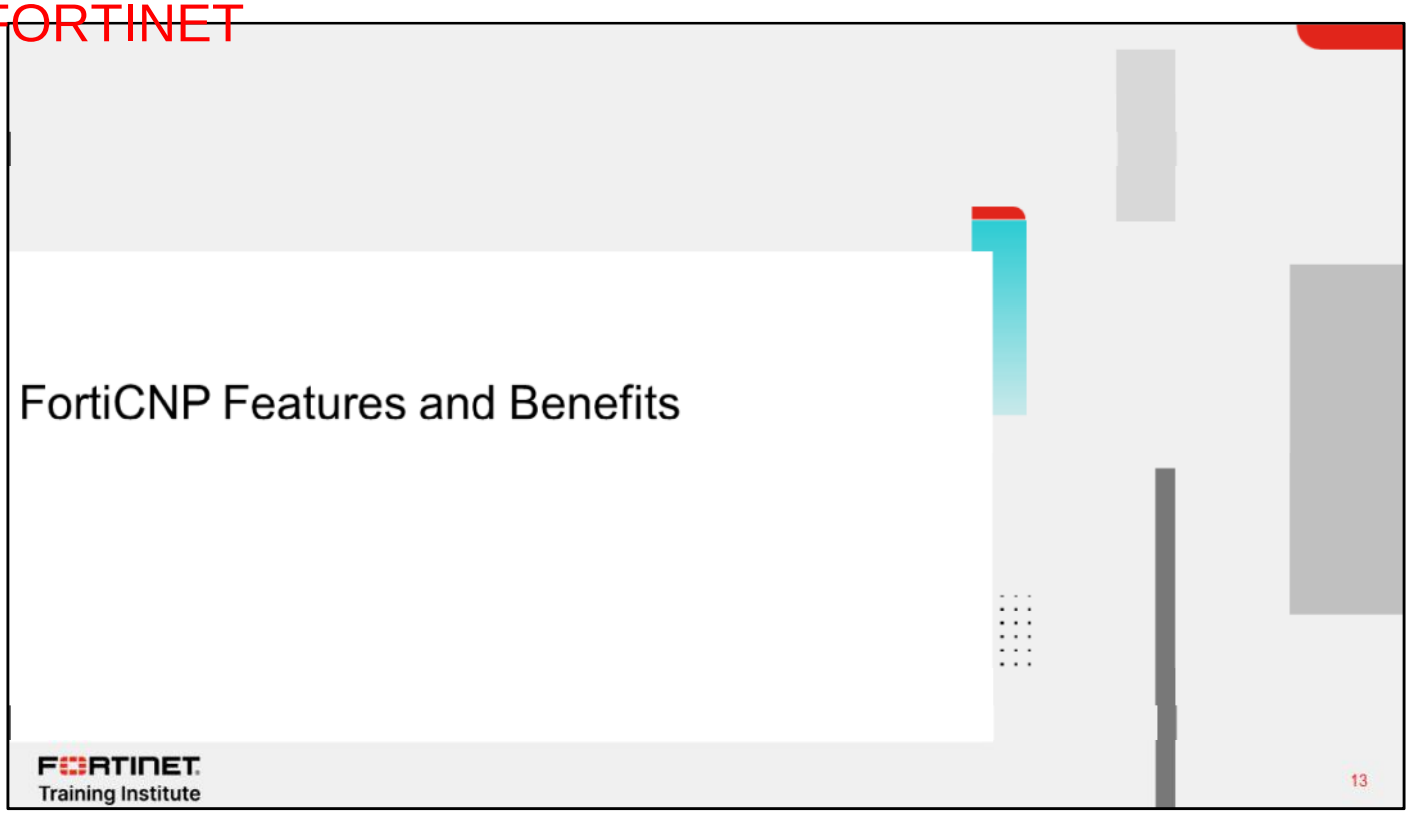


FortiCNP is a cloud-native protection solution that integrates with CSP-native security services and the Fortinet Security Fabric to help organizations prioritize and manage cloud risks with context-rich, actionable insights. This is a huge differentiator because no other solution is built on the security services provided by major cloud providers. The challenge is that these services generate a large amount of data that is difficult for security teams to correlate and understand what to do with.

FortiCNP helps rationalize all the security data, making it easier for security teams to understand where the most critical risks are and what to do to remediate them. FortiCNP has native integrations with different CSP security services. Given this, FortiCNP does not require separate permissions to be able to access the security details. As such, FortiCNP enables zero permissions security coverage, which essentially removes any integration friction that many organizations experience. Through FortiCNP, data security, and cloud security posture management (CSPM) and network detection capabilities support Google Cloud Platform (GCP). Additionally, through FortiCNP, vulnerability scanning for containers is also supported through GCP.

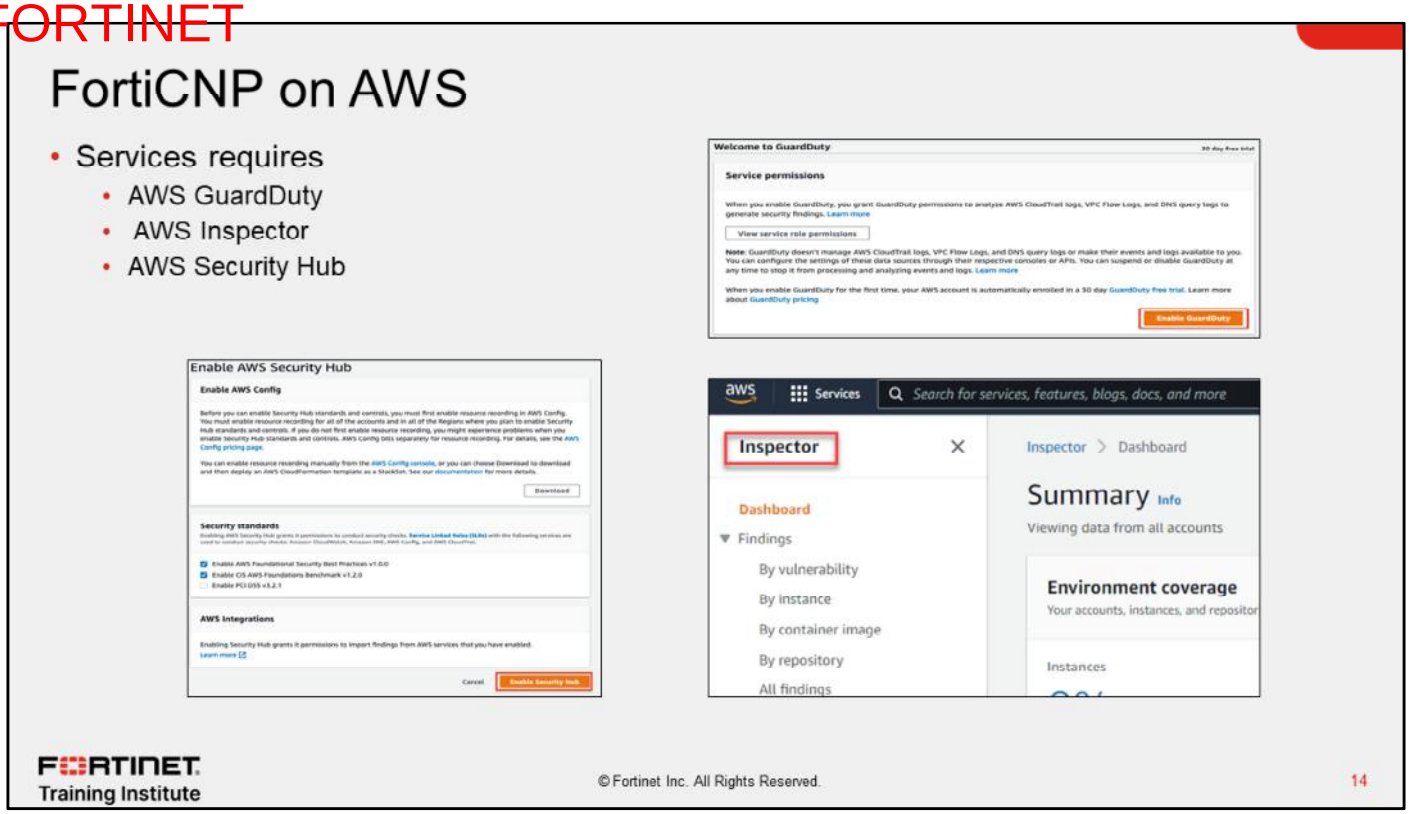
FortiCNP also introduces a new patented technology called Resource Risk Insights (RRI). The RRI will correlate and normalize security information generated by these security services and solutions to produce a normalized risk score. If you think about in another way, RRI adds context to all those security findings that it uses to stack rank the risks based on the scores, and to provide actionable insights for security teams to focus on the highest risk resources to mitigate and address.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the FortiCNP features and benefits.

DO NOT REPRINT
© FORTINET

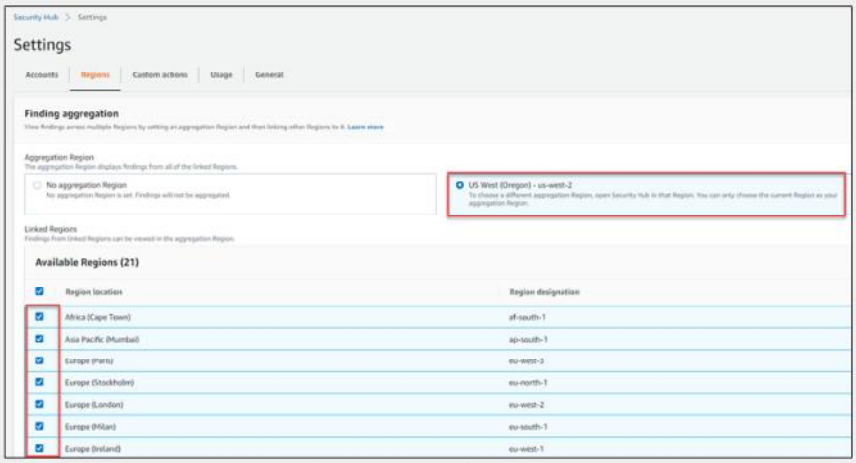


Now you will learn how to use the full array of FortiCNP features on AWS. In order to use FortiCNP on AWS, you must at least enable AWS services, such as **GuardDuty**, **Inspector**, and **Security Hub**. These services are not mandatory to get the FortiCNP started, but very useful to take full advantage of FortiCNP.

DO NOT REPRINT
© FORTINET

FortiCNP With Cross Region Aggregation

- Security events can be collected from multiple regions
- Enable Amazon GuardDuty and Amazon Inspector in the same region
  - To generate security events
- Enable AWS Security Hub to collect security events



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

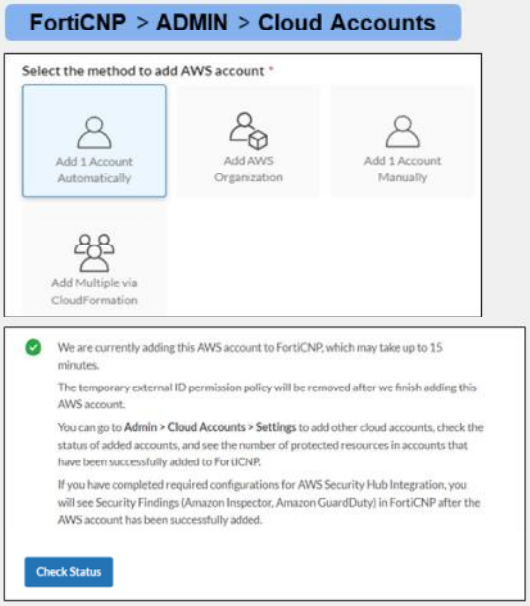
15

With FortiCNP cross region aggregation, you can aggregate findings from different regions using Amazon GuardDuty, Amazon Inspector, and Security HUB.

DO NOT REPRINT
© FORTINET

Add FortiCNP Account

- Add FortiCNP account from **ADMIN > Cloud Accounts**
- Configure the following details:
  - **AWS Account ID** and **Account Name**
  - Accept FortiCNP to create a **CloudTrail** for the account
  - Follow the AWS **CloudFormation** steps to **Create a Stack**
  - Check status



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

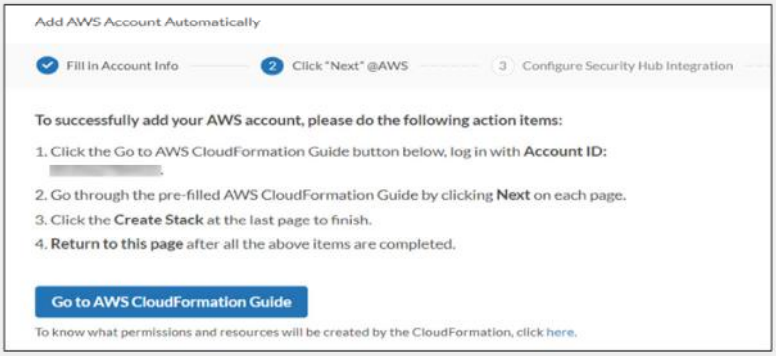
16

There are few steps that you must follow to enable FortiCNP on AWS. Add FortiCNP to AWS from FortiCNP by clicking **ADMIN** > **Cloud Accounts**. You must enter the AWS **Account ID**, and name your account. At this step, select the check mark to accept FortiCNP to create a **CloudTrail** for the account. AWS **CloudTrail** logs enables FortiCNP to monitor files in a monitored bucket.

DO NOT REPRINT
© FORTINET

Event Bus Through AWS CloudFormation

- Use AWS CloudFormation to configure the AWS **Event Bus** and **Events Rule**
- The **CloudFormation Guide** uses a JSON file to establish the AWS Event Bus and Event Rule
  - The Security Hub can send security findings to the AWS Event Bus



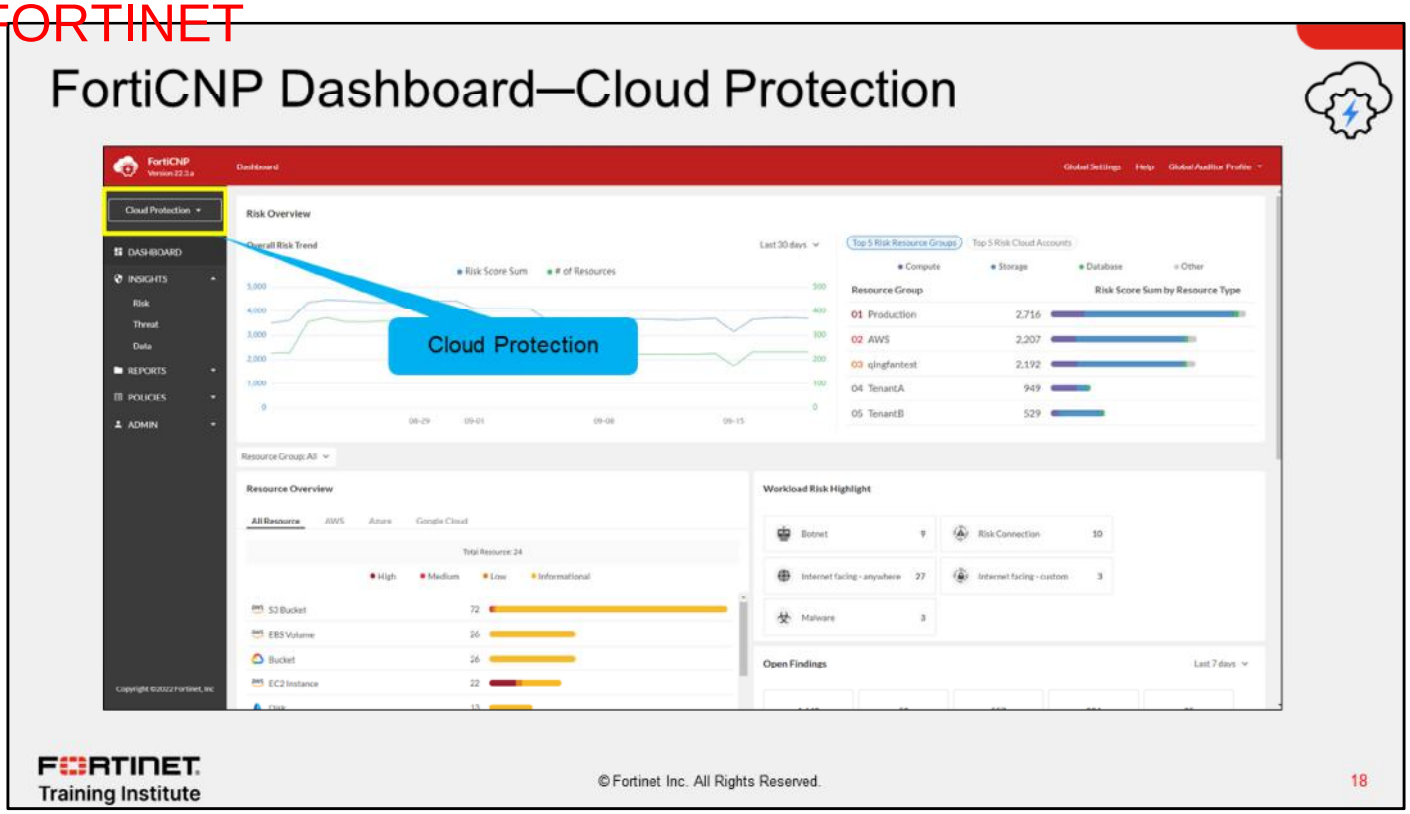
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

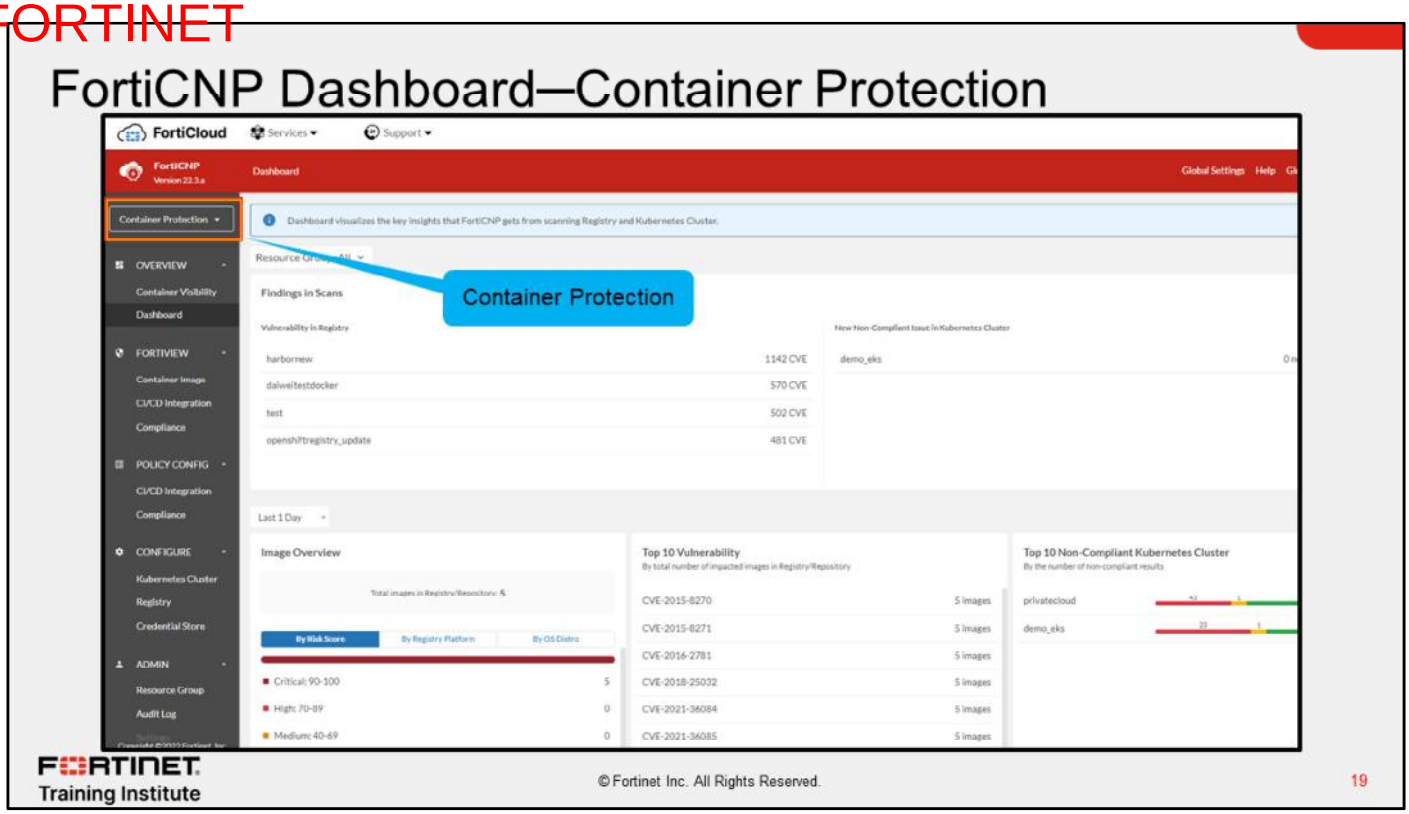
After finishing the security hub configuration, you will need to configure AWS Event Bus and Events Rule using the AWS CloudFormation guide. The Security Hub can send security findings to the AWS Event Bus under the FortiCNP AWS EventBridge.

DO NOT REPRINT
© FORTINET



The FortiCNP dashboard provides a quick snapshot of risk findings. You can start your review from the dashboard. The **Resource Overview** is one of the important places to check the risk score. You can click and navigate to the specific risk and know which of the findings contribute to the risk score. Also there are two main components in FortiCNP, **Cloud Protection** which is the default landing page and container protection. You can set the default landing page to container protection based on your requirements.

DO NOT REPRINT
© FORTINET

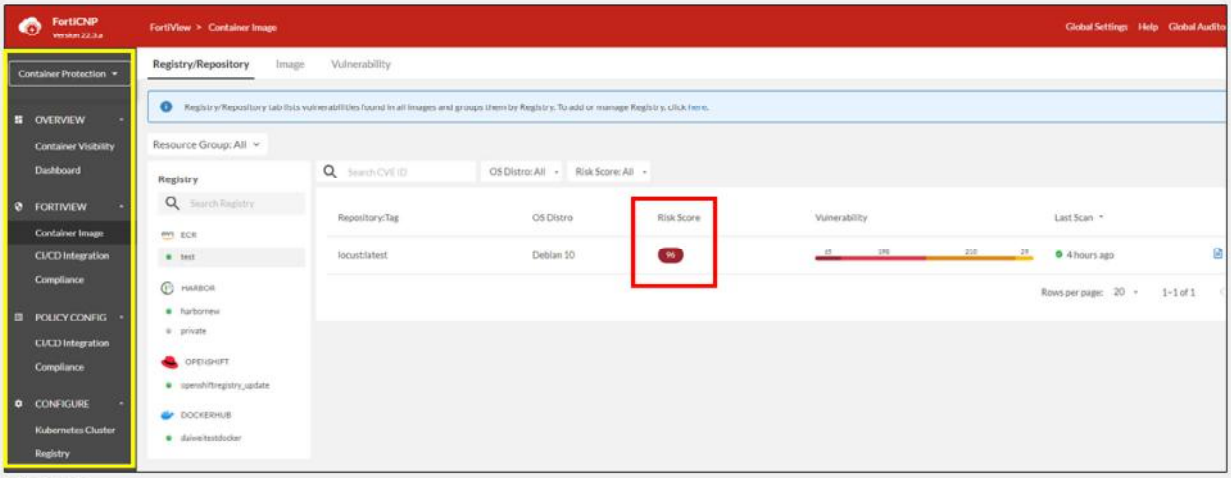


Container protection is one of the challenging components that security operations teams encounter on a day-to-day basis. The application developers are shifting away from the traditional application development process and developing more applications in the cloud. So, with containers in a multicloud and dynamic environment, security teams get overwhelmed with many tasks and securing all the containers. As a solution, FortiCNP Container Protection provides deeper visibility into the security posture for container-based workloads across multicloud environments. It simplifies DevSecOps adoption by integrating security in the early stages of the software development process to provide continuous visibility and protection for containers and Kubernetes workloads.

DO NOT REPRINT
© FORTINET

FortiCNP Dashboard—Container Protection (Contd)

- Container visibility
- Registry image scan
- Kubernetes cluster



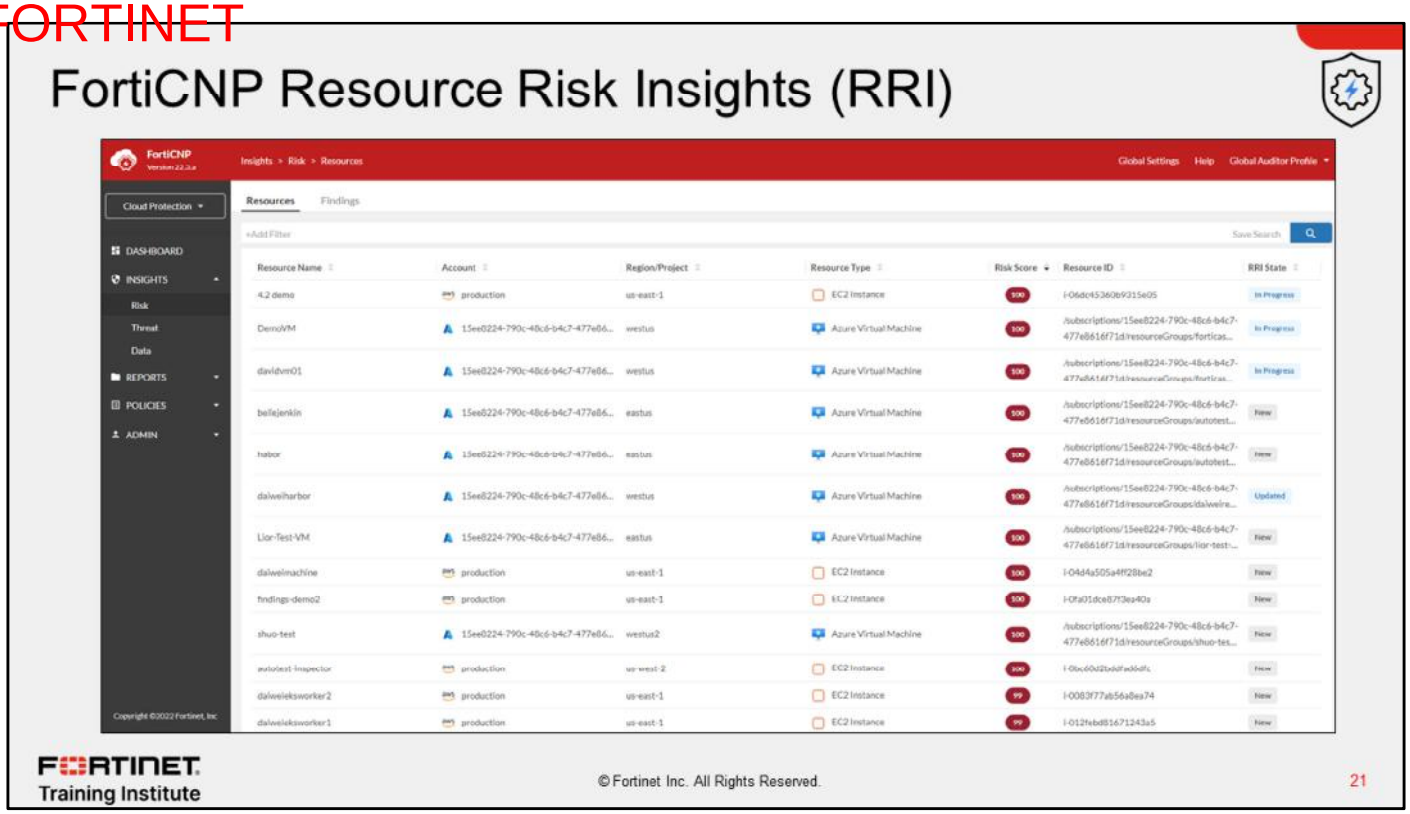
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

Container Protection offers vulnerability image scanning on either private cloud or supported container-based platforms, such as **Amazon EKS**, **Google GKE**, **Azure AKS**, **Harbor**, and **Openshift**. The integrated scanner analyzes the container images through **Common Vulnerability and Exposure (CVE)**. The vulnerability image scan result is interpreted with risk scores based on the severity of the vulnerability found. After a credential is registered with **Container Protection**, a kubernetes agent needs to be deployed on the kubernetes cluster. The kubernetes agent would enable **Container Protection** to provide vulnerability and compliance assessments on the registry images. **Kubernetes Agent** deployed on **Kubernetes Cluster** and FortiCNP Jenkins Plug-in are leveraged to provide image scanning capability when images are created just before they are deployed.

DO NOT REPRINT
© FORTINET

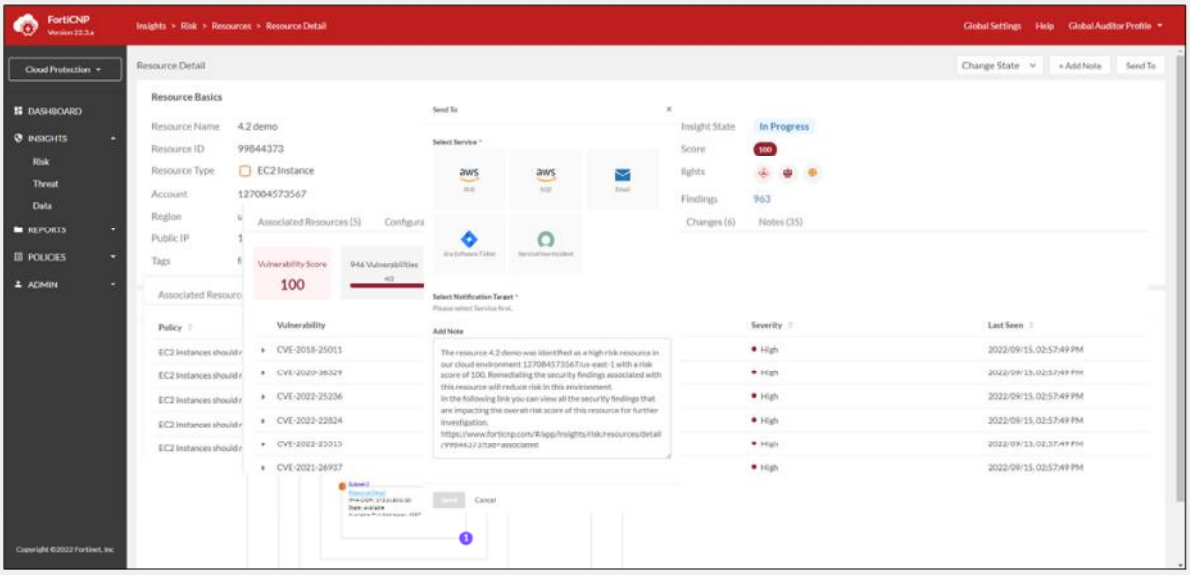


FortiCNP RRI enables consistent workflows across multiple cloud environments, helping security teams minimize gaps in security coverage consistently. This model eliminates the painful process of agent deployment and takes advantage of single-click deployment of cloud native security services. Once activated, FortiCNP ingests findings from these services, correlates them, and presents you with actionable insights. Security teams that use FortiCNP RRI do not need to have specialized knowledge in each cloud environment to mitigate risks because RRI provides insight for them.

FortiCNP provides comprehensive security for your cloud environments through integrations with AWS services (such as Inspector, GuardDuty, and Security Hub) for security monitoring and displaying relevant information regarding cloud assets. FortiCNP correlates all these findings (either locally generated or ingested) under each monitored resource type. Vulnerability findings from Inspector are ingested through Security Hub and are then used by FortiCNP when providing an overall risk score for a monitored resource.

DO NOT REPRINT
© FORTINET

FortiCNP RRI Details



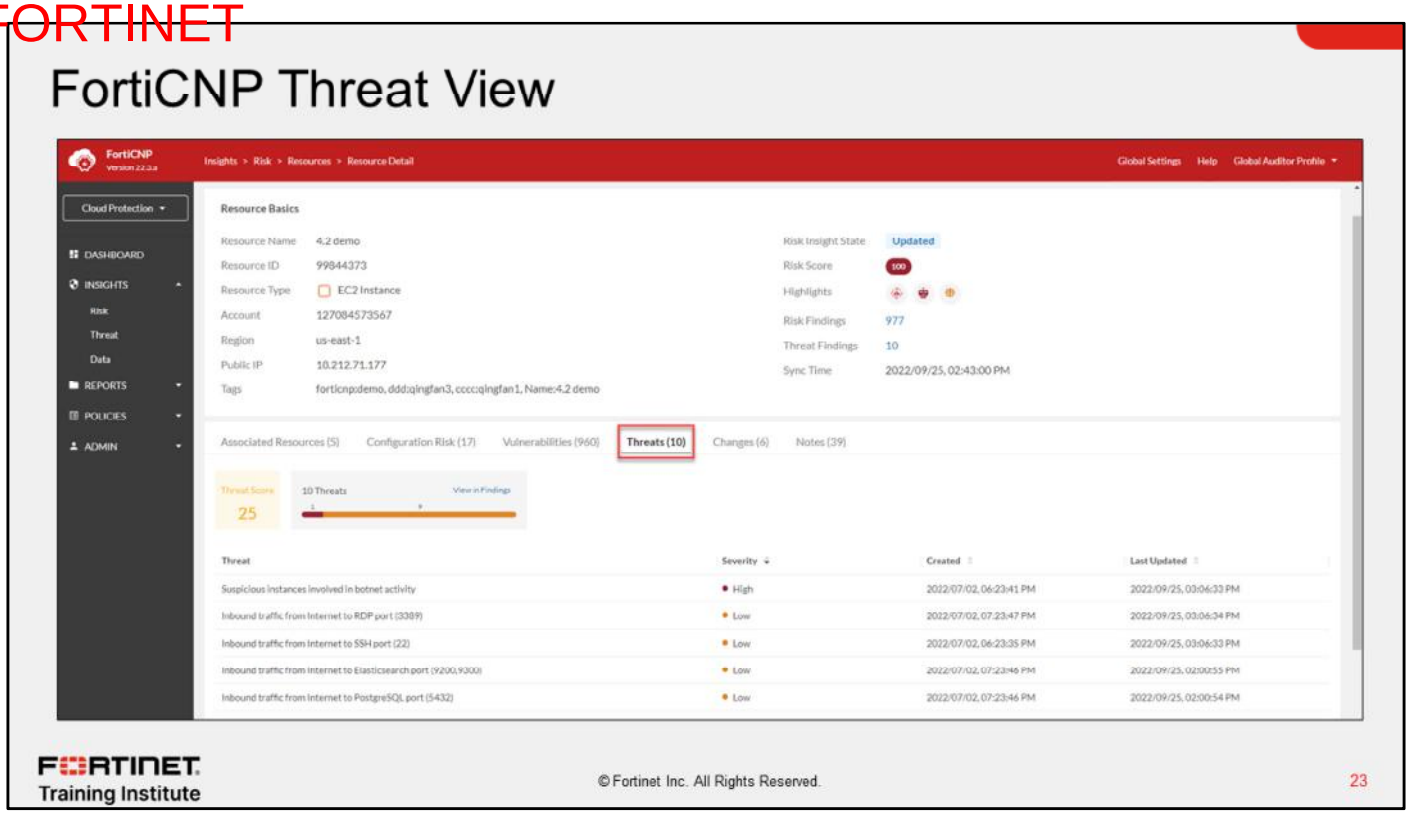
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

In the **Resource Detail** section, there are multiple tabs where FortiCNP correlates data. You can see **Associated Resources**, **Configuration Risk** findings are generated locally, and vulnerability findings imported from AWS Inspector through Security Hub and change logs, for example. Also, you can send notifications to several messaging and ticketing systems.

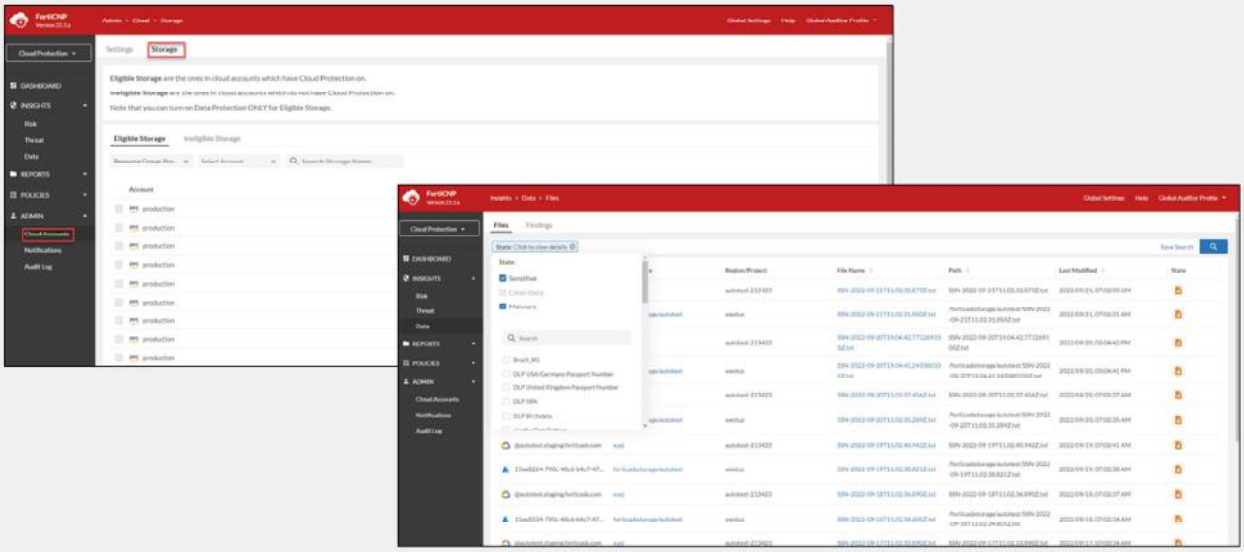
DO NOT REPRINT
© FORTINET



FortiCNP correlates all relevant threat findings for each resource on the **Threats** tab. These can be either from local policies under **Policies**, **Threat Detection**, **User Activity** or **Network** tabs or from AWS GuardDuty findings. Based on these findings, the resource is given a threat score which, calculated along with any configuration risk and vulnerability scores, gives a total risk score for the resource.

DO NOT REPRINT
© FORTINET

S3 Data Protection

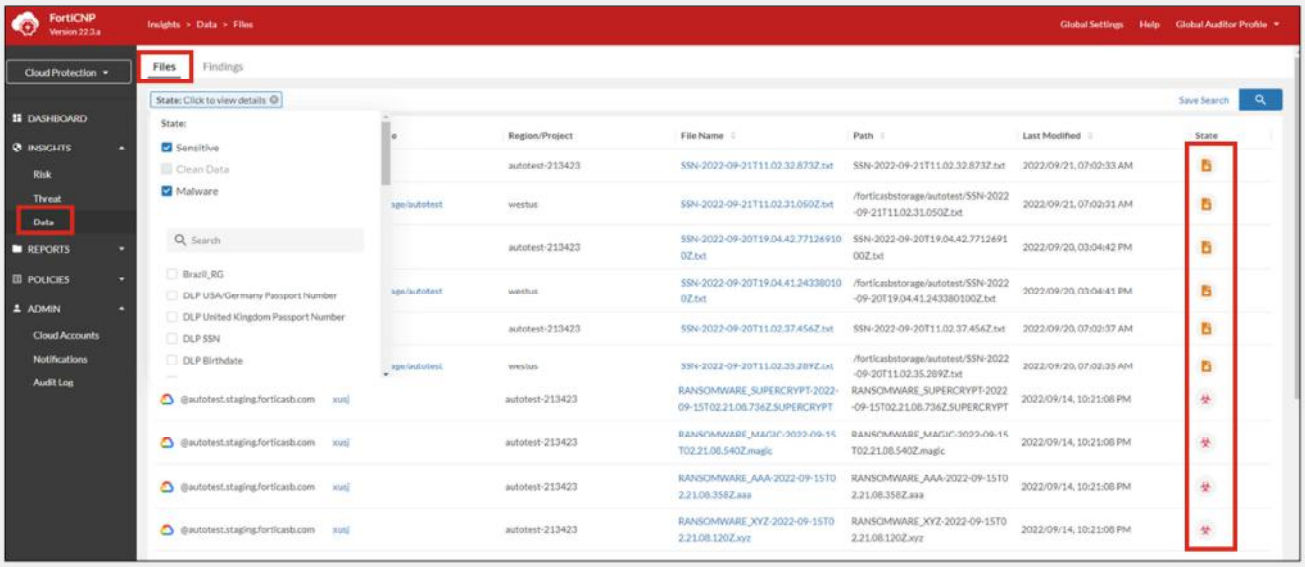


FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
24

FortiCNP not only provides comprehensive configuration assessment to ensure security of data storage, but it also analyzes documents inside the storage objects to identify and monitor sensitive data and malware. Security administrators can monitor and analyze sensitive data activity by drilling down into document profiles from generated alerts to investigate data leakage in the environment.

DO NOT REPRINT
© FORTINET

Scanned Files



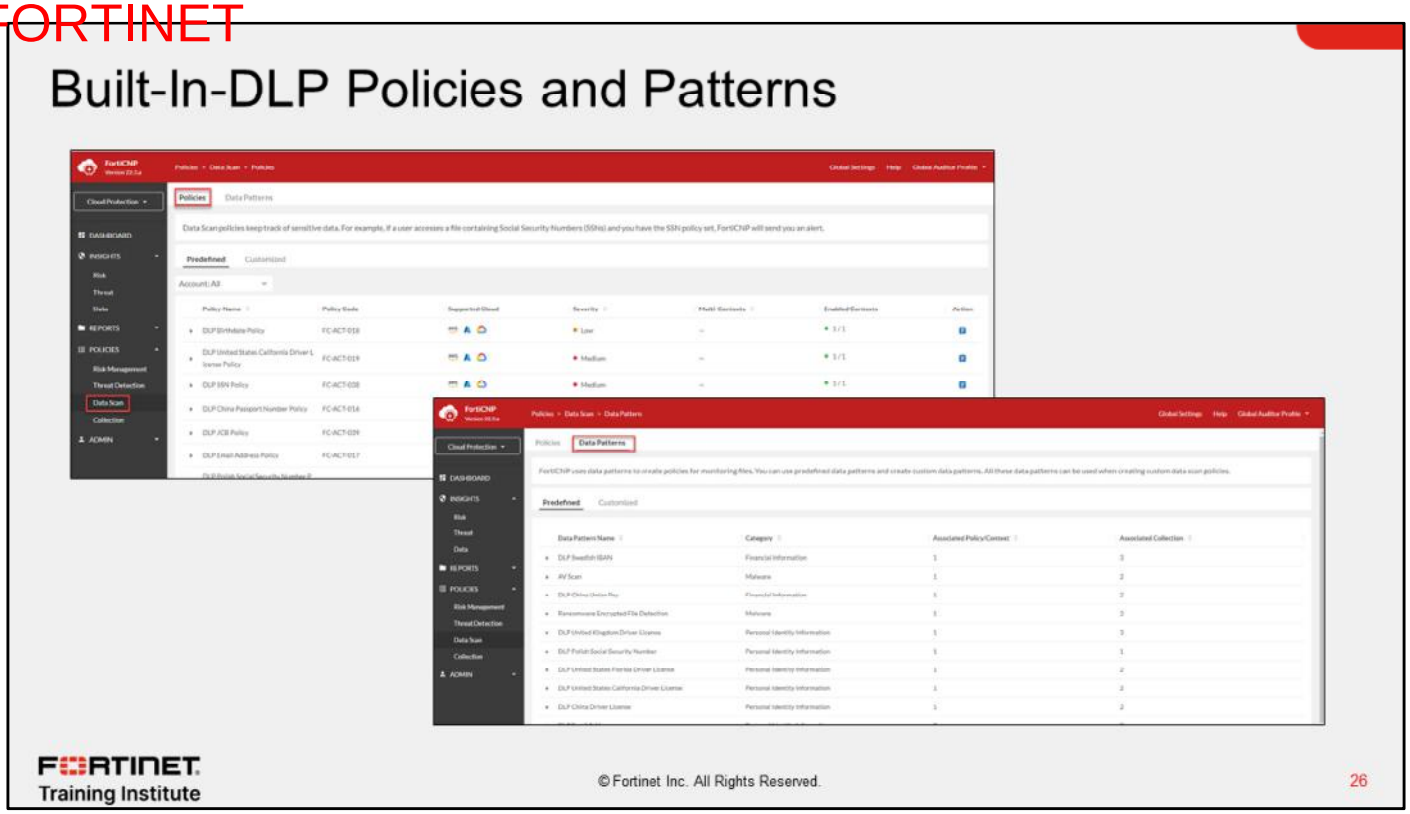
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

If there are any data findings reported after the file scan, you can find the detail information under **INSIGHTS**, **Data** section. You can further apply the filter to find out if the file is reported as **Sensitive** data or **Malware**. You can click the file name to get more information.

DO NOT REPRINT
© FORTINET

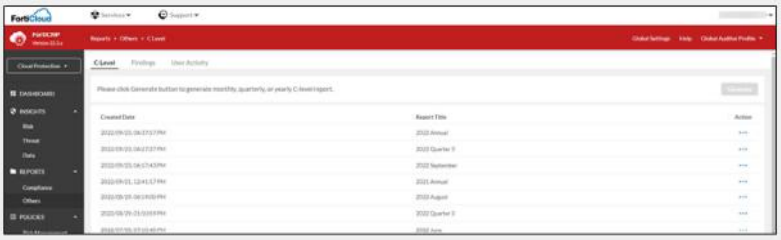


Data Scan policies keep track of sensitive data. If a user accesses a file and that file has a policy set, then FortiCNP will send the alert notification. You can view all the built-in policies and patterns. Also, the administrator can customize policies and create patterns with regex to avoid unwanted access to sensitive files.

DO NOT REPRINT
© FORTINET

FortiCNP Reports

- Compliance report
  - Overview of overall compliance of all cloud accounts such as HIPAA and SOX
- C-level report
  - Overall security status of cloud accounts on FortiCNP



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

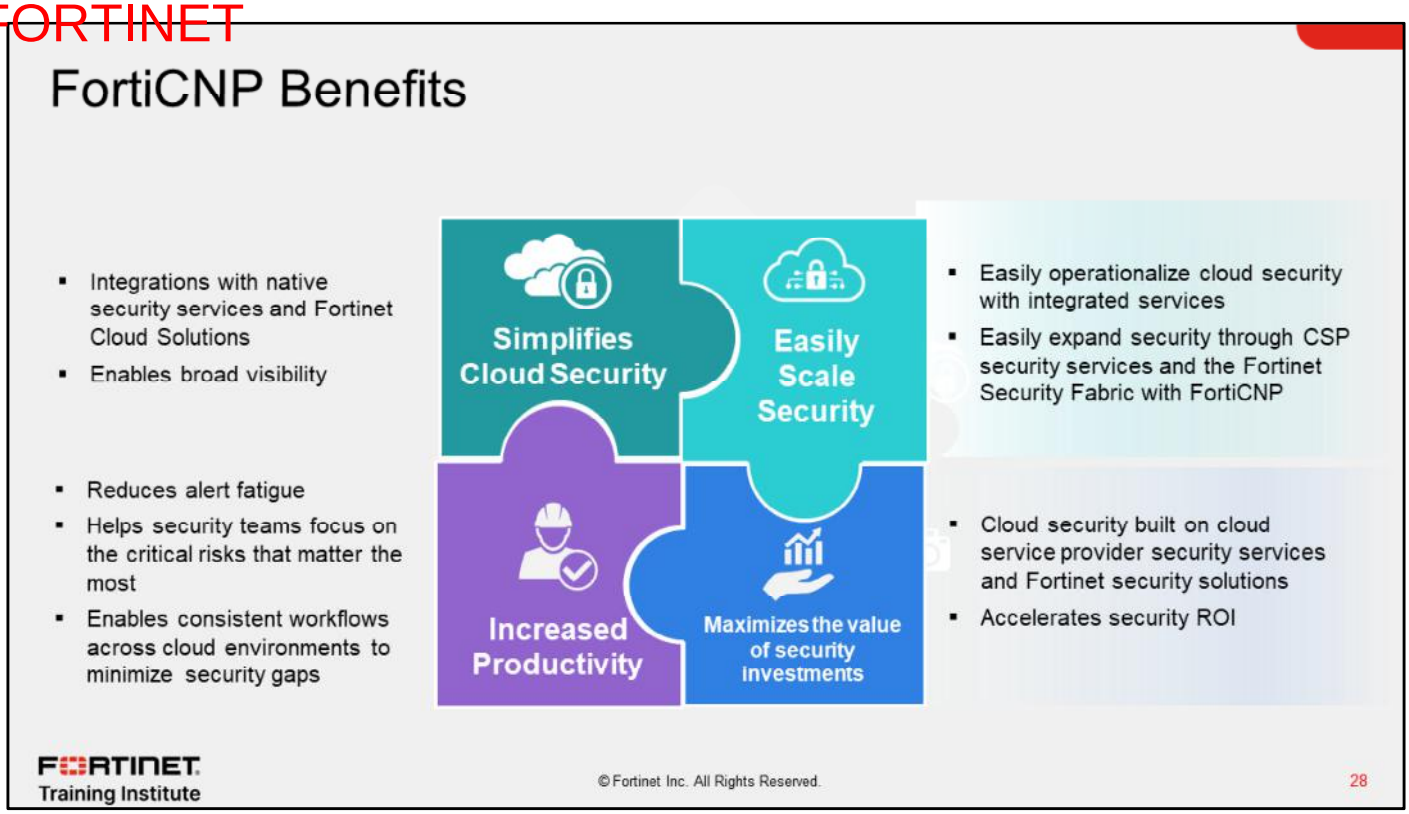
27

FortiCNP allows you to generate executive C-level and compliance reports.

Compliance reports provide an overview of the overall compliance of all cloud accounts with policies such as HIPAA, SOX/COBIT, and PCI. Compliance reports are automatically generated and ready to be downloaded on a quarterly, monthly, or annual basis.

C-level reports summarize the overall security status of your cloud accounts on FortiCNP. This includes the number of findings triggered, the regions affected by the findings, the cloud storage files that may have been exposed because of a security breach, and so on.

DO NOT REPRINT
© FORTINET



Now you will learn about the benefits of FortiCNP.

FortiCNP simplifies cloud security by removing integration complications. This makes it possible for the customer to deliver a cloud security solution that they can operationalize very quickly.

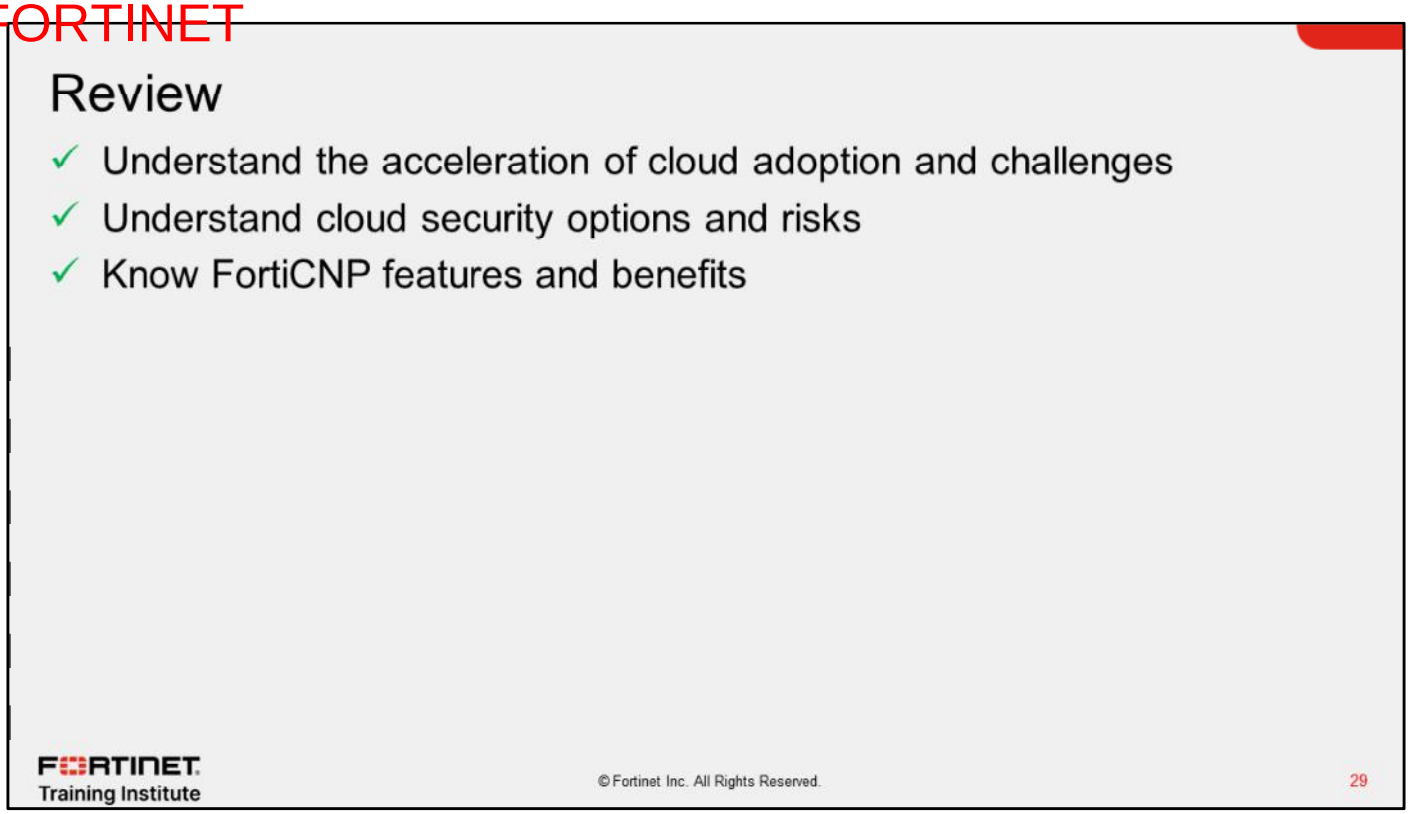
Using FortiCNP, customers can easily scale their security solutions. Native integrations help to operationalize CSP native security services alongside the Fortinet Security Fabric controls in the cloud. Customers will also be able to easily select from either coordinating cloud technologies from the Fortinet Security Fabric that are also CSP security competency solutions and, conversely, CSP security solutions with services that are integrated with FortiCNP. This gives customers more options to expand their security footprint across the cloud technology stack, helping them innovate and deliver applications and services faster.

FortiCNP helps increase productivity by correlating and normalizing the security findings from the integrated solutions, thereby reducing the noise, to provide actionable insights, helping security teams focus on the risks to remediate, that have the highest impact to the organization. FortiCNP also enables consistent workflows that scale security across clouds—helping teams proactively manage risk and improve security coverage, which helps to increase overall productivity

FortiCNP maximizes the value of customer security investments. FortiCNP leverages what customers already have in place, and applies RRI intelligence to contextualize the alerts.

For customers that have coordinating Fortinet Cloud security products, such as FortiWeb and FortiGate-VM, the security findings from these products are also correlated into the FortiCNP RRI technology to enrich the findings, which helps increase their return on investment. At the same time, customers are able to get the best value out of their investments in both AWS native services as well as Fortinet Cloud Security Fabric solutions.

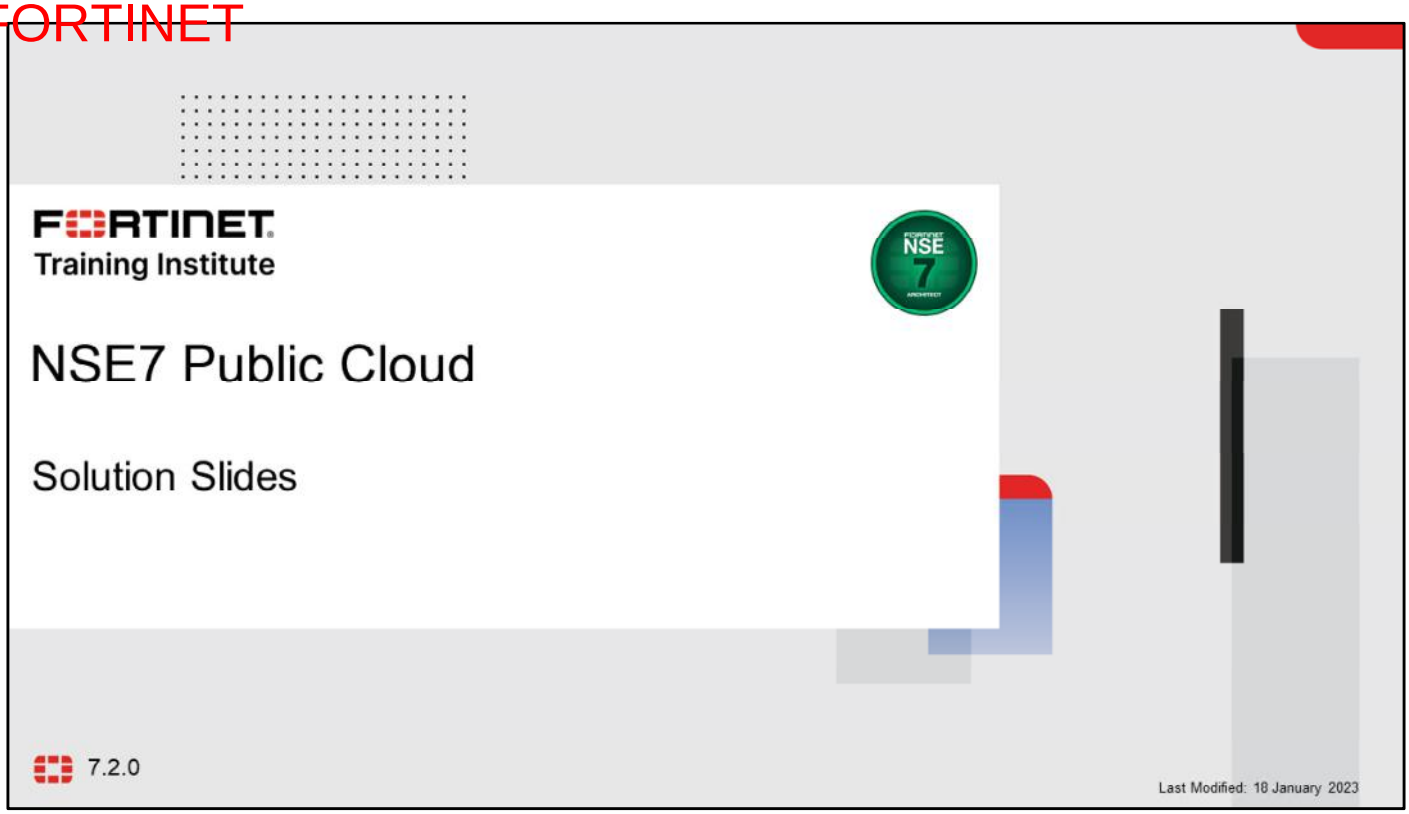
DO NOT REPRINT
© FORTINET



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

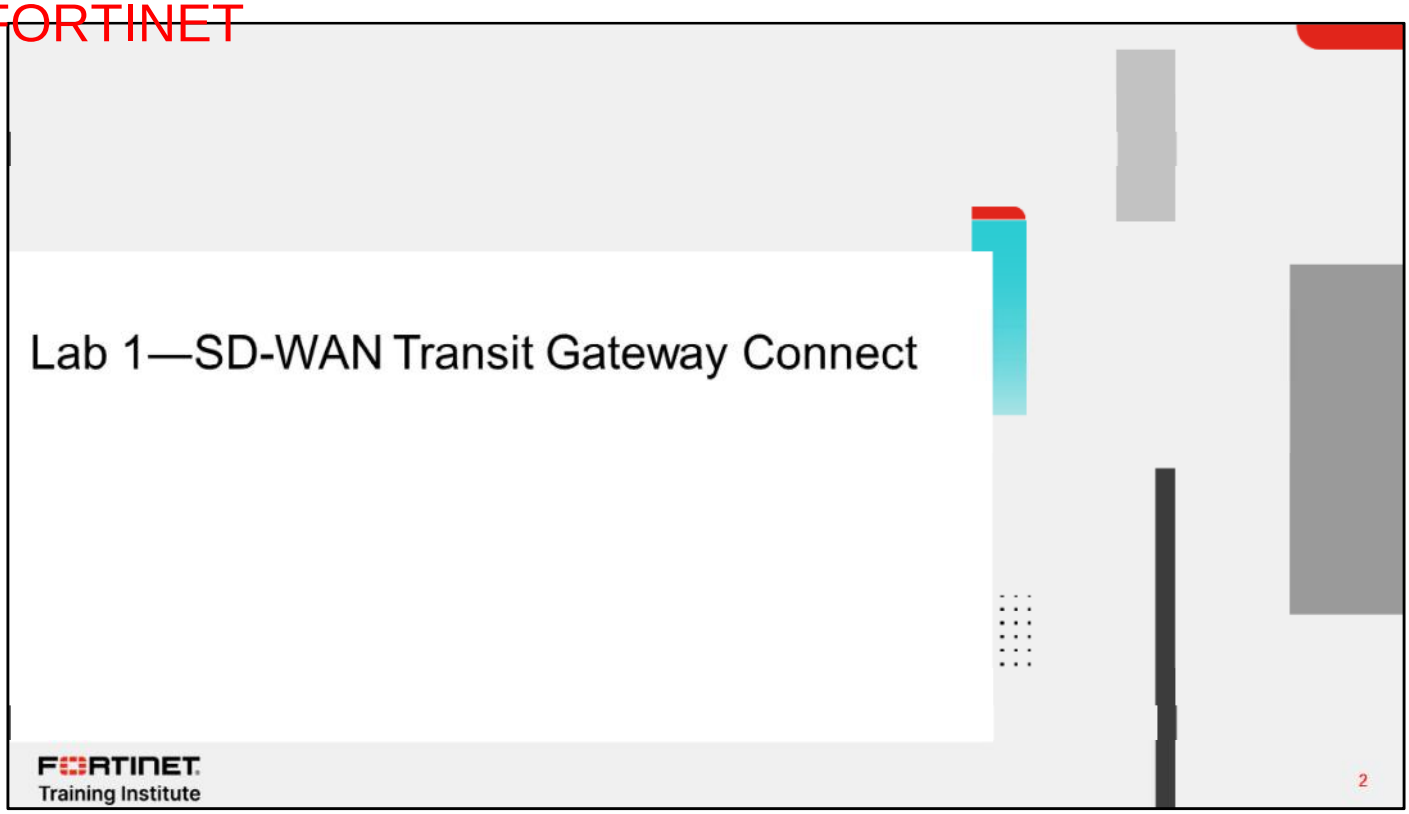
By mastering the objectives covered in this lesson, you learned about FortiCNP.

DO NOT REPRINT
© FORTINET



Solution slides.

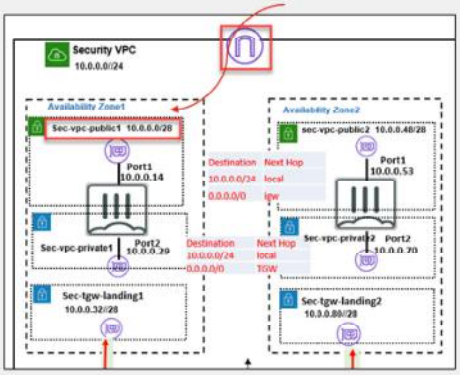
DO NOT REPRINT
© FORTINET

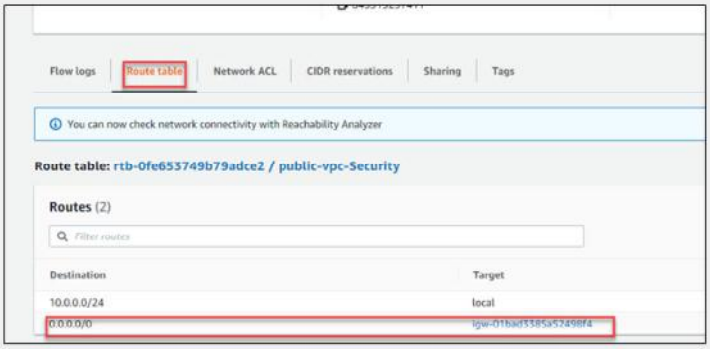


DO NOT REPRINT
© FORTINET

Lab1-Task 1—Access the FortiGate Instances

- There is no IGW attached to the Security VPC
- Create an IGW attached it to the Security VPC
- Attach the IGW to **sec-vpc-public1** subnet
- Create a `0.0.0.0/0` destination route to go through IGW





FORTINET Training Institute

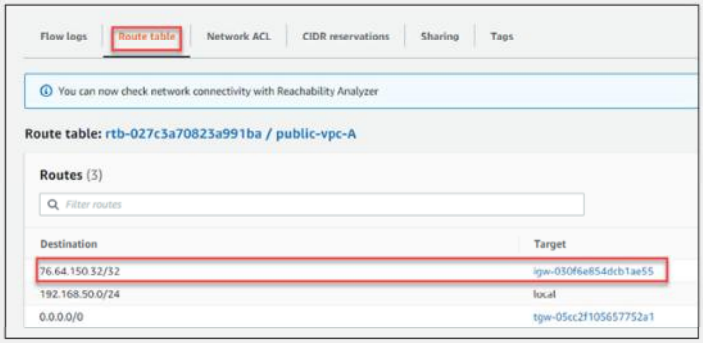
© Fortinet Inc. All Rights Reserved.

3

DO NOT REPRINT
© FORTINET

Lab1-To access the Linux instances

- Create two IGWs and attach to both Spoke-vpc-A and Spoke-vpc-B
- Edit main routing table public-vpc-A and B
- Add your local public IP address to go through the IGW
- Do not send `0.0.0.0/0` traffic to IGW



FORTINET Training Institute

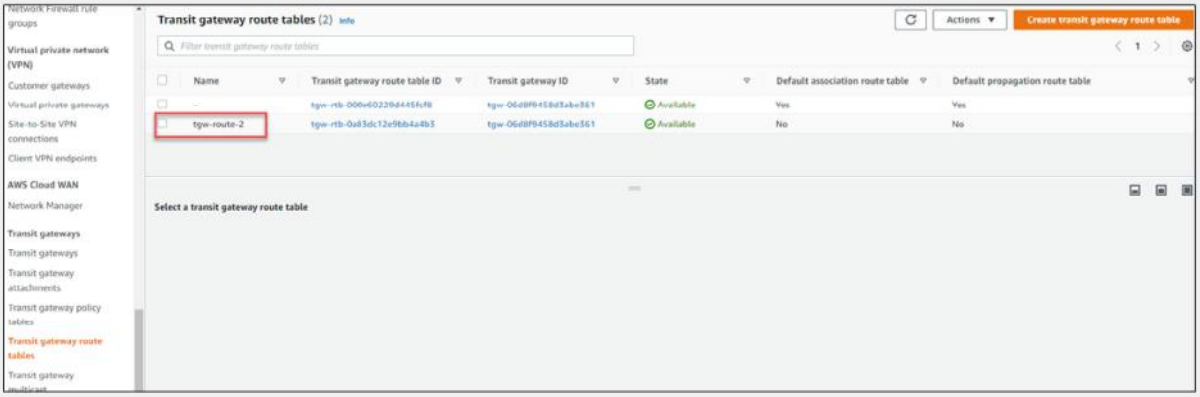
© Fortinet Inc. All Rights Reserved.

4

DO NOT REPRINT
© FORTINET

LAB1—Exercise—5—Task 1—Configure East-West Traffic Between Two Linux Instances

- There is only one TGW route table and all four attachments (vpc-A, vpc-B,Security vpc and connect) are attached to the same routing table
- So east-west traffic is not reaching the Security VPC FortiGate
- Create one more TGW route table



FORTINET Training Institute

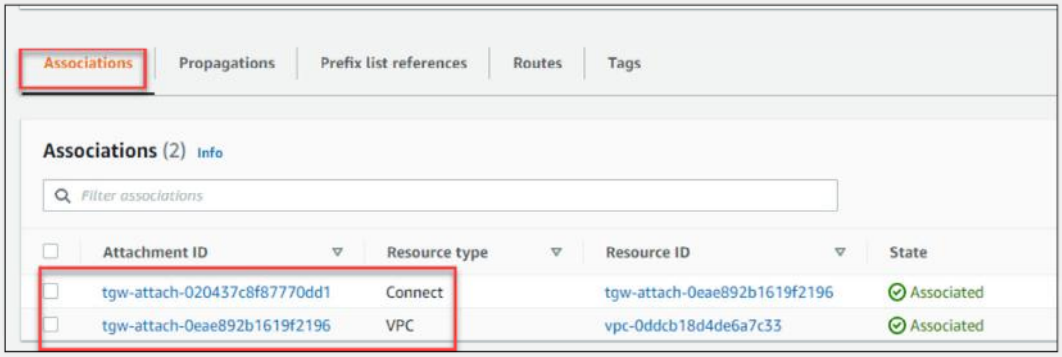
© Fortinet Inc. All Rights Reserved.

5

DO NOT REPRINT
© FORTINET

LAB1—Exercise—5—Task 1—Configure East-West Traffic Between Two Linux Instances (Contd)

- **TGW Route table 1** (Default route table)
  - **Association**- attach both **Security VPC attachment** and **Connect attachment**



FORTINET Training Institute

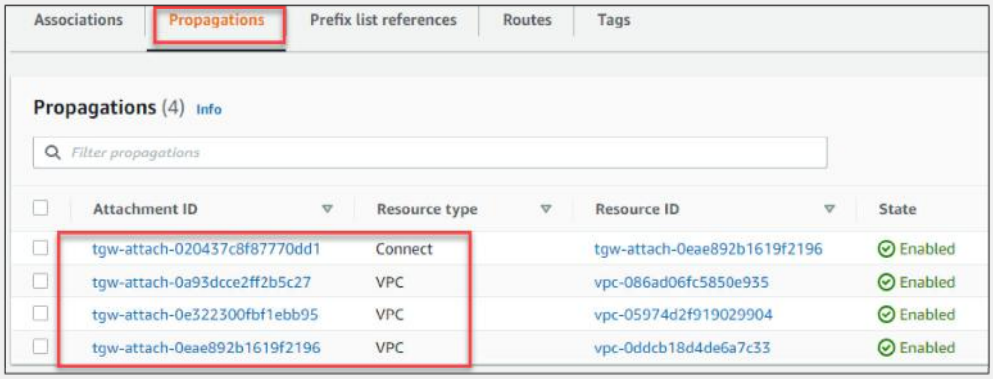
© Fortinet Inc. All Rights Reserved.

6

DO NOT REPRINT
© FORTINET

LAB1—Exercise—5—Task 1—Configure East-West Traffic Between Two Linux Instances (Contd)

- **TGW Route table 1** (Default route table)
  - **Propagation**- You can propagate all the attachments here



FORTINET Training Institute

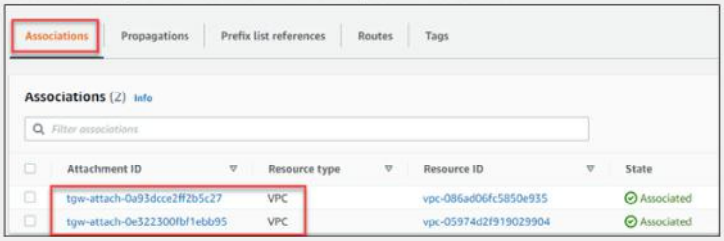
© Fortinet Inc. All Rights Reserved.

7

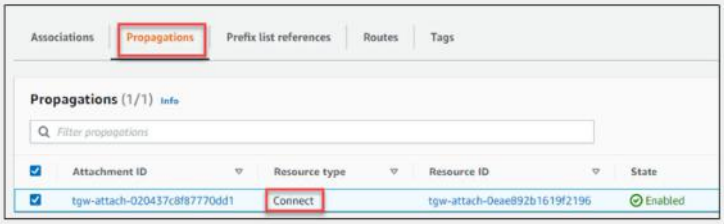
DO NOT REPRINT
© FORTINET

LAB1—Exercise—5—Task 1—Configure East-West Traffic Between Two Linux Instances (Contd)

- **TGW Route table 2 (New route table)**
  - **Association**- attach both **vpc-A** attachment and **vpc-B** attachment



  - **Propagation**-Attach **connect** attachment here



FORTINET Training Institute

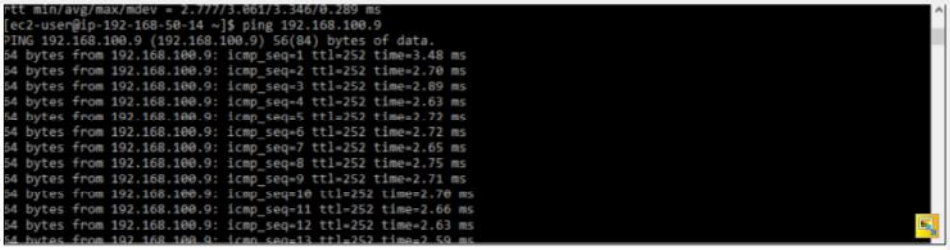
© Fortinet Inc. All Rights Reserved.

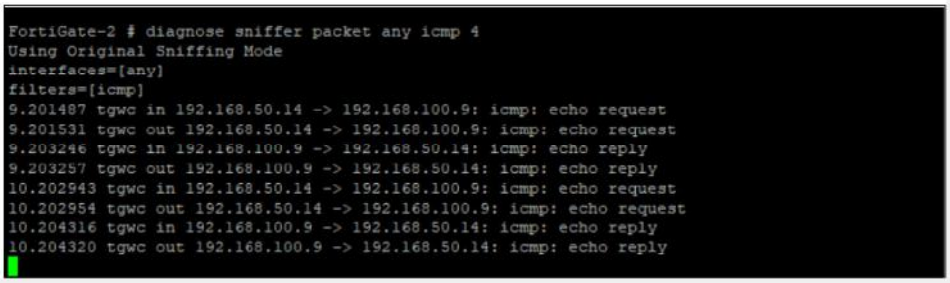
8

DO NOT REPRINT
© FORTINET

Traffic Reaching FGT

- Ping from Linux1 to Linux2, force traffic to go through security-vpc (East-west traffic)



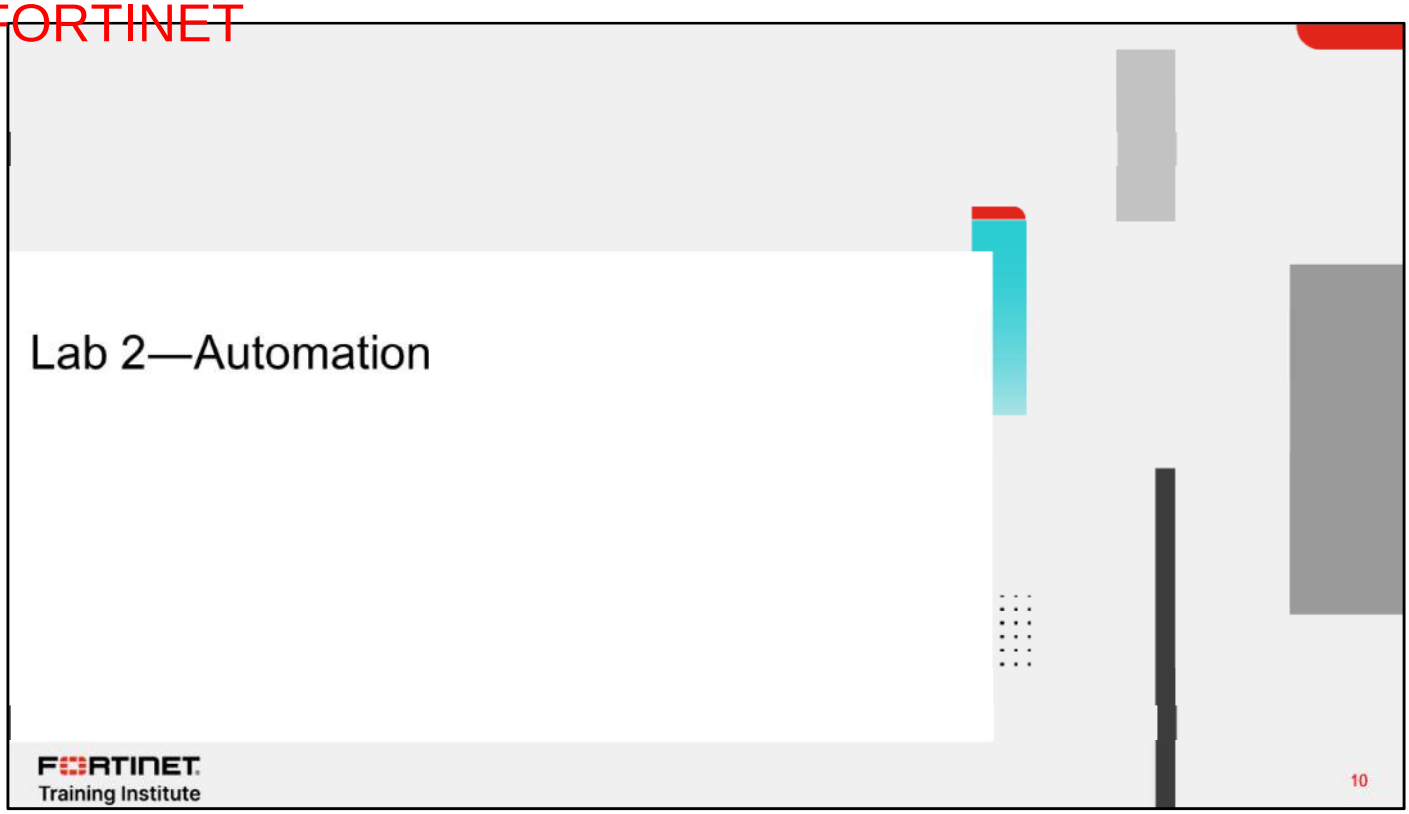


FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

DO NOT REPRINT
© FORTINET



DO NOT REPRINT
© FORTINET

Lab2-Task 2—Change the Deployment Location

- Edit variables.tf file
  - Change the default region and az1 to **us-east-2**

297 lines (280 sloc) | 6.16 KB

```
1   //AWS Configuration
2   variable "access_key" {}
3   variable "secret_key" {}
4
5   variable "region" {
6     default = "eu-west-1"
7   }
8
9   // Availability zones for the region
10  variable "az1" {
11    default = "eu-west-1a"
12  }
13
14  variable "vpccidr" {
15    default = "10.1.0.0/16"
16  }
17
18  variable "publiccidraz1" {
19    default = "10.1.0.0/24"
20  }
21
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

DO NOT REPRINT
© FORTINET

Task 3—Change the License Type

- Edit the varibles.tf file and make sure license type set to **payg**

```
26
27  // License Type to create FortiGate-VM
28  // Provide the license type for FortiGate-VM Instances, either byol or payg.
29  variable "license_type" {
30    default = "payg"
31  }
32
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

DO NOT REPRINT
© FORTINET

Task 4—Add AWS Key Pair Details

- Only provide AWS Key name reference

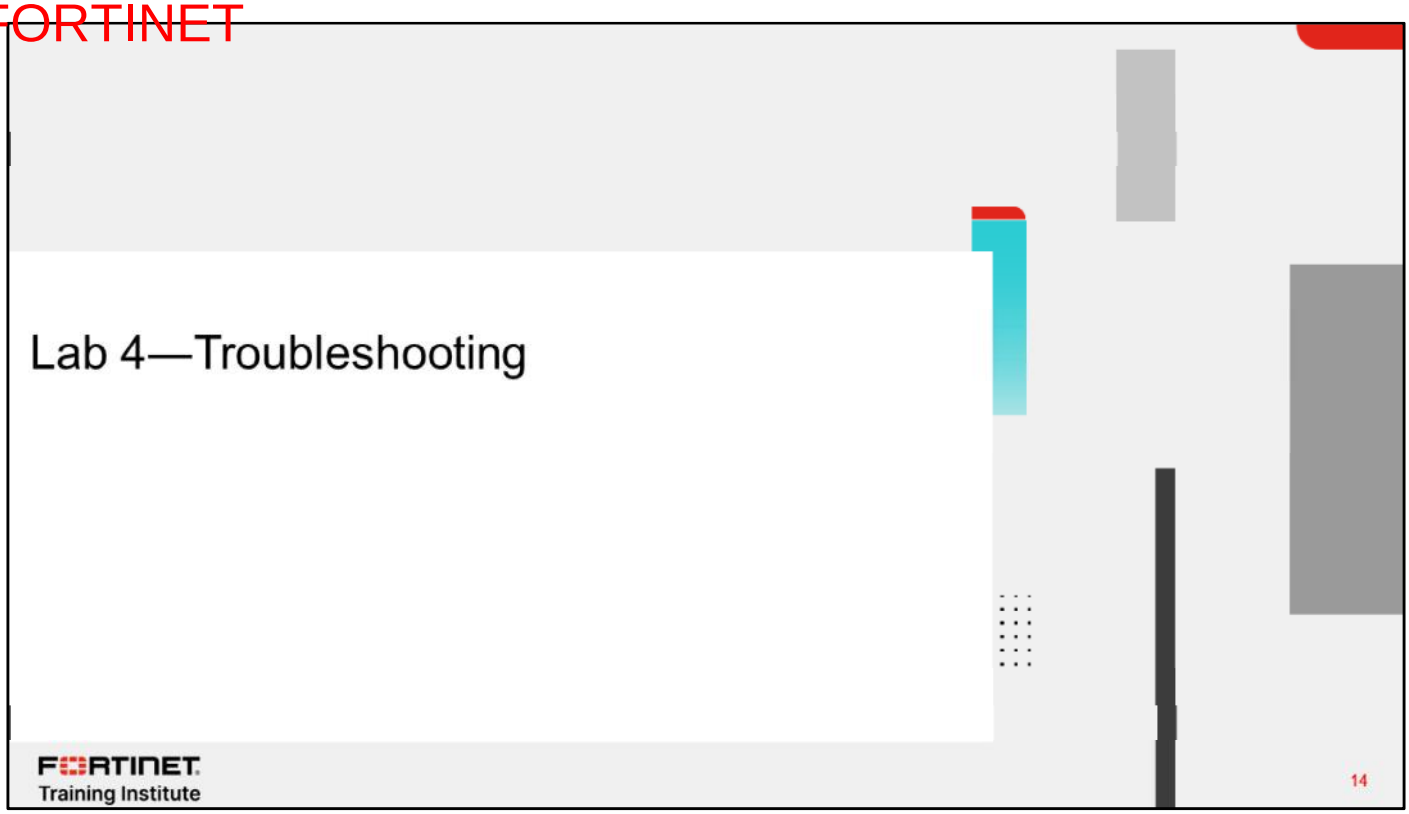
```
274  }
275
276  //  Existing SSH Key on the AWS
277  variable "keyname" {
278    default = "<AWS SSH KEY>"
279  }
280
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

DO NOT REPRINT
© FORTINET



DO NOT REPRINT
© FORTINET

LAB4-Service Principle Error

- Make sure tenant ID and other credentials are correct on your Terraform

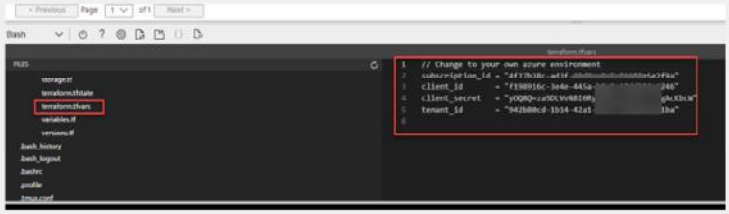
```
n@Azure:~/NSE7/terraform/Troubleshooting$ terraform plan

Error: building account: getting authenticated object ID: listing Service Principals: ServicePrincipalsClient.BaseClient.Get(): clientCredentialsToken: received HTT
P status 400 with response: {"error":"invalid_request","error_description":"AADSTS90002: Tenant '942b80cd-1b14-42a1-8dcf-4b21dece61bb' not found. Check to make sure y
ou have the correct tenant ID and are signing into the correct cloud. Check with your subscription administrator, this may happen if there are no active subscriptions
 for the tenant.\r\nTrace ID: fb39a7b9-1dc9-4d3f-a6c8-7f0569cf5600\r\nCorrelation ID: 81872e60-4daf-472a-967b-69960d36b66e\r\nTimestamp: 2022-09-14 19:53:26Z","error_
codes":[90002],"timestamp":"2022-09-14 19:53:26Z","trace_id":"fb39a7b9-1dc9-4d3f-a6c8-7f0569cf5600","correlation_id":"81872e60-4daf-472a-967b-69960d36b66e","error_uri
":"https://login.microsoftonline.com/error?code=90002"}

  with provider["registry.terraform.io/hashicorp/azurerm"],
  on provider.tf line 1, in provider "azurerm":
   1: provider "azurerm" {

n@Azure:~/NSE7/terraform/Troubleshooting$
```

- Edit **terraform.tfvars** file and add your Azure credentials



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

DO NOT REPRINT
© FORTINET

LAB4-Subnet Error

- Check variables.tf file and make sure your CIDRs are correct

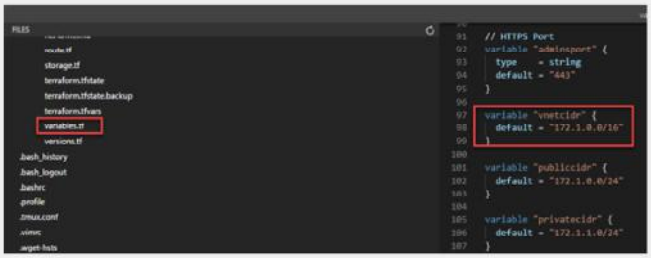
```
azurerm_network_security_rule.outgoing_public: Creation complete after 11s [id=/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/NSE7-TSGRP/providers
/Microsoft.Network/networkSecurityGroups/PublicNetworkSecurityGroup/securityRules/egress]
azurerm_storage_account.fgtstorageaccount: Still creating... [20s elapsed]
azurerm_storage_account.fgtstorageaccount: Creation complete after 24s [id=/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/NSE7-TSGRP/providers/Mic
rosoft.Storage/storageAccounts/diagd767935ee3733ff3]

Error: creating Subnet: (Name "publicSubnet" / Virtual Network Name "fgtvnetwork" / Resource Group "NSE7-TSGRP"): network.SubnetsClient#CreateOrUpdate: Failure send
ing request: StatusCode=400 -- Original Error: Code="NetcfgInvalidSubnet" Message="Subnet 'publicSubnet' is not valid in virtual network 'fgtvnetwork'." Details=[]

  with azurerm_subnet.publicsubnet,
  on network.tf line 14, in resource "azurerm_subnet" "publicsubnet":
  14: resource "azurerm_subnet" "publicsubnet" {


Error: creating Subnet: (Name "privateSubnet" / Virtual Network Name "fgtvnetwork" / Resource Group "NSE7-TSGRP"): network.SubnetsClient#CreateOrUpdate: Failure sen
```

- Edit **variables.tf** file and Change the **vnetcidr** to `172.1.0.0/16`



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

DO NOT REPRINT
© FORTINET

LAB4-Purchase Validation Error

- Edit **variable.tf** file and make sure to match the following table

Name	Value
publisher	fortinet
fgtoffer	fortinet_fortigate-vm_v5
fgtsku	fortinet_fg-vm_payg_2022

```
54
55  variable "publisher" {
56    type    = string
57    default = "fortinet"
58  }
59
60  variable "fgtoffer" {
61    type    = string
62    default = "fortinet_fortigate-vm_v5"
63  }
64
65  // BYOL sku: fortinet_fg-vm
66  // PAYG sku: fortinet_fg-vm_payg_2022
67  variable "fgtsku" {
68    type = map(any)
69    default = {
70      byol = "fortinet_fg-vm"
71      payg = "fortinet_fg-vm_payg_2022"
72    }
73  }
74
75  // FOS version
76  variable "fgtversion" {
77    type    = string
78    default = "7.2.1"
79  }
80
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

DO NOT REPRINT
© FORTINET

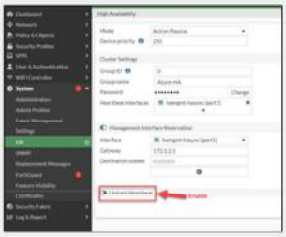
LAB4-Exercise 2-Access FGT

- Check the inbound network security group rules and make the necessary changes to allow access to HTTPS and SSH.
  - Delete deny rules and add two new rules for HTTPS and SSH

- HA is not Synchronizing issue
  - Make sure to enable Unicast Heartbeat from Primary device
  - Set the peer IP address on Primary to 172.1.3.11
  - Synchronize

```
config system ha
set unicast-hb enable
set unicast-hb-peerip 172.1.3.11
end
```

```
execute ha synchronize start
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

DO NOT REPRINT
© FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 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.