

DO NOT REPRINT
© FORTINET

FORTINET

**Network
Security
Expert**

7

Public Cloud Security Study Guide

for FortiGate 6.0 and FortiWeb 6.0

FORTINET

NSE

**NSE
Certification
Program**

DO NOT REPRINT © FORTINET

Fortinet Training

<http://www.fortinet.com/training>

Fortinet Document Library

<http://docs.fortinet.com>

Fortinet Knowledge Base

<http://kb.fortinet.com>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<http://www.fortiguard.com>

Fortinet Network Security Expert Program (NSE)

<https://www.fortinet.com/support-and-training/training/network-security-expert-program.html>

Feedback

Email: courseware@fortinet.com



TABLE OF CONTENTS



01 Introduction to the Public Cloud.....	4
02 Fortinet Solutions for the Public Cloud.....	24
03 Fortinet Solution for AWS.....	47
04 Fortinet Solution for Microsoft Azure.....	95
05 Fortinet Solution for Google Cloud Platform.....	138
06 FortiCWP and FortiCASB.....	163

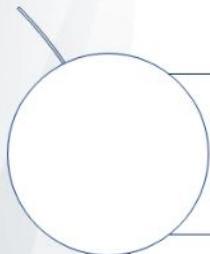
DO NOT REPRINT
© FORTINET



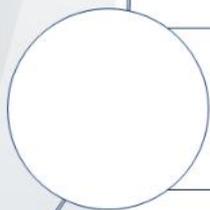
In this lesson, you will learn about public cloud security.

**DO NOT REPRINT
© FORTINET**

Lesson Overview



Public Cloud Fundamentals



Networking in Public Cloud

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

**DO NOT REPRINT
© FORTINET**

Public Cloud Fundamentals

Objectives

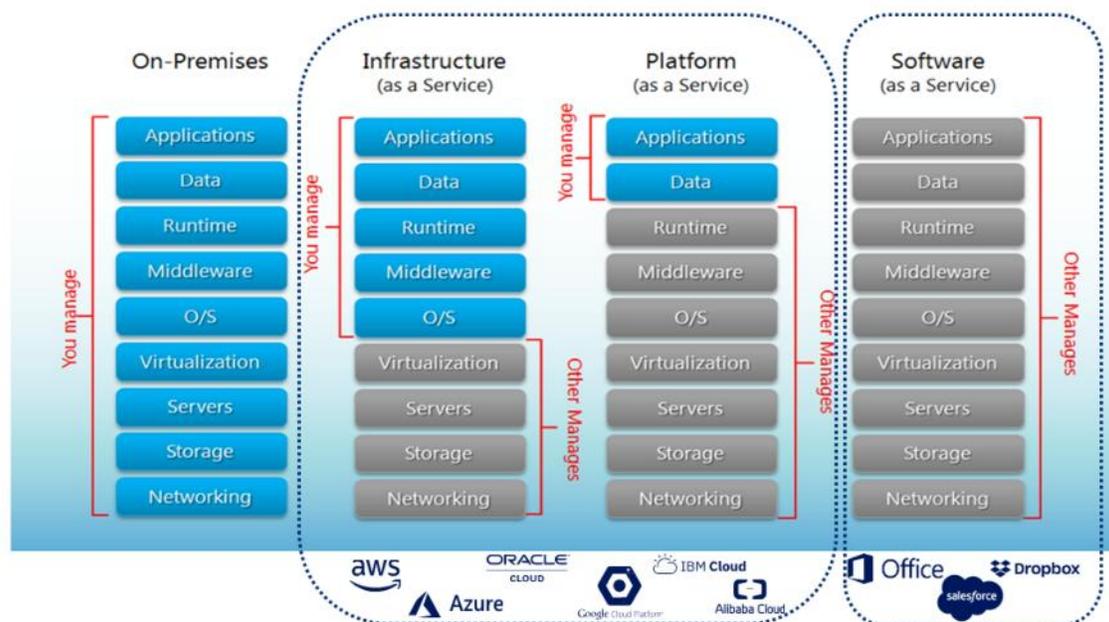
- Understand the concept of public cloud
- Know the public cloud vendors
- Know the public cloud components
- Understand public cloud security
- Understand hybrid cloud

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

By demonstrating competence in understanding the fundamentals of public cloud, you will be able to understand how public cloud applies to your network.

DO NOT REPRINT
© FORTINET

No Single Concept of Public Cloud



FORTINET

© Fortinet Inc. All Rights Reserved.

4

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 virtual machines (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), 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

Who Are the Players?



Google Cloud Platform



And many more...

FORTINET

© Fortinet Inc. All Rights Reserved.

5

An IaaS solution involves multiple vendors. The most popular vendors are AWS and Azure. The cloud solution vendor AWS is the most popular in North America, Azure is the most popular in the rest of the world. Other cloud solution vendors are Google Cloud, IBM Cloud, ORACLE Cloud, and Alibaba Cloud, to name a few.

DO NOT REPRINT
© FORTINET

Cheat Sheet–Vendor Service Names

Service category	Service	Amazon Web Services	Azure	Google Cloud Platform
Compute	IaaS	Amazon Elastic Compute Cloud (EC2)	Virtual Machines	Google Compute Engine
	PaaS	AWS Elastic Beanstalk	App Service, Cloud Services	Google App Engine
	Containers	Amazon Elastic Compute Cloud Container Service	Azure Container Service, Azure Service Fabric	Google Kubernetes Engine
Network	Serverless functions	AWS Lambda	Function	Google Cloud Functions
	Virtual networks	AWS VPC	Azure VNets	VPC networks
	Load Balancer	Elastic Load Balancer (ELB)	Azure Load Balancer, Application Gateway	Google Cloud Load Balancing
	Dedicated Interconnect / Peering	Direct Connect	ExpressRoute	Google Cloud Interconnect
	DNS	Amazon Route 53	Azure DNS	Google Cloud DNS
Storage	CDN	Amazon CloudFront	Azure CDN	Google Cloud CDN
	Object Storage	Amazon Simple Storage Service (S3)	Azure Blob Storage	Google Cloud Storage
	Block Storage	Amazon Elastic Block Store	Disk Storage	Google Compute Engine persistent disks
	File Storage	Amazon Elastic File System	Azure File Storage	ZFS / Avere
	Reduced-availability Storage	Amazon S3 Reduced Redundancy Storage	Azure Cool Blob Storage	Google Cloud Storage Nearline
Database	RDBMS	Amazon Relational Database Service	SQL Database	Google Cloud SQL
	NoSQL: Key-value	Amazon DynamoDB	Table Storage	Google Cloud Datastore, Google Cloud Bigtable
	NoSQL: Indexed	Amazon SimpleDB	Cosmos DB	Google Cloud Datastore
Big Data & Analytics	Batch Data Processing	Amazon Elastic MapReduce	HDInsight, Batch	Google Cloud Dataproc, Google Cloud Dataflow
	Stream Data Processing	Amazon Kinesis	Stream Analytics	Google Cloud Dataflow
	Stream Data Ingest	Amazon Kinesis	Event Hubs, Service Bus	Google Cloud Pub/Sub
	Analytics	Amazon Redshift	Data Lake Analytics, Data Lake Store	Google BigQuery
Application Services	Messaging	Amazon Simple Notification Service	Service Bus	Google Cloud Pub/Sub
Management Services	Monitoring	Amazon CloudWatch	Application Insights	Stackdriver Monitoring
	Logging	Amazon CloudWatch	Application Insights	Stackdriver Logging
	Deployment	AWS CloudFormation	Azure Resource Manager	Google Cloud Deployment Manager

Also check: <https://docs.microsoft.com/en-us/azure/architecture/aws-professional/services>

FORTINET

© Fortinet Inc. All Rights Reserved.

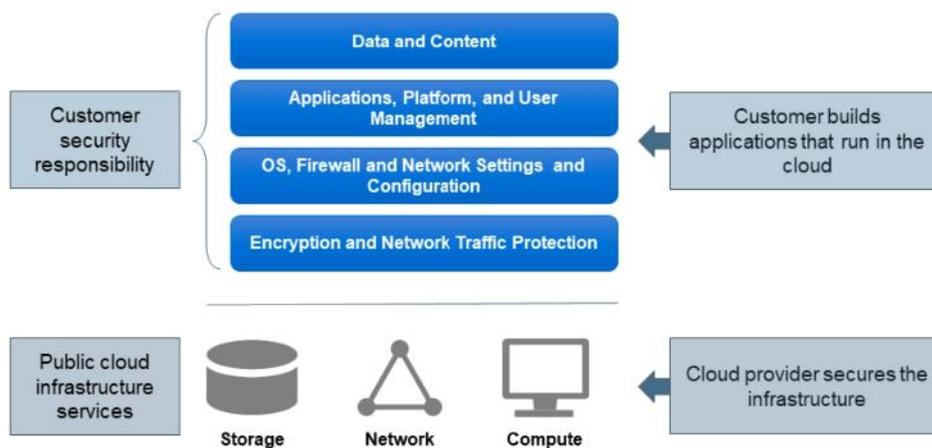
6

Vendor service names are vendor specific. As shown on this cheat sheet, the VM is named differently for each vendor. For example, the Amazon Web Services VM is named Amazon Elastic Compute Cloud (EC2). For Azure, the VM is named as Virtual Machines, and for Google Cloud Platform, the VM is named Google Compute Engine. There are also different names for DNS. For example, Amazon Route 53, Azure DNS, and Google Cloud DNS. The content delivery network name is also based on the vendor, such as Amazon Cloudfront, Azure CDN, and Google Cloud CDN.

DO NOT REPRINT
© FORTINET

Security–Shared Responsibility

- The majority of cloud security is the responsibility of the user, not the provider



FORTINET

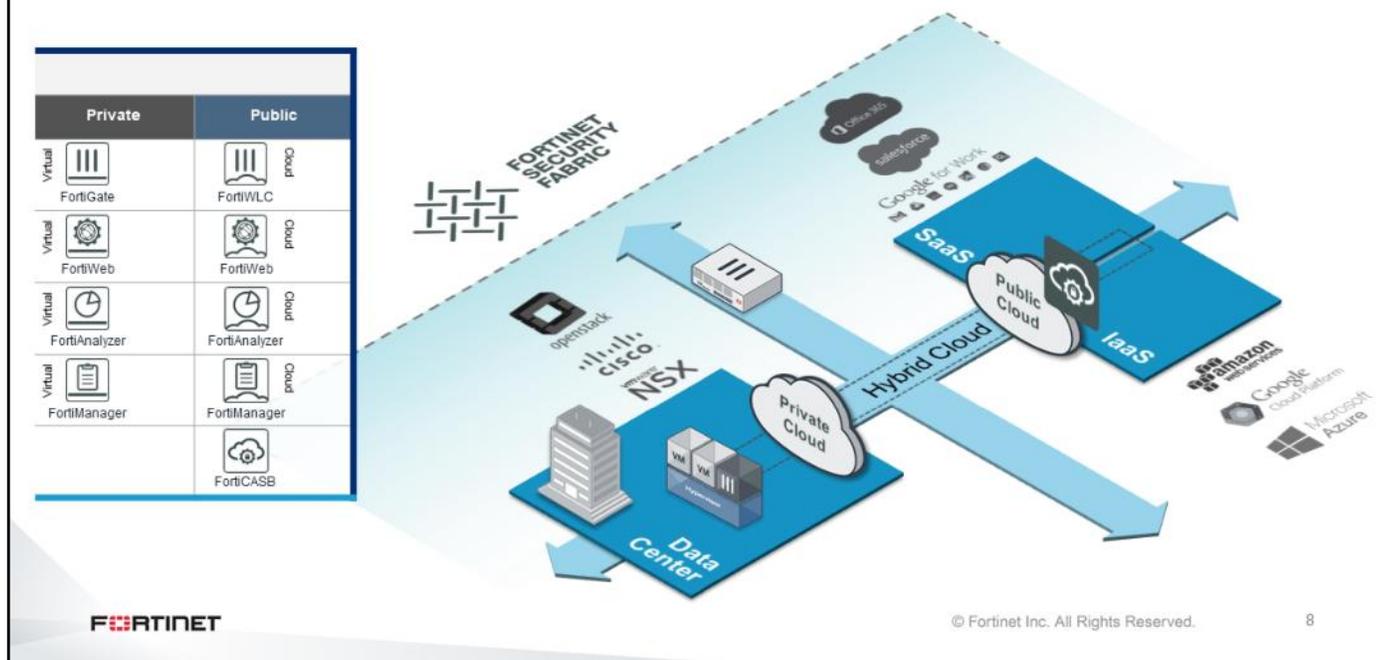
© Fortinet Inc. All Rights Reserved.

7

This slide shows the cloud security shared responsibility model. The lower stack includes the elements that are provided and, therefore, secured by the cloud service provider. Cloud *customers* are responsible for securing the remaining elements—network, applications, and data. The cloud security model is commonly broken down using the familiar OSI layers model; however, the OSI layers model doesn't represent the security responsibility breakdown. In some cases, cloud users will build overlay networks on top of the cloud network, or layer additional services on top of existing infrastructure services. In cases like these, responsibility for the security of the modified infrastructure belongs to the customer. Essentially, if you manage it, you are responsible for it.

DO NOT REPRINT
© FORTINET

Hybrid Cloud—The Best of Both Worlds



Hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud, and third-party, public cloud services, with orchestration between the two platforms. This scenario can be found in enterprises that are moving to the cloud. A hybrid cloud environment accommodates applications that should run only on-premises and applications that can run on only a public cloud. A hybrid cloud lets you allocate public cloud resources for short-term projects, at a lower cost than using your own data center's IT infrastructure. That way, you don't overinvest in equipment that you will need only temporarily. For example a customer could choose to run an ecommerce application locally during the normal sale days, but then use a paid public cloud service to run the same ecommerce application during a peak sales event like Black Friday, when more computing power is needed to meet the higher sales demand.

**DO NOT REPRINT
© FORTINET**

Networking in Public Cloud

Objectives

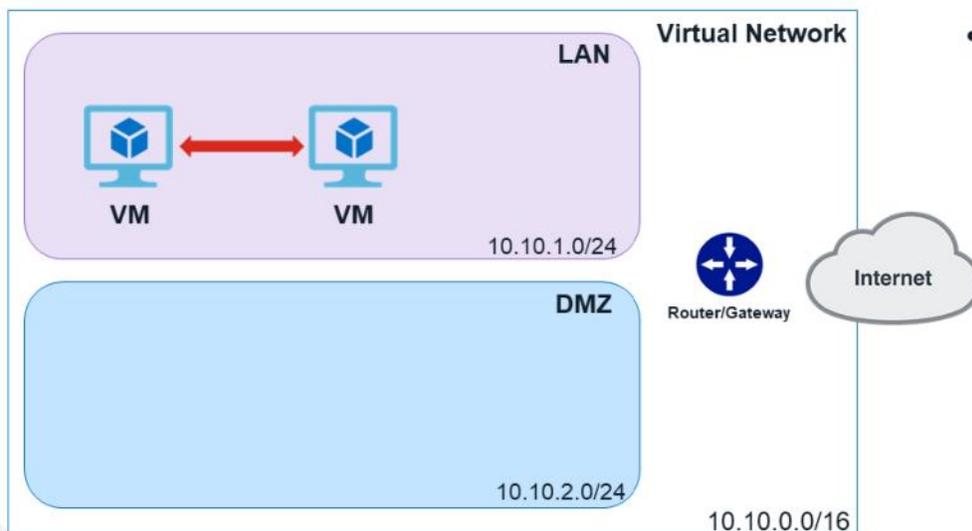
- Understand traffic flow in a virtual network
- Understand Layer 2 traffic flow
- Understand routing and restrictions
- Understand the role of access control lists

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

By demonstrating competence in networking in public cloud, you will be able to understand traffic flow and how to manipulate traffic using routes in a virtual network.

DO NOT REPRINT
© FORTINET

Virtual Network–Traffic Flow



- **Within a subnet**

FORTINET

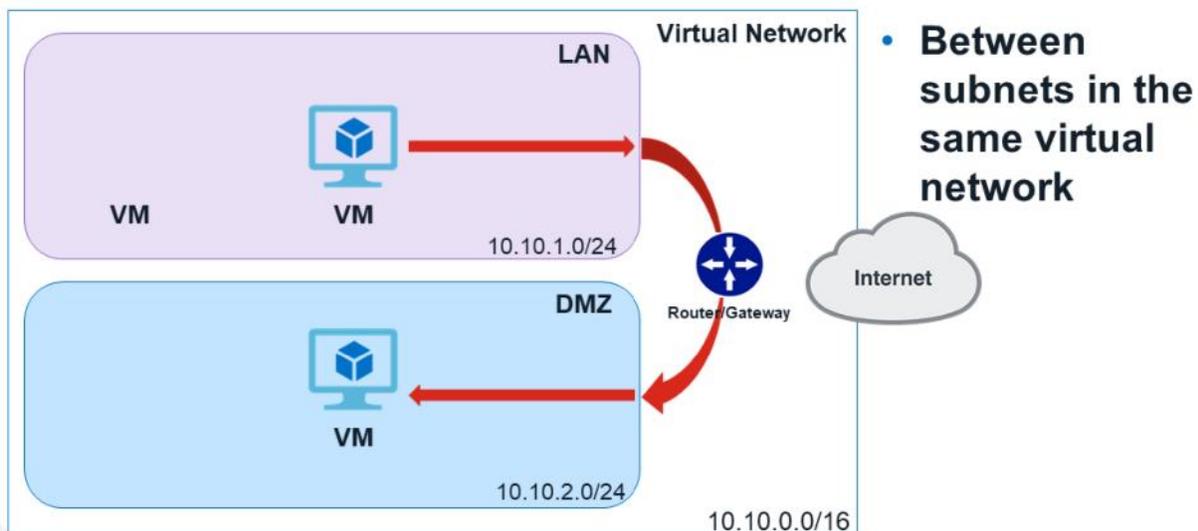
© Fortinet Inc. All Rights Reserved.

10

Now you will learn about traffic flow in a virtual network. As shown on this slide, there is a virtual network. The virtual network is a group of different subnets within the same networking block. The name of the virtual network is based on the vendor. In AWS, the virtual network is called VPC, and in Azure, it is called Vnet, but in general, it is called virtual network. Within the virtual network, there are different subnets, for example LAN subnet and DMZ subnet. Every virtual network contains a central router. At a first glance, the virtual network seems to have a very simple setup—one virtual machine (VM) needs connect to another VM which is in the same network. However, the setup is not as simple as appears on this slide.

DO NOT REPRINT
© FORTINET

Virtual Network–Traffic Flow (Contd)



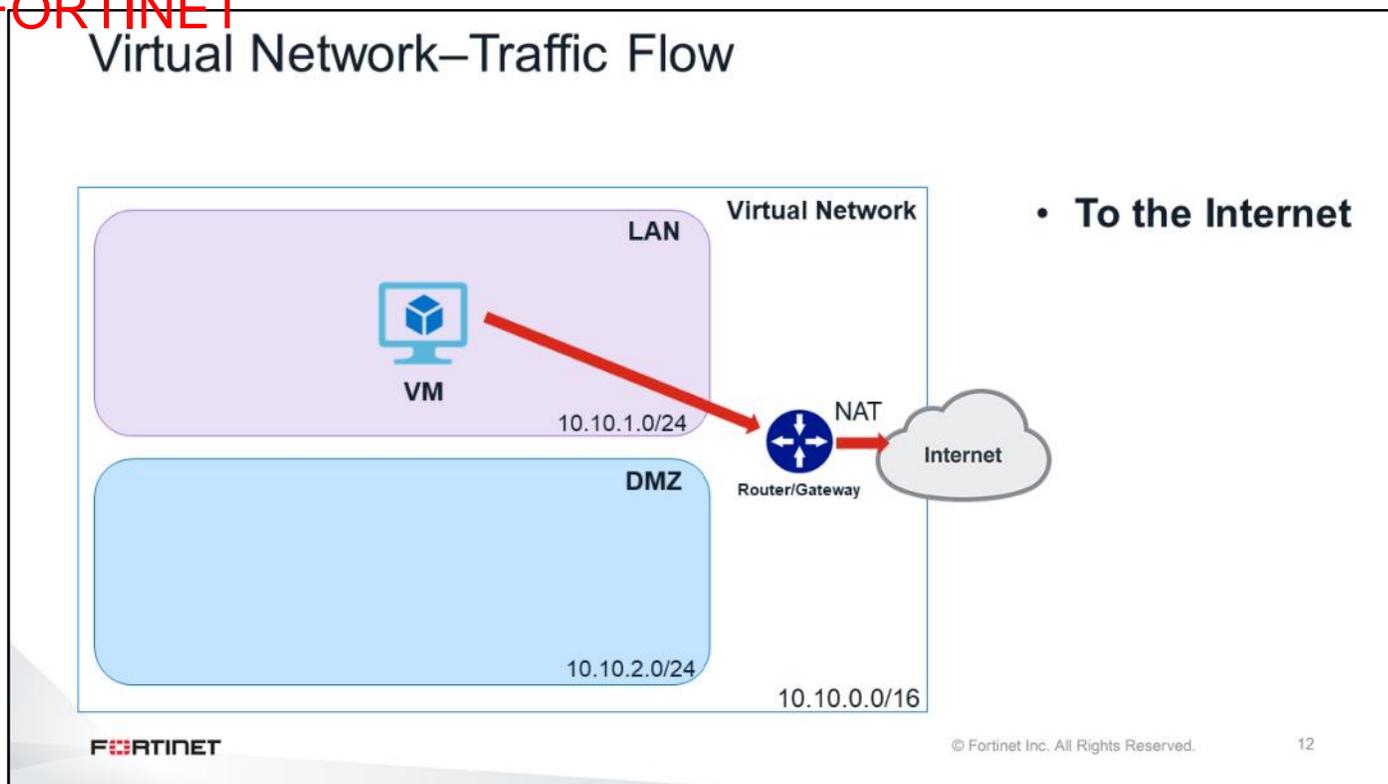
FORTINET

© Fortinet Inc. All Rights Reserved.

11

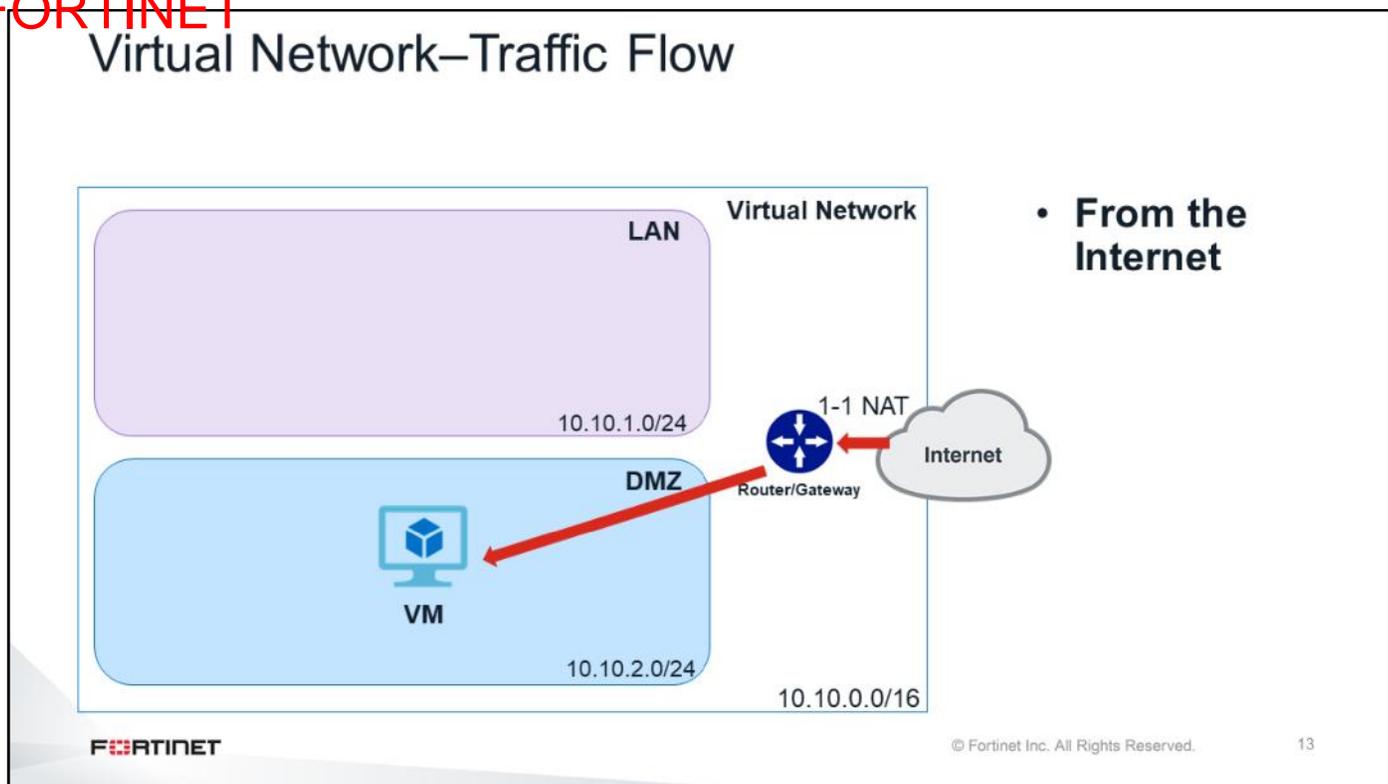
In the scenario shown on this slide, two VMs connect to each other using a router, basically connecting between subnets in the same virtual network using a router.

DO NOT REPRINT
© FORTINET



When a VM needs to connect to the Internet, it must first connect to the router that sits between it and the Internet. In this scenario, traffic must NAT using a router that sits between the private IP address and the public IP address. The VM cannot have a public IP address on its network interface. The public IP address is managed by the cloud vendor.

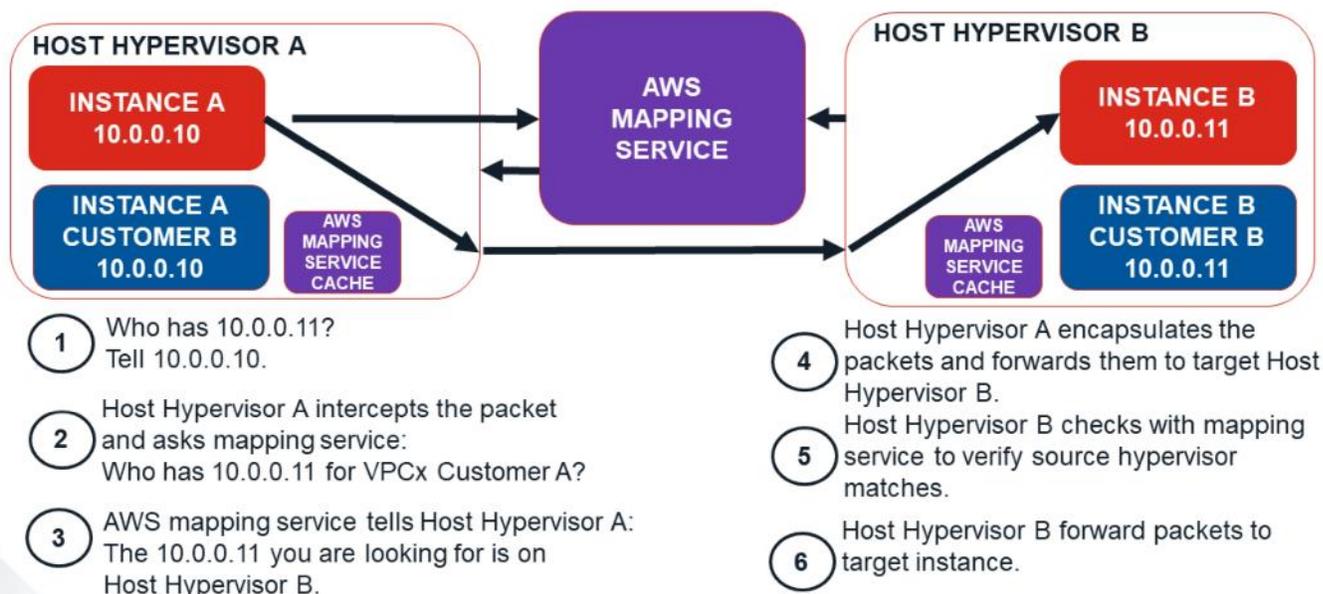
DO NOT REPRINT
© FORTINET



How does the traffic flow from the Internet to the VM? One-to-one NAT connects the Internet to the VM. Note that all the VMs have a private IP address on their interface and cannot have a public IP address. Configuring a public IP address on the VM interface is a mistake that is commonly made by administrators.

DO NOT REPRINT
© FORTINET

Layer 2–AWS Example for Same Subnet Traffic



FORTINET

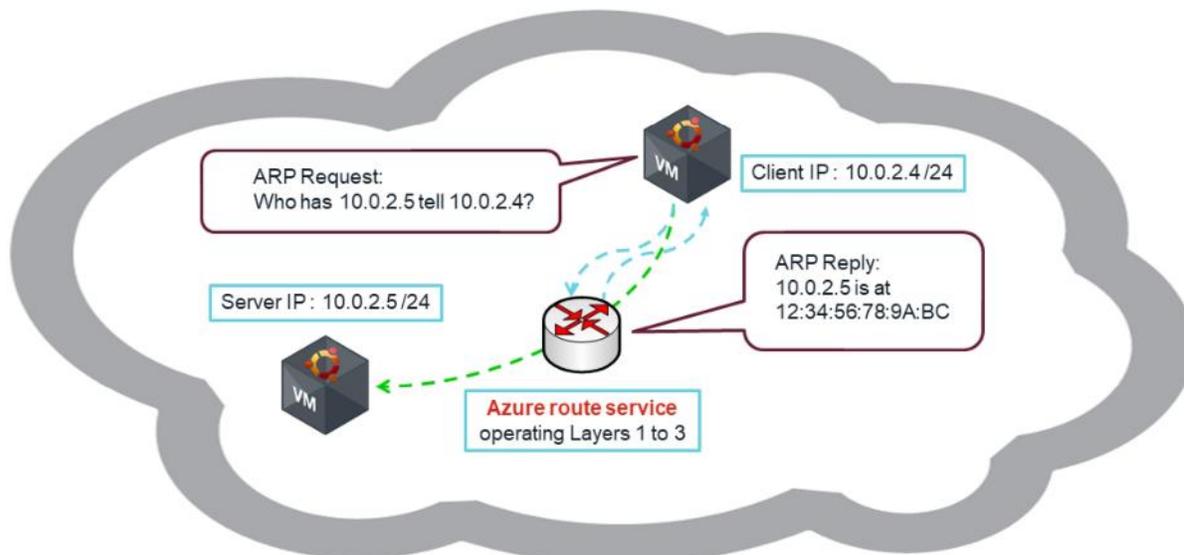
© Fortinet Inc. All Rights Reserved.

14

Now you will learn about Layer 2 networking in AWS cloud computing. Layer 2 networking works differently in cloud computing. How does instance A communicate with instance B? As computer nodes in a regular network, instance B must do the ARP request; therefore, do the broadcast requesting the MAC address. However, in the cloud environment, there could be thousands of machines between two instances generating lots of broadcast traffic in cloud switches, which is very problematic. So, what solution minimizes the vast amount of broadcast traffic in cloud computing? The solution is the AWS mapping service, which contains all the MAC addresses and IP addresses of the subnet as a database. As shown in this scenario, AWS mapping service is responsible for capturing the request packet and replying with the correct MAC address, of instance B. AWS mapping service then checks its database for the correct IP address and corresponding MAC address, then the traffic flows from MAC address to the MAC address on instance B. So, there is no broadcast going over the network. It is important to know that you must assign and declare all your VM IP addresses in cloud portal. The cloud vendor console must sync IP information with the VMs. If you add an IP address to the VM, you must add the IP addresses to the configuration of the cloud console. Also, there is a cache service available inside the physical host which records all the information. If you change the IP address of the VM, it may take some time to update that information in the cache service; especially if you encounter any connectivity issues after changing the IP address of the host.

DO NOT REPRINT
© FORTINET

Layer 2–ARP Traffic in Azure



FORTINET

© Fortinet Inc. All Rights Reserved.

15

The Azure networking component manages all ARP traffic. In the scenario shown on this slide, Azure route service is responsible for ARP reply. When client IP 10.0.2.4 does the ARP request, Azure route service always replies with the MAC address 12:34:56:78:9A:BC. If you check the ARP table, you will see the same MAC address for all the neighbors; however, if AWS is used, you will see actual MAC addresses of the VMs. Keep in mind that all the traffic always directs to the route service. When client A wants to talk to client B, client A generates a unicast packet directed to the MAC address 12:34:56:78:9A:BC. The mapping service does the sort of destination NAT to the MAC address, and replaces the actual MAC address of the destination VM. Note that Azure route service is not actually a router, but a service that facilitates communication between VMs.

DO NOT REPRINT**© FORTINET**

Layer 2–Restrictions

- An instance will receive traffic only on an IP address defined in the cloud console
- No static or virtual IP addresses on the VM without matching the cloud console
- No traditional Layer 2
 - Only packets destined for an IP address will leave an instance; all other traffic is dropped. This means:
 - No FGCP
 - No gratuitous ARP or proxy ARP
 - No instant IP failover
 - No custom frames/ethertypes/L2 manipulation
 - No multicast or broadcast
 - No 802.1q
- All Layer 2 modes are forbidden: transparent or virtual wire

* Not all restrictions apply to all cloud vendors and some vendors have additional restrictions.

FORTINET

© Fortinet Inc. All Rights Reserved.

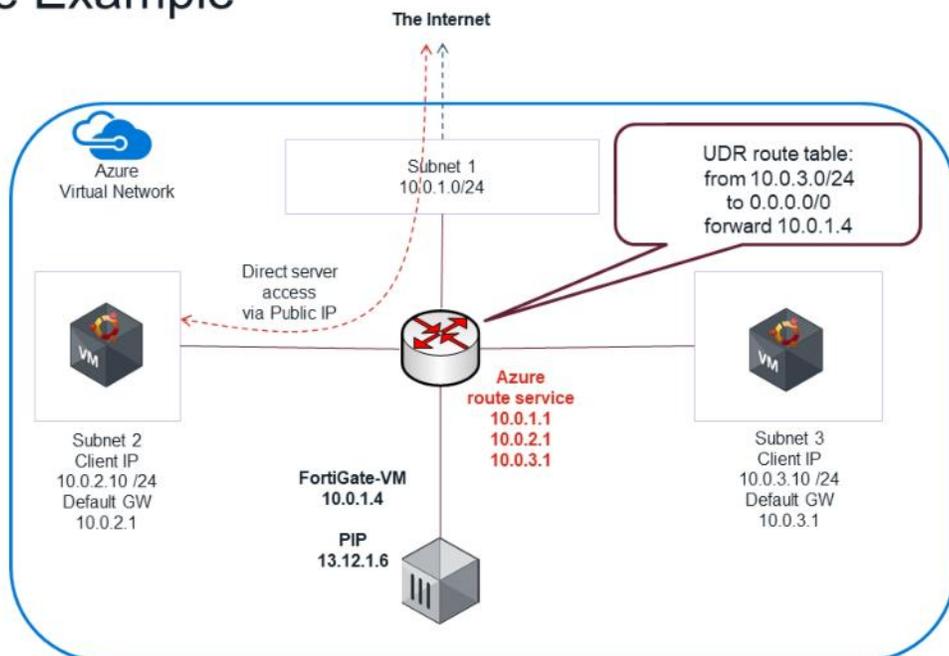
16

Now you will learn about Layer 2 restrictions in cloud computing. An instance will only receive the traffic if the IP address is defined in the cloud console. If there are static or virtual IP addresses configured on the virtual machine, you must make sure that those IP addresses are configured on the cloud console as well. In terms of Layer 2 restrictions, there shouldn't be any traditional Layer 2 traffic such as FortiGate clustering protocol, gratuitous ARP, instant IP failover and, so on. Basically there is no broadcast or multicast traffic in cloud computing; only unicast traffic is allowed. Also no Layer 2 modes are allowed in cloud computing, for example, transparent mode or virtual wire.

DO NOT REPRINT
© FORTINET

Routing–Azure Example

- Public IP (PIP) would be directly associated with a VM giving direct Internet access
- Having a routing firewall requires user defined routes (UDRs)
- VMs always speak to Azure route service first



FORTINET

© Fortinet Inc. All Rights Reserved.

17

In Azure you can use user defined routes. An administrator can configure all the routes to force traffic to the correct destinations. UDRs are similar to the policy routes in FortiGate. Shown on this slide are two VMs and one FortiGate device. If the VM in subnet 3 needs to connect to the Internet, the administrator can configure a UDR to force traffic to FortiGate first, then from FortiGate to the Internet. In this scenario traffic can be inspected by FortiGate before going out to the Internet. Any traffic going to the Internet is source NATed to the public IP address; however, that public IP address is not configured directly on the FortiGate device. At the same time, the administrator can configure a route to inspect traffic going from one subnet to another. Traffic destined to subnet 2 from subnet 3 can be forced to go to FortiGate first then to subnet 2. As shown in this example FortiGate can have only a single interface for both incoming and outgoing traffic. When creating a policy, you can create a policy from port1 to port1, source 10.0.3.0/24 and destination 0.0.0.0/0 to go to the Internet.

Also keep in mind that the router shown on this slide does not exist, and it is only a service moving traffic based on the UDR. By default, can communicate directly out to the Internet. If they have a public IP (PIP) assigned, public clients can connect directly to any services enabled on these VMs.

DO NOT REPRINT
© FORTINET

Routing Restrictions

- Traffic entering a virtual network *always* goes through a routing table that you can configure on the cloud console
 - This traffic passes directly to the target instance through the embedded router
- Traffic leaving a VM instance *must* have a route from the local subnet router or it will be blackholed
- There is *always* an embedded router on every subnet
 - All VMs use the embedded router as default gateway

* Not all restrictions may apply to all cloud vendors. Some vendors have additional restrictions.

Now you will learn about routing restrictions in cloud computing. When traffic enters to the virtual network, it must first go through the routing table which is configured on the cloud console. At the same time, traffic leaving a VM instance must have a valid route from the local subnet router; otherwise, traffic will be blackholed. Keep in mind that there is always an embedded router on every subnet and all virtual machines use the embedded router as default gateway.

DO NOT REPRINT
© FORTINET

Access Control Lists

- Very basic capabilities:
 - Only Layer 4
 - Poor logging
 - Hard to maintain
- Names vary:
 - AWS has ACLs and security groups
 - Azure has network security groups and Azure firewall
- They are everywhere: vNIC, VM, subnet, load balancers, and more
- Keep them in mind when configuring and troubleshooting

Now, you will learn about the security aspect of the cloud computing. There are access control lists directly embedded to the networking part of cloud computing. However, these access control lists are very basic and have some limitations. ACLs only Layer 4, poor or no logging capabilities and are very hard to maintain. Moreover, access list names are based on vendor. For example, AWS has both ACLs and security groups, Azure has network security groups and Azure firewall. You will learn more about these lists in this course. Access control lists can be applied in different places, such as virtual NICs, VMs, and subnets, to name a few. Why is the cloud considered more secure than a traditional network? This is mainly related ACLs. ACLs can be directly applied on to network interfaces and help to secure east-west traffic, by default. Keep in mind that if you encounter any issues during the lab and troubleshooting, it could be an ACL, so you need to pay extra attention during the labs.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand the concept of public cloud
- ✓ Identify public cloud components, security, and hybrid cloud
- ✓ Understand traffic flow in a virtual network
- ✓ Identify Layer 2 traffic flow and routing
- ✓ Understand the role of access control lists

This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned the concept of public cloud and how to use it in your network.

DO NOT REPRINT
© FORTINET



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

**DO NOT REPRINT
© FORTINET**

Fortinet Solutions for the Public Cloud

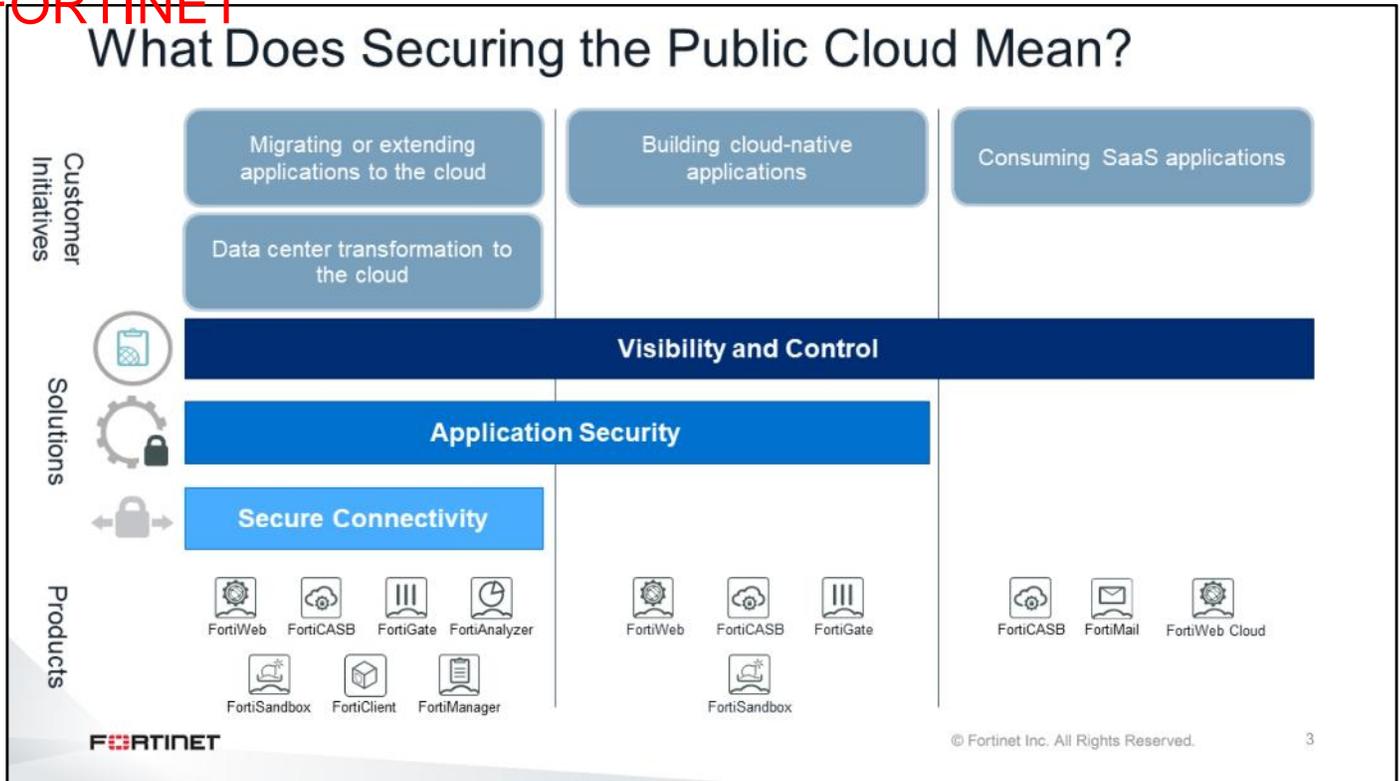
Objectives

- Secure the public cloud
- Understand licensing models
- Understand high availability (HA), load balancer, and autoscaling
- Be familiar with Fortinet Github

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

By demonstrating competence in understanding Fortinet solutions for the public cloud, you will be able to secure your cloud network using Fortinet solutions.

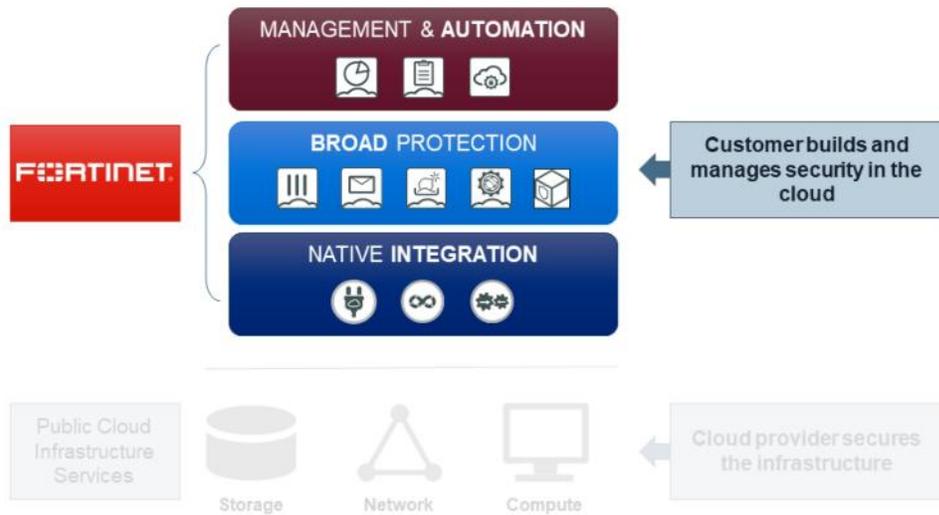
DO NOT REPRINT
© FORTINET



There are three Fortinet solutions for securing the public cloud: the secure connectivity solution, which belongs to the category of infrastructure as a service (IaaS); application security; and visibility and control. Fortinet provides solutions for each of these categories. For example, Fortinet can provide secure connectivity for IaaS, but cannot provide the same solution for software as a service (SaaS) applications. So, for SaaS, Fortinet can provide only visibility and control. In other words, you cannot create an IPsec tunnel or web application firewall (WAF) to a Dropbox (SaaS).

DO NOT REPRINT
© FORTINET

Fortinet Can Help You Secure the Public Cloud



FORTINET

© Fortinet Inc. All Rights Reserved.

4

As shown on this slide, Fortinet can provide different products to secure the public cloud.

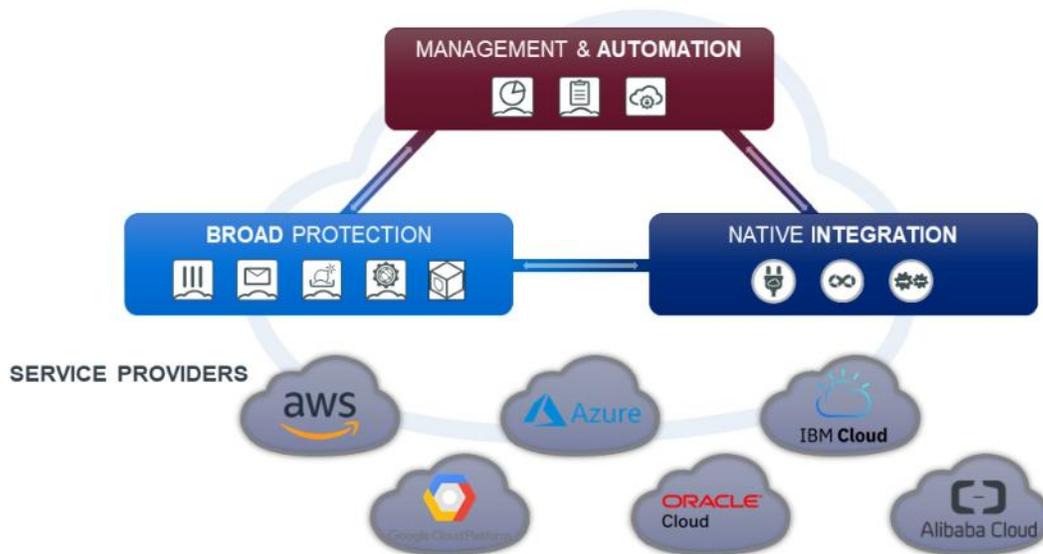
Management & Automation: In order to make the best use of their often limited and overstretched security personnel, Fortinet provides customers with a unique single-pane-of-glass solution that empowers them to consistently manage the broad set of protection services that is natively integrated into the cloud infrastructure. This approach also enables the ability to automate the management of these capabilities through the use of standard web-based APIs, as well as consume predefined automation recipes. By extending this automation framework across multiple cloud environments, customers can integrate the consumption of security services into their emerging DevOps-oriented application lifecycles, while supporting a more agile application and business operation.

Broad Protection: Offering the broadest set of security products both in and out of the cloud allows customers to consistently build the most secure infrastructures possible, regardless of deployment mode, workflow complexity, or degree of distribution and elasticity. The ability to natively integrate in to the cloud infrastructure allows Fortinet to uniquely offer multiple security products in—and between—the cloud environments offered by every major cloud service provider. This helps customers build consumable and automation-ready security services to protect their cloud applications, regardless of where they choose to deploy them.

Native Integration: Integration seamlessly extends consistent security across the platforms of every major cloud provider, enabling organizations to define security similarly across their multi-cloud and on-premises deployments. Likewise, native integration provides the ability to natively consume cloud services by security products, providing faster and more seamless protection and response, and extends the web service-based APIs of products that are running in the cloud.

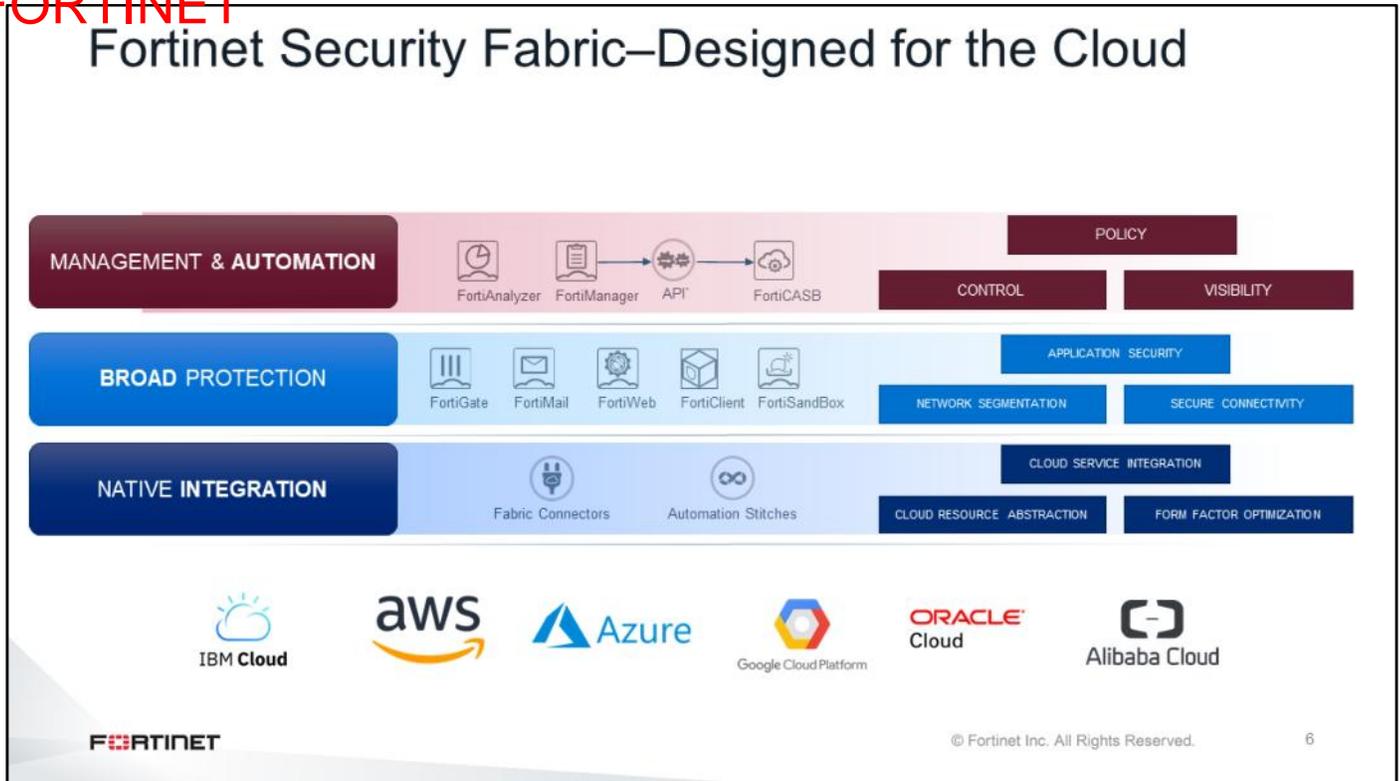
DO NOT REPRINT
© FORTINET

Fortinet Security Fabric



This slide shows the Fortinet Security Fabric overlaid onto the multi-cloud reality that was previously outlined. The key pillars are integration, protection, and management. As part of the Fortinet Security Fabric, FortiManager and FortiAnalyzer provide automation-ready, single-pane-of-glass management, transparent visibility, advanced compliance reporting, and network-aware rapid response across on-premises, cloud, and hybrid environments.

DO NOT REPRINT
© FORTINET



This slide shows the three pillars of the Fortinet Security Fabric for the cloud, and the services and capabilities each pillar enables. Fortinet is investing in each of these pillars to provide native integration and capabilities across clouds.

The Fortinet Security Fabric enables the following services and capabilities:

- Seamless integration of separate cloud infrastructures, and use of native cloud services
- Broad protection for each product, regardless of cloud platform—effectively running virtual versions of the enforcement products on each cloud
- Management products that interact with, and manage the security of, the Fortinet products that run on each cloud

DO NOT REPRINT
© FORTINET

Public Cloud Integration

Service Integration	WAF Partner Rules			
Config Templates	Cloud Formation Templates	HA ARM Template*		
Auto-Scaling	Configuration Synchronization	Config Sync		
High Availability	Session and Config Sync	Config Sync	External LB	External LB
Threat Feeds	Guard Duty			
Automation Scripts	Lambda, Cloud-init	Azure Functions, Cloud-Init	Cloud Init	Cloud Init
Form Factors optimization	SR-IOV on C5			
Connectors	Topology, Meta-Data	Meta-Data	Meta-Data	Meta-Data









FORTINET
*Azure Resource Manager (ARM)
© Fortinet Inc. All Rights Reserved.
7

This slide shows the features provided by leading cloud service providers.

DO NOT REPRINT
© FORTINET

Fabric Connectors



Application
Centric
Infrastructure
(ACI)



Amazon Web
Services
(AWS)



Microsoft
Azure



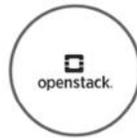
VMware NSX



Nuage
Virtualized
Services
Platform



Oracle Cloud
Infrastructure
(OCI)



OpenStack
(Horizon)



Google Cloud
Platform
(GCP)

FORTINET

© Fortinet Inc. All Rights Reserved.

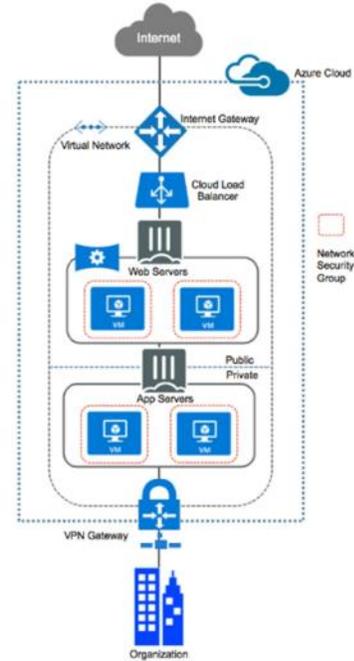
8

On the FortiGate interface, the connectors shown on this slide are called Fabric Connectors. They are software-defined network (SDN) connectors that provide integration and orchestration of Fortinet products with key SDN solutions. In other words, Fabric Connectors help Fortinet products speak to the cloud. The Fortinet Security Fabric provides visibility into your security posture across multiple cloud networks, spanning private, public, and SaaS clouds. By using the Fabric Connector with the Microsoft Azure IaaS, you can automatically update changes to attributes in the Azure environment in the Fortinet Security Fabric.

**DO NOT REPRINT
© FORTINET**

Born in the Cloud

- No physical on-premises IT equipment
- Cost benefits with hourly billing
- Compliance regulations and policy enforcement
- Full enterprise-class security
- Broad portfolio of solutions



FORTINET

© Fortinet Inc. All Rights Reserved.

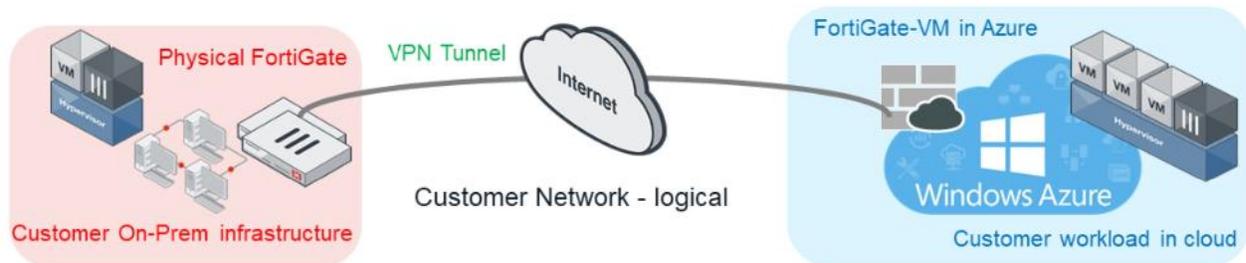
9

An interesting aspect of the Fortinet solution is that the customer can run all devices on the cloud. There is no need for the customer to run physical devices on-premises. Unlike other vendors, Fortinet can offer all security products in cloud-based form, for example, FortiGate, FortiManager, FortiAnalyzer, and so on.

DO NOT REPRINT
© FORTINET

Extending to the Public Cloud

- Customer on-premises infrastructure extends to the cloud through the VPN
 - From on-premises FortiGate to FortiGate-VM in the cloud



FORTINET

© Fortinet Inc. All Rights Reserved.

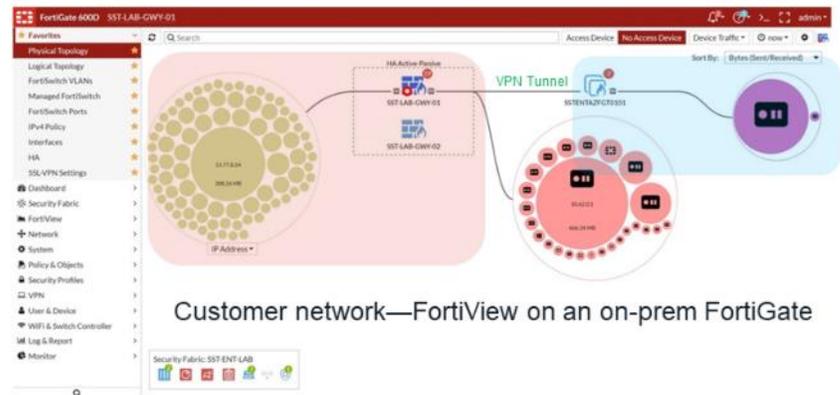
10

The customer can extend the on-premises infrastructure to the cloud through the VPN. As shown on this slide, the customer can run an IPsec tunnel between the cloud and the FortiGate on-premises. On the cloud side, you can deploy a cloud vendor's native IPsec service, which is not recommended, or you can deploy a virtual FortiGate, which is highly recommended.

**DO NOT REPRINT
© FORTINET**

Securing the Public Cloud—Security Fabric Hybrid Cloud

- Fabric view
- Fabric audit
- Consolidated logging
- V-series licensing (no VDOMs)



Customer network—FortiView on an on-prem FortiGate

FORTINET

© Fortinet Inc. All Rights Reserved.

11

The Fortinet Security Fabric supports a hybrid cloud. You can configure an on-premises FortiGate to connect to the FortiGate on the cloud through the VPN tunnel, and share all the information from the Fortigate device on the cloud, within the Fortinet Security Fabric. You can create a multicloud environment in the Security Fabric. For example, an on-premises FortiGate can connect to Azure and AWS through VPN tunnels, and have the entire topology view within the Security Fabric.

DO NOT REPRINT
© FORTINET

Fortinet Cloud Security Solution

- Extends to physical, virtual, and cloud appliances with advanced security orchestration and unified threat protection
- Provides more control and visibility by identifying and setting policy by user applications, device specifications, IP addresses, and network interfaces
- Delivers a highly optimized solution in which application workloads can be protected beyond native cloud vendor security options



© Fortinet Inc. All Rights Reserved.

12

It is important to know that the Fortinet cloud security solution is not a replacement for the existing cloud vendor security. It is just an extra layer of security in addition to the cloud vendor security solutions. The Fortinet cloud security solution provides more control and visibility, and delivers a highly optimized security solution beyond native cloud vendor security options.

**DO NOT REPRINT
© FORTINET**

Licensing Models

- Bring your own license:
 - Just like FortiGate-VM but a different SKU
 - Acquired through partners
- Pay as you go/on demand:
 - Hourly or yearly
 - Based on instance type
 - Paid through the cloud vendor
- For both models, you have to pay infrastructure running costs directly to the cloud vendor

FORTINET

© Fortinet Inc. All Rights Reserved.

13

There are different Fortinet licensing models to pick and choose based on the customer requirements.

- Bring your own license: The customer pays for the cloud vendor for the VMs and pays Fortinet for Fortinet products running 24/7 on the cloud. This model is recommended for VMs running all the time on the cloud. The customer gets Fortinet 24/7 support with the enterprise bundle.
- Pay as you go/on demand: The customer is paying for both through the cloud vendor, but pays for the service based on usage. The customer gets Fortinet 8x5 support with the UTM bundle.

In both cases, the customer must pay infrastructure running costs directly to the cloud vendor.

DO NOT REPRINT
© FORTINET

Marketplace Availability

	FortiGate ^{BYOL}	FortiGate ^{PAYG}	FortiWeb ^{BYOL}	FortiWeb ^{PAYG}	FortiSandbox ^{BYOL}	FortiSandbox ^{PAYG}	FortiMail ^{BYOL}	FortiSIEM ^{BYOL}	FortiManager ^{BYOL}	FortiAnalyzer ^{BYOL}	FortiAnalyzer ^{PAYG}	FortiADC ^{BYOL}	FortiVoice ^{BYOL}	FortiAuthenticator ^{BYOL}	FortiRecorder ^{PAYG}
 AWS	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
 Azure	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
 Google Cloud Platform	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
 ORACLE Cloud	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
 Alibaba Cloud	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

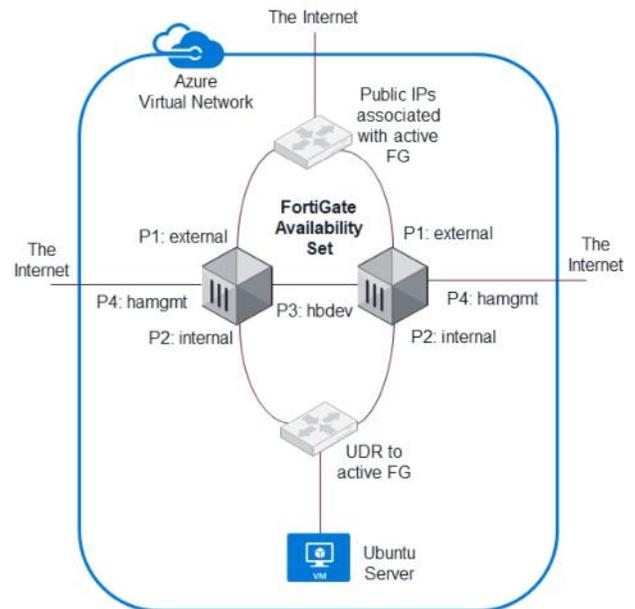
© Fortinet Inc. All Rights Reserved. 14

This slide shows the market availability of Fortinet products. Keep in mind that this information changes based on new support availability for Fortinet products.

**DO NOT REPRINT
© FORTINET**

HA-Active-Passive Unicast FGCP

- Minimum three interfaces, but four are better
- Heartbeat and management interfaces in (hidden) system VDOMs are unusable for productive traffic
- Management interface (port4) for accessing firewalls and reaching out to Azure management for failover commands



© Fortinet Inc. All Rights Reserved.

15

As you learned in another lesson, there is no traditional FortiGate Clustering Protocol (FGCP) to use in high availability (HA) in cloud computing. The solution is to use HA active-passive unicast FGCP, which is a modified version of the traditional FGCP. In this scenario, there is no multicast traffic between heartbeat interfaces; instead, there is only unicast traffic. In order to form two HA FortiGate devices, you must configure the peer IP address on each FortiGate device. Also, there is a management interface (port4), which is unique to each cluster member and has a subnet with Internet access. Each cluster member can be accessed separately through management interfaces. There are two interfaces processing traffic, external and internal. Both heartbeat and management interfaces are system VDOMs that are hidden and unusable for processing production traffic.

DO NOT REPRINT
© FORTINET

HA–Unicast Heart Beat (HB) CLI

- HA sync must use unicast IP to sync; cannot use Layer 2
- Configuration sync works over unicast IP addresses
- Failover mechanism: commands sent directly to AWS/Azure
 - Move public IP addresses
 - Change outbound routing table
- Failover times unpredictable
 - Depends on number of items to rewrite
 - Serial change, not parallel

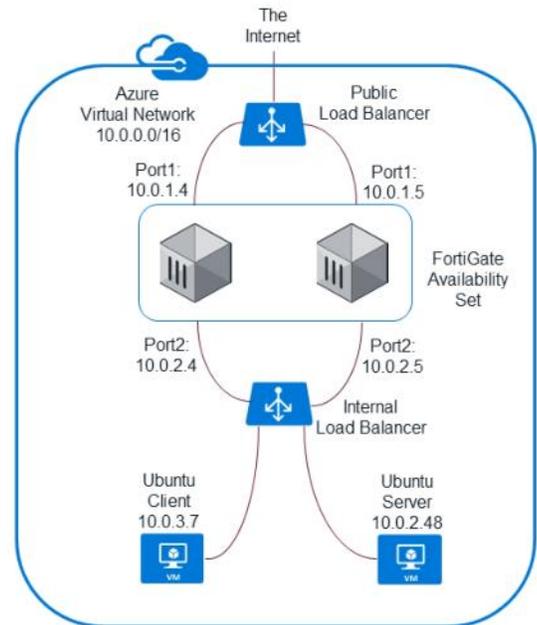
```
config system ha
  set group-name "CloudHA"
  set mode a-p
  set hbdev "port3" 100
  set session-pickup enable
  set session-pickup-connectionless enable
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
      set gateway 10.1.3.1
    next
  end
  set override disable
  set priority 255
  set unicast-hb enable
  set unicast-hb-peerip 10.1.2.5
end
```

HA must use the unicast IP address to sync between cluster members. You must add the two commands that are highlighted on the slide to the traditional HA cluster configurations. These settings are unique to each cluster member because the peer IP address is the other member of the cluster. When failover happens, FortiGate uses AWS and Azure APIs to communicate to the cloud and report the failover. Commands are sent directly to AWS or Azure to change the public IP address and the outbound routing table to the FortiGate IP address and routing table. Also, failover times are unpredictable because of the number of items to rewrite, serial changes, and so on.

DO NOT REPRINT
© FORTINET

HA–Active-Active with Load Balancer

- Each interface pair needs a load balancer
- External load balancer hosts all public IP addresses for protected hosts and FortiGate devices
- Load balancer NATs incoming public connections to the FortiGate devices
- FortiGate VIP translates inbound connections to the protected hosts
- FortiGate can SNAT inbound connections to ensure that reply packets arrive at the same firewall
- Outbound traffic should use the internal load balancer—this is called a load balancer sandwich
- Use FortiManager for configuration sync
- Can use FGSP to sync connections
- Direct server return with user-defined routes (UDRs) enables failover of connections
- Use `session-pickup-expectation` enable to enable asymmetric packet flow
- By default, only established TCP connections are synced



FORTINET

© Fortinet Inc. All Rights Reserved.

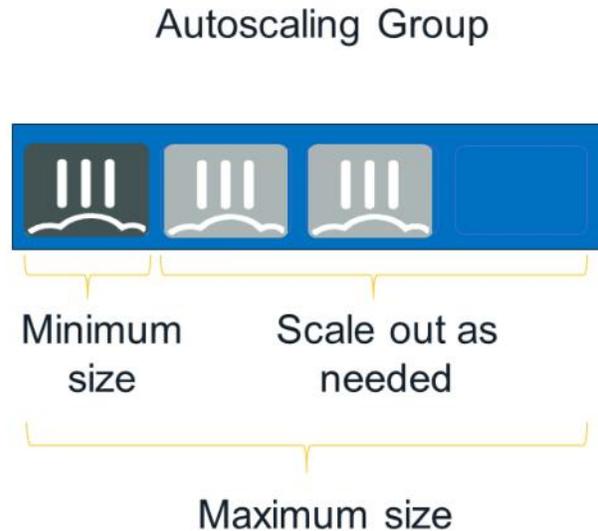
17

This slide shows an example of an active-active load balancing scenario. There are two load balancers, the public load balancer and the internal load balancer. Also, there are two FortiGate devices in the same availability set. You must pair both port1 interfaces of the FortiGate devices with the public load balancer. The Internet traffic goes to the public load balancer first, where it load balances the traffic to two FortiGate devices. Then it goes to the internal load balancer, and finally, to the virtual machines. Every cloud vendor has its own load balancing solutions.

DO NOT REPRINT
© FORTINET

Autoscaling Groups

- Allow you to dynamically grow (scale out) and shrink (scale in) a group of FortiGate devices to match the traffic and performance requirements
- You can define a minimum and maximum number of FortiGate devices allowed in the group
- When you use autoscaling, your applications gain better:
 - Fault tolerance
 - Availability
 - Cost management



FORTINET

© Fortinet Inc. All Rights Reserved.

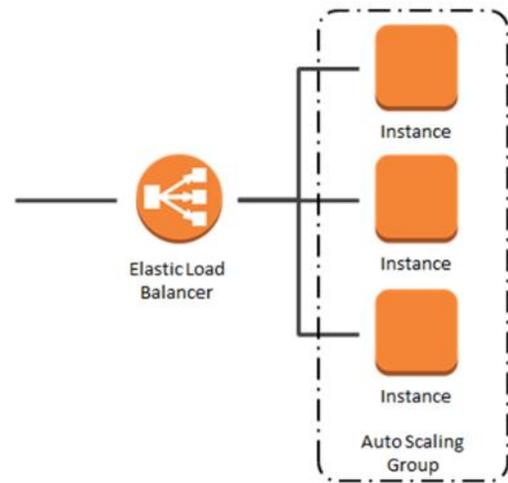
19

Autoscaling allows you to dynamically grow and shrink a group of FortiGate devices to match the traffic and performance requirements. You can set a minimum and maximum number of FortiGate devices and scale out as needed. The main benefits of using autoscaling are fault tolerance, availability, and cost management.

DO NOT REPRINT
© FORTINET

How Autoscaling Works

- Monitors your applications or instances and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost
- Provides easy application scaling for multiple resources across multiple services in minutes
- Makes scaling simple with recommendations that allow you to optimize performance, costs, or balance between them



FORTINET

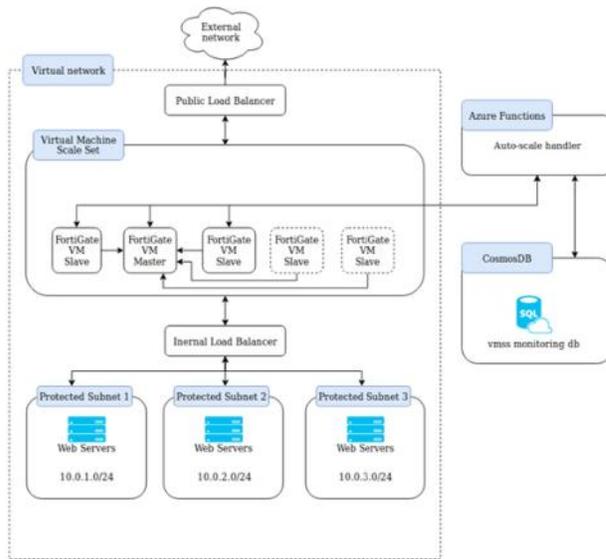
© Fortinet Inc. All Rights Reserved.

20

Load balancing is used in autoscaling. For example, you can start with two FortiGate devices in an autoscaling group as a minimum number, and then increase the number of FortiGate devices based on application needs. If CPU usage becomes high during the minimum number set, you can configure rules to increase the number of FortiGate devices to meet the demand. Autoscaling provides easy application scaling for multiple resources across multiple services, in a short time.

DO NOT REPRINT
© FORTINET

FortiGate Autoscaling–Azure Example



- Azure load balancer sandwich design
- Autoscaling for inbound and outbound traffic
- Avoid asymmetric routing using Azure load balancer session persistence
- Azure function scales FortiGate layer
- Can act as an HA design
 - Base configuratin with FortiManager
- FortiGate configuration sync supported
- Licensing is pay-as-you-go only
- Find the templates on GitHub

FORTINET

© Fortinet Inc. All Rights Reserved.

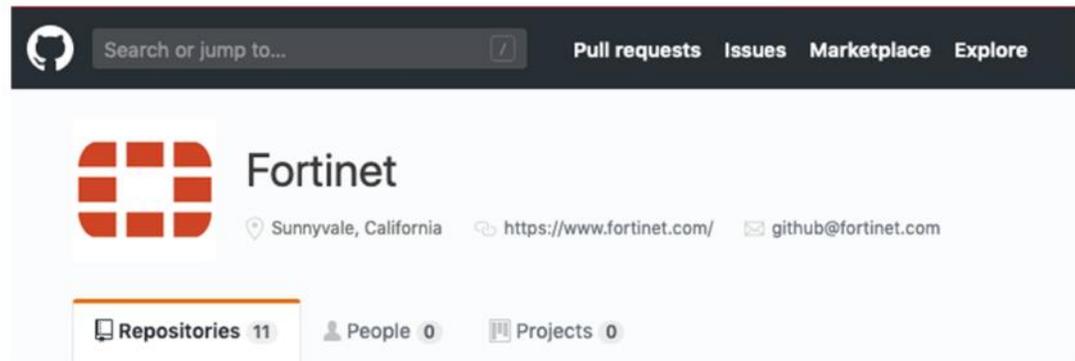
21

Fortigate autoscaling consists of a collection of Node.js modules and cloud-specific templates that support basic autoscale functionality for groups of FortiGate VM instances through Microsoft Azure Functions and Amazon AWS. This slide shows an example of FortiGate autoscaling with Azure. This scenario comprises two load balancers and, in the middle, multiple FortiGate devices in the VM scale set. There is one FortiGate master device and a few FortiGate slave devices. When this template is deployed, it will create a database with ID numbers based on FortiGate roles. So, every time a new FortiGate is deployed, it will check the database to find the IP address of the master FortiGate, and then get the configuration of the master FortiGate. All the configuration changes must be applied to the master device. You can locate autoscaling templates on GitHub.

DO NOT REPRINT
© FORTINET

Fortinet GitHub

- Public cloud templates:
 - <https://github.com/fortinet>



You can visit the official Fortinet GitHub at the website shown on this slide. However, during the lab you will be using a different GitHub, which is the Fortinet Solution GitHub (developer GitHub).

**DO NOT REPRINT
© FORTINET**

Review

- ✓ Secure the public cloud
- ✓ Identify licensing models
- ✓ Understand and deploy HA, load balancer, and autoscaling
- ✓ Use Fortinet Github to deploy templates

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned methods to secure the public cloud using Fortinet solutions.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about the Fortinet solution for Amazon Web Services (AWS).

**DO NOT REPRINT
© FORTINET**

AWS Fundamentals

Objectives

- Understand AWS basic concepts
- Understand AWS components
- Understand AWS networking
- Understand AWS security

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

By demonstrating competence in understanding AWS fundamentals, you will be able to use AWS successfully and efficiently to deploy your security devices.

DO NOT REPRINT
© FORTINET

AWS Services

- Broad portfolio of services

Compute EC2 LightSail ECR ECS EKS Lambda Batch Elastic Beanstalk Serverless Application Repository	Developer Tools CodeStar CodeCommit CodeBuild CodeDeploy CodePipeline Cloud9 X-Ray	Machine Learning Amazon SageMaker Amazon Comprehend AWS DeepLens Amazon Lex Machine Learning Amazon Polly Rekognition Amazon Transcribe Amazon Translate Amazon Personalize Amazon Forecast Amazon TextRank	Mobile AWS Amplify Mobile Hub AWS AppSync Device Farm
Storage S3 SFS FSx S3 Glacier Storage Gateway AWS Backup	Robotics AWS RoboMaker	Analytics Athena EMR CloudSearch Elasticsearch Service Kinesis QuickSight Data Pipeline AWS Glue MSK	AR & VR Amazon Sumerai
Database RDS DynamoDB ElastiCache Neptune Amazon Redshift Amazon DocumentDB	Blockchain Amazon Managed Blockchain	Management & Governance CloudWatch AWS Auto Scaling CloudFormation CloudTrail Config OpsWorks Service Catalog Systems Manager Trusted Advisor Managed Services Control Tower AWS License Manager AWS Well-Architected Tool Personal Health Dashboard	Application Integration Step Functions Amazon MQ Simple Notification Service Simple Queue Service SWF
Migration & Transfer AWS Migration Hub Application Discovery Service Database Migration Service Server Migration Service AWS Transfer for SFTP Snowball DataSync	Satellite Ground Station	Security, Identity, & Compliance IAM Resource Access Manager Cognito Secrets Manager GuardDuty Inspector Amazon Macie AWS Organizations AWS Single Sign-On Certificate Manager Key Management Service CloudHSM Directory Service WAF & Shield Artifact Security Hub	Customer Engagement Amazon Connect ProQuest Simple Email Service
Networking & Content Delivery VPC CloudFront Route 53 API Gateway Direct Connect AWS Cloud Map Global Accelerator	Media Services Elastic Transcoder Kinesis Video Streams MediaConnect MediaConvert MediaLive MediaPackage MediaStore MediaTailor	AWS Cost Management AWS Cost Explorer AWS Budgets AWS Marketplace Subscriptions	Business Applications Alexa for Business Amazon Chime WorkMail
			End User Computing WorkSpaces AppConfig 2.0 WorkDocs WorkLink
			Internet of Things IoT Core Amazon FreeRTOS IoT 3-Click IoT Analytics IoT Device Defender IoT Device Management IoT Events IoT Greengrass IoT SiteWise IoT Things Graph
			Game Development Amazon GameLift

FORTINET

© Fortinet Inc. All Rights Reserved.

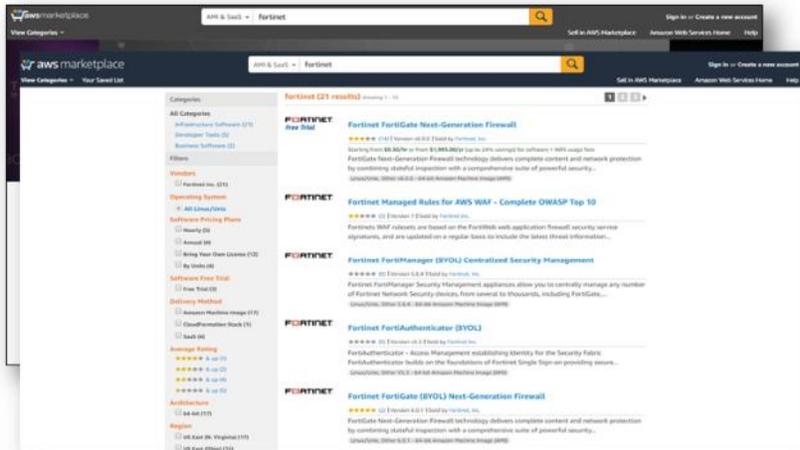
3

As shown on this slide AWS, has a broad portfolio of services. You will see all available services when you click the service manual on the console. However, in this course, you will mainly focus on EC2, VPC, IAM, and DynamoDB.

DO NOT REPRINT
© FORTINET

AWS Marketplace

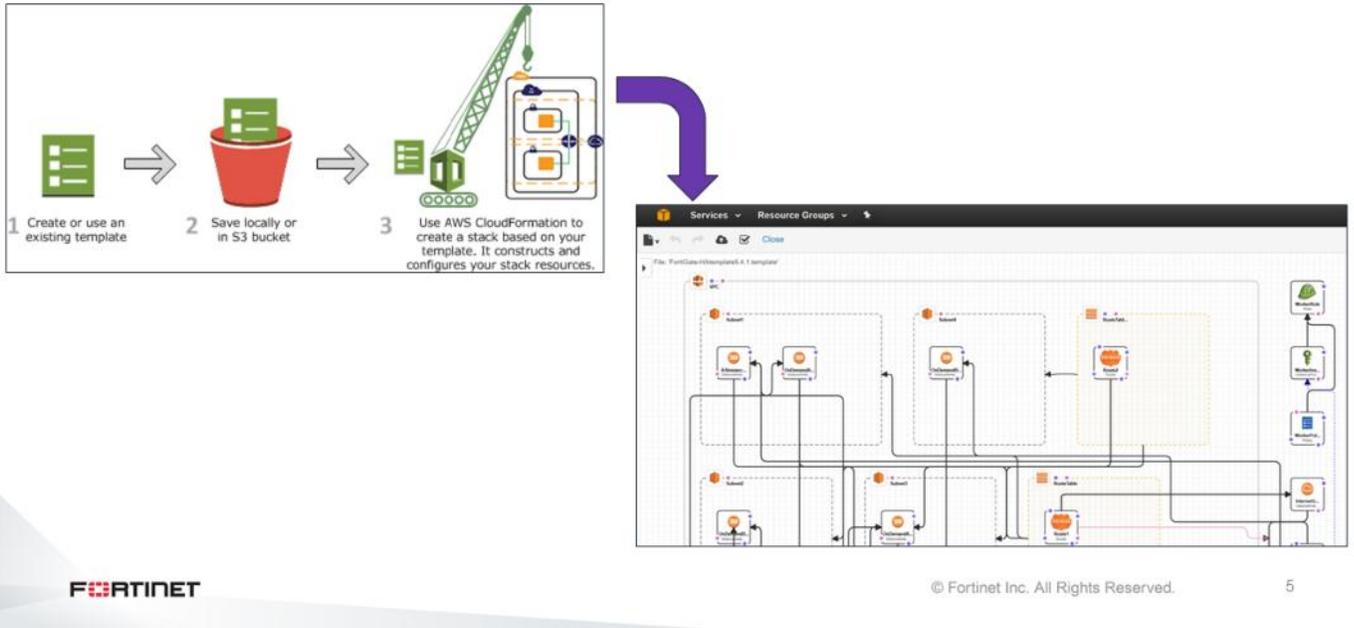
- An online store where customers can find, buy, and immediately start using the software and services they need to build products and run their businesses



AWS Marketplace is an online store where customers can find, buy, and immediately start using the software and services they need to build products and run their businesses. In AWS Marketplace you can find preconfigured images under AMI community images. These are easy to deploy instances uploaded by vendors.

DO NOT REPRINT
© FORTINET

AWS CloudFormation Templates



AWS CloudFormation templates provide an easy way to create and manage a collection of related AWS resources, enabling you to provision and update in an orderly and predictable fashion. You can use AWS CloudFormation sample templates or create your own templates to describe the AWS resources. An AWS CloudFormation template is a set of code, based on JSON, where you can specify the kind of VMs, number of subnets, and IP addresses to deploy then pass into the FortiGate devices. After AWS resources are deployed, you can modify and update them in a controlled and structured way. You can apply version control to your AWS infrastructure the same way you do with your software. Keep in mind that you cannot find AWS CloudFormation templates in AWS Marketplace. First, you must upload them to GitHub, and then upload them to AWS Marketplace.

DO NOT REPRINT
© FORTINET

AWS Regions

- AWS Cloud spans 69 availability zones (AZs) within 22 geographic regions and 1 local region around the world



North America

US East (Northern Virginia) Region
EC2 Availability Zones: 6
Launched 2006

US East (Ohio) Region
EC2 Availability Zones: 3
Launched 2016

US West (Oregon) Region
EC2 Availability Zones: 3
Launched 2011

US West (Northern California) Region
EC2 Availability Zones: 3*
Launched 2009

AWS GovCloud (US-West) Region
EC2 Availability Zones: 3
Launched 2011

Canada (Central)
EC2 Availability Zones: 2
Launched 2016
[Learn more at AWS Canada](#)

AWS Edge Network Locations:

Edge locations - Ashburn, VA (3); Atlanta GA (3); Boston, MA; Chicago, IL (2); Dallas/Fort Worth, TX (4); Denver, CO; Hayward, CA; Jacksonville, FL; Los Angeles, CA (3); Miami, FL (2); Minneapolis, MN; Montreal, QC; New York, NY (3); Newark, NJ (2); Palo Alto, CA; Phoenix, AZ; Philadelphia, PA; San Jose, CA; Seattle, WA (3); South Bend, IN; St. Louis, MO; Toronto, ON

Regional Edge Caches - Northern Virginia, Ohio, Oregon

*New customers can access two EC2 Availability Zones in US West (Northern California).

FORTINET

© Fortinet Inc. All Rights Reserved.

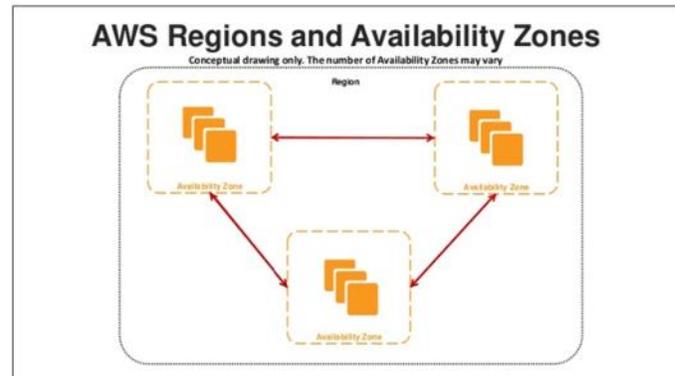
6

Amazon EC2 is hosted in multiple locations worldwide. These locations are composed of regions and AZs. Each region is a separate geographic area with multiple, isolated locations known as AZs. When you view your resources, you'll see only the resources tied to the region you've specified. Regions are isolated from each other, and AWS does not replicate resources across regions automatically. There is a charge for data transfer between regions, but not all regions have the same features, functions, and offers.

DO NOT REPRINT
© FORTINET

AZs

- AZs are isolated from each other
- AZs in a region are connected through low-latency links
- Amazon EC2 resources are either global, tied to a region, or tied to an AZ
- Number of AZs varies per region
- Minimum two AZs per region



FORTINET

© Fortinet Inc. All Rights Reserved.

7

By launching your instances in separate AZs, you can protect your applications from a failure in a single location. Think of it as a physical hypervisor located in a different data center. If data center A fails, your workloads are redundantly deployed in data center B. An AWS best practice is to place instances in more than one AZ. Each AZ is isolated, but the AZs in a region are connected through low-latency links. The new unicast HA solution deploys into a single AZ; therefore, the best practice is to break them up and deploy them into two AZs. You cannot have one FortiGate sitting between AZs; instead, you can have a load balancer between AZs. An AZ is represented by a region code, followed by a letter identifier, for example, us-east-1a.

DO NOT REPRINT
© FORTINET

Elastic Compute Cloud (EC2)

- Basically, your VMs running in AWS
- EC2 is a web service that provides resizable compute capacity in the AWS Cloud
- FortiGate and FortiWeb VMs and on-demand instances are sized to align with EC2 instances

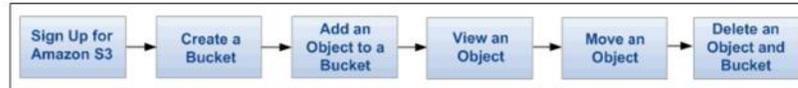


The compute elements in AWS are called elastic compute cloud (EC2). The Amazon EC2 simple web service interface let's you obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. So, EC2 is a VM instance running inside AWS, for example, FortiGate or FortiWeb VM running as EC2 instances.

**DO NOT REPRINT
© FORTINET**

Amazon Simple Storage Service (S3)

- Storage for the Internet
- Used to store and retrieve any amount of data, at any time, from anywhere on the web



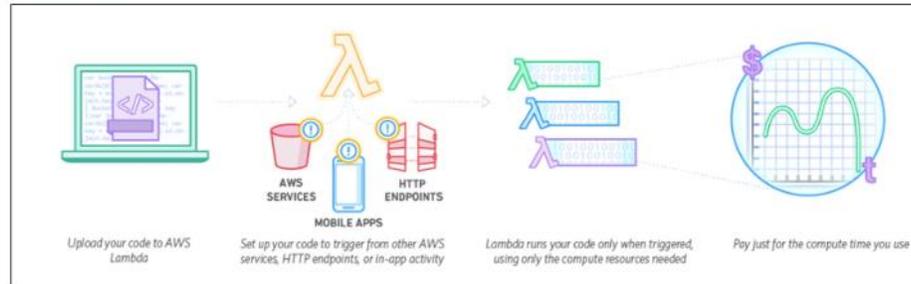
- By default, S3 is publicly accessible

Amazon S3 is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the AWS Management Console, which is a simple and intuitive web interface. This is a file sharing service that you can use to create buckets and then access them over FTP, HTTP, and NFS, to name a few. This is a sort of NAS service. For example, a user can upload FortiGate licenses into the S3 bucket and use a script to grab the licenses and renew your device licenses, as needed. Another example is if you deploy a FortiMail cluster and you would like to have your mailboxes outside FortiMail, you can use an S3 bucket storage for mailbox data.

DO NOT REPRINT
© FORTINET

AWS Lambda

- Lambda lets you run code without provisioning or managing servers
- You pay only for the compute time you consume—there is no charge when your code is not running
- You can run code for virtually any type of application or backend service—all with zero administration
- Upload your code and Lambda takes care of everything required to run and scale your code with HA



FORTINET

© Fortinet Inc. All Rights Reserved.

10

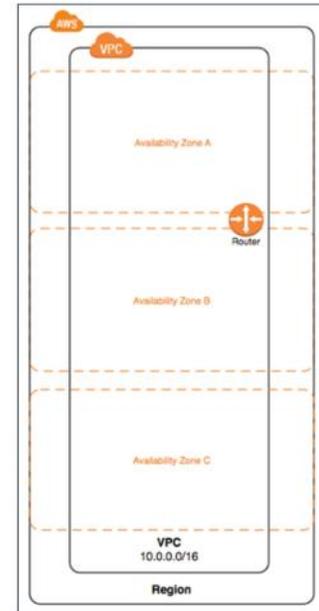
AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume, and there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service—all with zero administration. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

You can use this feature in HA deployments, where the HA functions use AWS Lambda functions to call the failover. You can also use Lambda functions in FortiGate automation stiches. For example, you can create Lambda functions, and then use FortiGate to trigger those functions, based on the situation.

DO NOT REPRINT
© FORTINET

Virtual Private Cloud (VPC)

- Your own network instance
 - The base CIDR is defined here
- You can have more than one VPC
- Defined within a region
- Spread among the AZs of the region where it is defined
- Contains the subnets, EC2 instances, ELBs, and so on



© Fortinet Inc. All Rights Reserved.

11

Virtual Private Cloud (VPC) enables you to define a virtual network in your own logically isolated area within AWS Cloud, known as a VPC. This is the same concept as a VNET in Microsoft Azure. The VPC belongs to a region, and within the VPC, you can create different subnets. All subnets should be in the same CIDR block that is defined for the VPC, for example, $10.0.0.0/16$ block.

As shown on this slide, the VPC belongs to a region but not to any AZs. Within the VPC, you can deploy subnets that belong to different AZs. Keep in mind that the interim router belongs to the VPC only and not to a specific subnet.

DO NOT REPRINT
© FORTINET

Elastic Network Interfaces (ENIs)

- An ENI is a virtual network interface
- ENI attributes (IP/MAC/security group) follow the ENI when it is attached to or detached from an instance
- When you move an ENI, network traffic is redirected to the new instance
- Each instance in your VPC has a default network interface (the primary network interface) that is assigned a private IPv4 address from the IPv4 address range of your VPC
 - You cannot detach a primary network interface from an instance
- An ENI cannot move between AZs

An ENI is a virtual network interface. In an ENI, you can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. The attributes of a network interface follow it as it's attached to or detached from one instance, and reattached to another instance. When you move a network interface from one instance to another, network traffic is redirected to the new instance. You can also modify the attributes of your network interface, including changing its security groups and managing its IP addresses. Keep in mind that once an ENI is created inside the AZ, it cannot be moved outside the AZ.

DO NOT REPRINT
© FORTINET

Source/Destination Check

- Set by network interface
- Allows source and destination IP addresses different from the assigned IP address of the interface
- Required on private FortiGate interface when routing traffic to other networks like the Internet

Change Source/Dest. Check ×

Network Interface eni-0e8938776ba5c1c3a

Source/dest. check Enabled
 Disabled

Cancel Save

FORTINET

© Fortinet Inc. All Rights Reserved.

13

The source/destination check feature is set by network interface. If source/destination checks are disabled (not default behavior) in AWS, source and destination IP addresses that are different from the assigned IP address of the interface are allowed. In AWS, the source/destination check feature is enabled by default. In Azure, it is disabled by default.

DO NOT REPRINT
© FORTINET

Subnets

- **Public:** Internet gateway connected subnet
 - Doesn't mean public addressing within the subnet
- **Private:** Internal subnet without an Internet gateway
 - They must follow the addressing space defined on the VPC that they belong to
- All subnets are connected to an intrinsic router that resides at the VPC level (in all AZs)
- **Reserved IP addresses:**
 - First IP address (X.X.X.1): Intrinsic router
 - Second IP address (X.X.X.2): AWS DNS
 - Third IP address (X.X.X.3): Reserved for future use

There are two different kinds subnets: public and private. A public subnet means that the subnet has an Internet gateway attached, and therefore has Internet access. It may or may not have public IP addressing in it. A private subnet is an internal subnet that doesn't have an Internet gateway attached to it. Private subnets must follow the addressing space defined on the VPC that they belong to. As we learned earlier, all the subnets are connected to an intrinsic router that resides at the VPC level. For example, if you want to deploy a FortiGate device for outgoing traffic protection, you can have one interface connect to the private subnet and the other interface connect to the public subnet. Once you have both interfaces connected, then you will define a routing table on the private subnet to route Internet traffic through the FortiGate device and then to public subnet.

The first three usable IP addresses are reserved in AWS. The first IP address is reserved for the intrinsic router, the second IP address is reserved for AWS DNS, and the third IP address is reserved for future use. If you deploy a FortiGate device, you will need to use the fourth usable IP address.

DO NOT REPRINT
© FORTINET

Internet Gateway

- An Internet gateway is a redundant, highly available VPC component that allows communication between instances in your VPC and the Internet
- An Internet gateway serves two purposes:
 - Provides a target in your VPC route tables for Internet-routable traffic
 - Performs NAT for instances that have been assigned public IPv4 addresses
- To enable communication over the Internet, your instance must have a public IPv4 address or an elastic IP (EIP) that's associated with a private IPv4 address on your instance

	Default VPC	Nondefault VPC
Internet gateway	Yes	Yes, if you created the VPC using the first or second option in the VPC wizard. Otherwise, you must manually create and attach the internet gateway.
Route table with route to internet gateway for IPv4 traffic (0.0.0.0/0)	Yes	Yes, if you created the VPC using the first or second option in the VPC wizard. Otherwise, you must manually create the route table and add the route.
Route table with route to internet gateway for IPv6 traffic (::/0)	No	Yes, if you created the VPC using the first or second option in the VPC wizard, and if you specified the option to associate an IPv6 CIDR block with the VPC. Otherwise, you must manually create the route table and add the route.
Public IPv4 address automatically assigned to instance launched into subnet	Yes (default subnet)	No (nondefault subnet)
IPv6 address automatically assigned to instance launched into subnet	No (default subnet)	No (nondefault subnet)

FORTINET

© Fortinet Inc. All Rights Reserved.

15

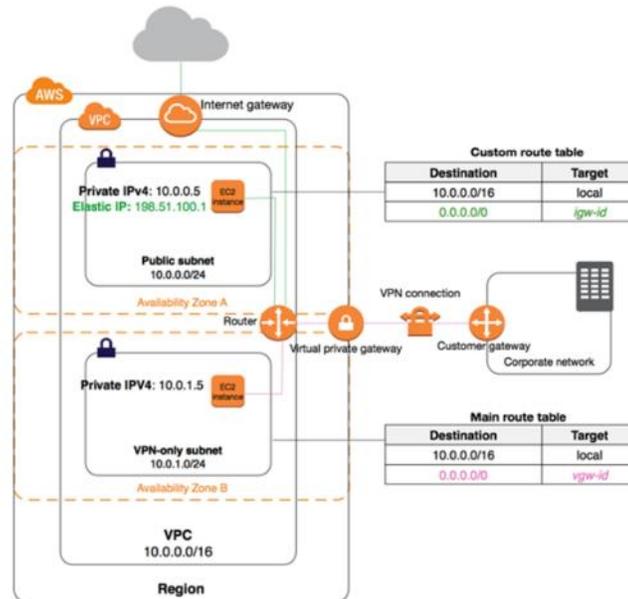
An Internet gateway is a redundant, highly available VPC component that allows communication between instances in your VPC and the Internet. Internet gateway is a feature that you enable in the subnet, allowing intrinsic router to connect to the Internet. If you want to make the subnet public, first you must create an Internet gateway, and then attach it to the appropriate subnet.

An Internet gateway serves two purposes:

- It provides a target in your VPC route tables for Internet-routable traffic.
- It performs NAT for instances that have been assigned public IPv4 addresses.

DO NOT REPRINT
© FORTINET

Implicit Router and Internet Gateway



FORTINET

© Fortinet Inc. All Rights Reserved.

16

The diagram on this slide shows the routing for a VPC with both an Internet gateway and a virtual private gateway, plus a public subnet and a VPN-only subnet. The main route table came with the VPC, and it also has a route for the VPN-only subnet. A custom route table is associated with the public subnet. The custom route table has a route over the Internet gateway (the destination is 0.0.0.0/0, and the target is the Internet gateway). There is a global AWS within the AWS, and there is a region, and the VPC is created in the region. Also, there are AZs inside the VPC. There are two different subnets, 10.0.0.0/24 and 10.0.1.0/24, which belong to two AZs. A router between two AZs is responsible for routing traffic between the AZs. When you create a VPC, it creates a default main routing table that can be used when there is no specific routing table created for a subnet. You can create additional routing tables, and then attach them to a subnet.

DO NOT REPRINT
© FORTINET

Routing Tables

- By default, subnets are associated with a main routing table
- You can create more routing tables and explicitly associate them with subnets
- A gateway is not defined by an IP address
 - Instead, it uses the ENI object
- EC2 instances always use the intrinsic router as the default gateway, but they are then redirected to each gateway defined in the routing table

You can use static or traditional routing within an instance, but automation could be affected

As mentioned in this lesson, when you create a VPC, it creates a default main routing table by default, and subnets are associated with the main routing table. The gateway uses an ENI object and is not defined by an IP address. EC2 instances always use the intrinsic router as the default gateway, but they are then redirected to each gateway defined in the routing table. Note that you can create and use traditional or static routes within an instance, but this will be problematic for future automation.

**DO NOT REPRINT
© FORTINET**

EIP Addresses

- An elastic IP (EIP) address is a static, public IPv4 address
- You can associate an EIP address with any instance or network interface for any VPC in your account
- You can use an EIP address to mask the failure of an instance by rapidly remapping the address to another instance in your VPC
- Associating the EIP address with the network interface instead of directly with the instance, means that you can move all the attributes of the network interface from one instance to another, in a single step

An EIP address is a static, public IPv4 address. You can associate an EIP address with any instance or network interface for any VPC in your account. You can use an EIP address to mask the failure of an instance by rapidly remapping the address to another instance in your VPC. Associating the EIP address with the network interface instead of directly with the instance, means that you can move all the attributes of the network interface from one instance to another, in a single step.

During the lab, you will see both EIP and non-EIP addresses. Keep in mind that in an active-passive HA setup, you must use an elastic IP address to move one instance to another during the failover.

**DO NOT REPRINT
© FORTINET**

Other Services

- DHCP:
 - EC2 interfaces should use DHCP
 - All addressing is defined at the AWS console level
 - You can use static IP addresses, but they must match the AWS configuration
- DNS:
 - Each EC2 instance has an internal DNS name that should be used to address traffic to it
 - This DNS server is present on all subnets as the second valid IP address, and is the default DHCP option

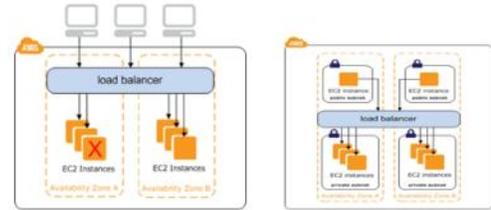
Other services inside the VPC are the DHCP and DNS services. EC2 interfaces should use DHCP and, by default, when you assign an IP address to a network interface, the DHCP service will be automatically activated and deliver the IP address to the DHCP-enabled interface of the device. You can enable the DHCP feature from the FortiGate interface to receive the IP address. You can also create specific options inside the DHCP server.

Each EC2 instance has an internal DNS name that you should use to address traffic to it. This DNS server is present on all subnets as the second valid IP address, and is the default DHCP option. At the same time, every time you deploy a network interface, it gets assigned a random DNS name without any VPC reference. The random DNS name can be resolved both inside and outside the VPC.

DO NOT REPRINT
© FORTINET

Basic AWS Infrastructure Components

- Elastic load balancer (ELB)
 - Network load balancer
 - Takes decision on transport layer (Layer 3 and 4)
 - Application load balance (HTTP/HTTPS)
 - Takes decision on Layer 7
 - Can do content-based routing and load balancing
 - Classic load balance
 - Works on Layer 4 and 7 (TCP/SSL,HTTP/HTTPS, no UDP)
 - Supports classic EC2
 - Target group members must be listening on the same port



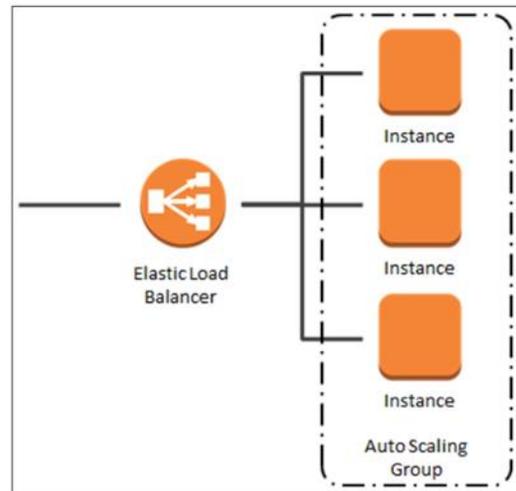
Feature	Application Load Balancer	Network Load Balancer	Classic Load Balancer
Protocols	HTTP, HTTPS	TCP	TCP, SSL, HTTP, HTTPS
Platforms	VPC	VPC	EC2-Classical, VPC

Now, you will learn about basic AWS infrastructure components. There are three main load balancers in AWS: network load balancer, application load balancer, and classic load balancer.

DO NOT REPRINT © FORTINET

ELB

- ELB automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses
- It is at the VPC level and can handle the varying load of your application traffic in a single AZ or across multiple AZs
- Always uses SNAT

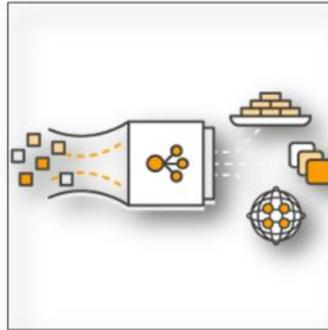


Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. ELB can handle the varying load of your application traffic in a single AZ or across multiple AZs. ELBs sit at the VPC level, so they have access to different subnets in different AZs. In order to have traffic and services load balancing between different AZs in a high availability setup, you must use ELB.

DO NOT REPRINT
© FORTINET

Application Load Balancer

- Best suited for load balancing of HTTP and HTTPS traffic
- Provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers
- Operating at Layer 7, application load balancer routes traffic to targets within Amazon VPC, based on the content of the request



FORTINET

© Fortinet Inc. All Rights Reserved.

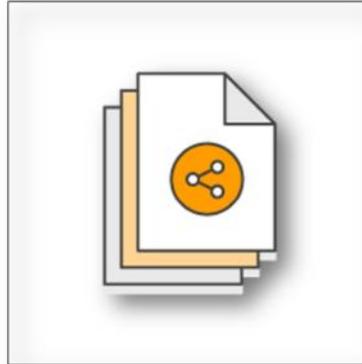
22

Application load balancer is best suited for load balancing HTTP and HTTPS traffic, and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. Operating at the individual request level (Layer 7), application load balancer routes traffic to targets within Amazon virtual private cloud (VPC), based on the content of the request.

DO NOT REPRINT
© FORTINET

Classic Load Balancer

- Provides basic load balancing across multiple Amazon EC2 instances
- Operates at both the request level and connection level
- Classic load balancer is intended for applications that were built within the EC2-classic network



FORTINET

© Fortinet Inc. All Rights Reserved.

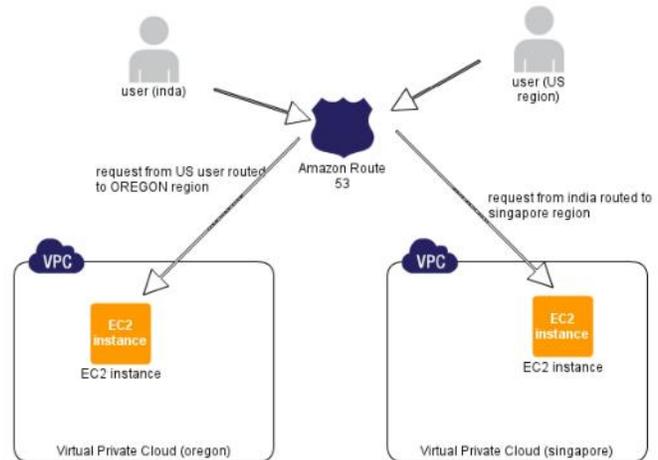
23

Classic load balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic load balancer is intended for applications that were built within the EC2 classic network.

DO NOT REPRINT
© FORTINET

Amazon Route 53

- The AWS DNS service
 - Both public and private
- You can transfer or buy domains in Amazon Route 53
- Has health checks and distribution rules
- Implicit distributed denial of service (DDoS) protection



FORTINET

© Fortinet Inc. All Rights Reserved.

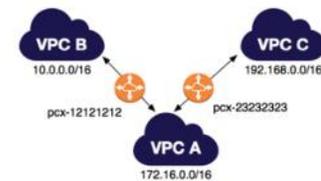
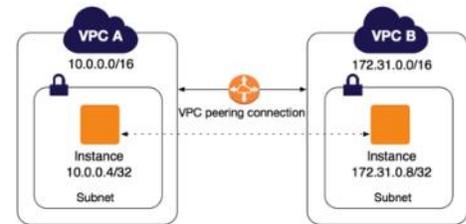
24

Amazon Route 53 is a global load balancing service. The load balancer sits inside the VPC, which is inside the region. So, if you would like to have a multi-region load balancer, this is the Amazon Route 53 coming in to the picture. You can also use Amazon Route 53 as a regular DNS service. By default, the Amazon Route 53 service comes with DoS protection.

DO NOT REPRINT
© FORTINET

VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private addresses
- Instances in either VPC can communicate with each other as if they are in the same network
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account
 - The VPCs can be in different regions (also known as an *inter-region* VPC peering connection)
- There is no single point of failure for communication or a bandwidth bottleneck
- A VPC peering connection is a one-to-one relationship between two VPCs
 - You can create multiple VPC peering connections for each VPC, but transitive peering relationships are not supported
 - You do not have any peering relationships with VPCs that your VPC is not directly peered with



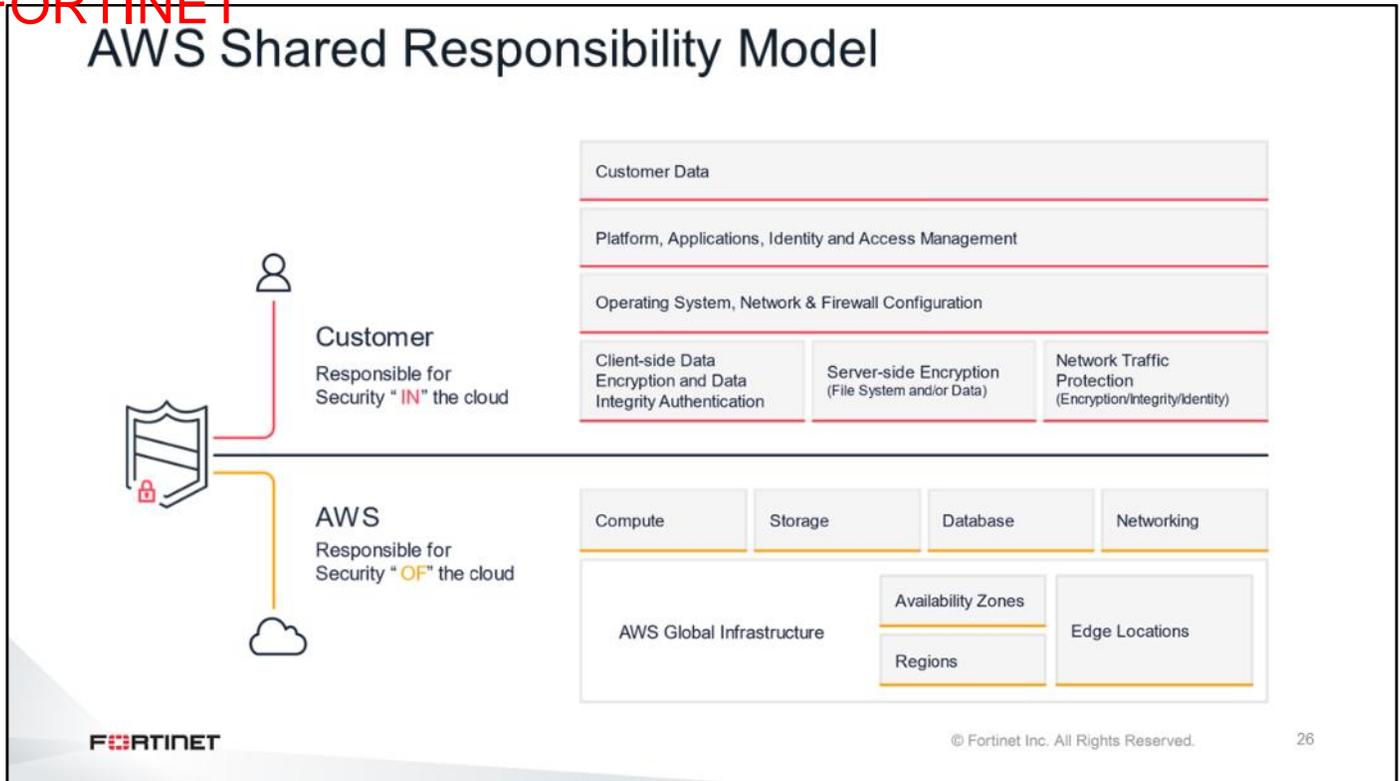
FORTINET

© Fortinet Inc. All Rights Reserved.

25

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private addresses. Instances in either VPC can communicate with each other as if they are in the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. You can connect VPCs between different regions, inside regions. It is similar to connecting both VPCs using a single cable and having a route existing in the routing table. For example, you can have a route to force traffic to go to from one specific VPC to another VPC. A VPC peering connection is a one-to-one relationship between two VPCs. Note that the cost associated with VPC peering varies depending on how they connect between the same region or a different region.

DO NOT REPRINT
© FORTINET



This slide shows the official screenshot of the AWS shared responsibility model. This means that a customer is responsible for security in the cloud, and AWS responsible for the security of the cloud. It is very clear that not only cloud vendors, but also customers, play an important role of securing data in the cloud.

DO NOT REPRINT**© FORTINET**

Security Groups (SGs)

- An SG acts as a virtual firewall that controls the traffic for one or more instances
- SGs are associated with network interfaces. Changing the SGs of an instance changes the SG associated with the primary network interface (eth0)
- By default, SGs allow all outbound traffic
 - SG rules are always permissive; you can't create rules that deny access
 - SGs are stateful
- Instances are automatically associated with the default SG (unless you specify an SG)
 - Allows all inbound traffic from other instances associated with the default security group
 - Allows all outbound traffic from the instance
- When you associate multiple SGs with an instance, the rules from each SG are effectively aggregated to create one set of rules
- You can create your own security groups and specify them when you launch your instances
- **Tip:** If things aren't working, check the SGs first

An SG acts as a virtual firewall that controls the traffic for one or more instances. SGs are associated with network interfaces. Changing the SGs of an instance changes the SG associated with the primary network interface (eth0). By default, SGs allow all outbound traffic. Instances are automatically associated with the default SG (unless you specify an SG). When you associate multiple SGs with an instance, the rules from each SG are effectively aggregated to create one set of rules. You can create your own SGs and specify them when you launch your instances. The only difference between the SGs in AWS and Azure, is that in AWS, SGs are attached to the network interfaces.

DO NOT REPRINT
© FORTINET

Network Access Control Lists (NACLs)

- An NACL is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets
- Your VPC automatically comes with a modifiable default NACL
 - By default, it allows all inbound and outbound IPv4 traffic
- You can create a custom NACL and associate it with a subnet
 - By default, each custom NACL denies all inbound and outbound traffic until you add rules
- Each subnet in your VPC must be associated with an NACL
 - If you don't explicitly associate a subnet, it is associated with the default NACL
- An NACL has separate inbound and outbound rules, and each rule can either allow or deny traffic
- NACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and the reverse)

An NACL is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. Your VPC automatically comes with a modifiable default NACL. By default, it allows all inbound and outbound IPv4 traffic. You can create a custom NACL and associate it with a subnet. By default, each custom NACL denies all inbound and outbound traffic until you add rules. Each subnet in your VPC must be associated with an NACL. If you don't explicitly associate a subnet with a NACL, it is associated with the default NACL. An NACL has separate inbound and outbound rules, and each rule can either allow or deny traffic. NACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and the reverse).

**DO NOT REPRINT
© FORTINET**

Flow Logs and CloudWatch

- VPC flow logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC
 - There is no additional charge for using flow logs; however, standard CloudWatch Logs charges apply
 - Flow log data is published to a log group in CloudWatch Logs, and each network interface has a unique log stream
- Flow logs do not capture:
 - Traffic to and from 169.254.169.254 for instance metadata
 - Traffic to and from 169.254.169.123 for the Amazon Time Sync Service
 - DHCP traffic
 - Traffic to the reserved IP address for the default VPC router
 - Flow logs do not capture real-time log streams for your network interfaces
- You can use flow logs as a security tool to monitor the traffic that is reaching your instance

VPC flow logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. There is no additional charge for using flow logs; however, standard CloudWatch Logs charges apply. Flow log data is published to a log group in CloudWatch Logs, and each network interface has a unique log stream. Flow logs do not capture traffic to and from 169.254.169.254, such as metadata traffic to and from 169.254.169.123 for the Amazon Time Sync Service, DHCP traffic, and traffic to the reserved IP address for the default VPC router. Also, flow logs do not capture real-time log streams for your network interfaces. You can use flow logs as a security tool to monitor the traffic that is reaching your instance. Flow logs are useful if you want to perform quick troubleshooting and to see the behavior of the security groups.

**DO NOT REPRINT
© FORTINET**

Amazon GuardDuty

- Managed threat detection service
- Monitors for malicious or unauthorized behavior
- Helps to protect AWS accounts and workloads
- Monitors for activity, such as:
 - Unusual API calls
 - Potentially unauthorized deployments that indicate a possible account compromise
- GuardDuty also detects potentially compromised instances or reconnaissance by attackers

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. You can use the FortiGate threat feed feature to obtain all blacklisted IP addresses from GuardDuty and then create appropriate firewall policies to block traffic.

DO NOT REPRINT
© FORTINET

Other AWS Security Products

- **AWS web application firewall (WAF)**
 - AWS WAF monitors the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an application load balancer

- **AWS Inspector**
 - Amazon Inspector enables you to analyze the behavior of your AWS resources
 - Helps to identify potential security issues

- **AWS Shield**
 - You can use AWS WAF web access control lists (web ACLs) to minimize the effects of a DDoS attack



AWS WAF



AWS Inspector



AWS Shield

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow to or block from your web applications by defining customizable web security rules. AWS WAF monitors the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an application load balancer.

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

AWS Shield is a managed distributed denial of service (DDoS) protection service that safeguards applications running on AWS. You can use AWS WAF web access control lists (web ACLs) to minimize the effects of a DDoS attack.

**DO NOT REPRINT
© FORTINET**

Fortinet Solutions for AWS

Objectives

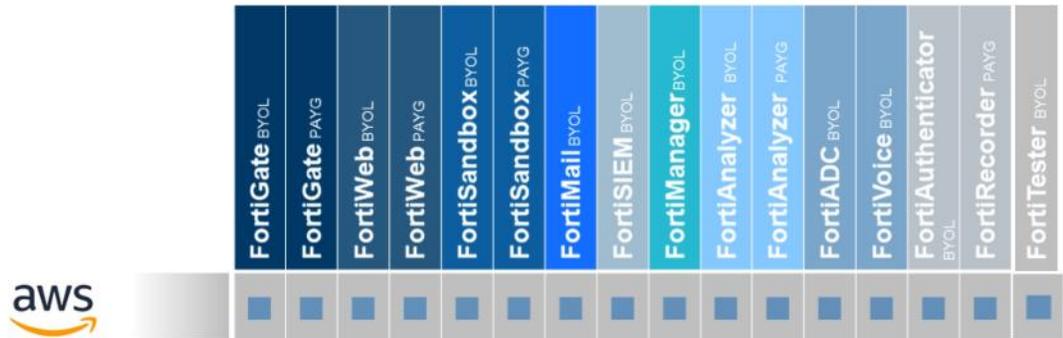
- Understand Fortinet Security Fabric for AWS
- Understand Fortinet products on AWS Marketplace
- Understand FortiGate AWS SDN integration
- Understand Fortinet WAF solutions for AWS
- Understand FortiGate native active-passive HA
- Understand FortiGate active-active HA with AWS ELB
- Understand FortiGate autoscaling

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

By demonstrating competence in understanding AWS and Fortinet solutions for AWS, you will be able to successfully use AWS with Fortinet solutions.

DO NOT REPRINT
© FORTINET

Fortinet Products in AWS Marketplace



FORTINET

© Fortinet Inc. All Rights Reserved.

33

This slide shows the Fortinet solutions for AWS. AWS is the most broadly supported cloud vendor for Fortinet products.

DO NOT REPRINT
© FORTINET

FortiSandbox for AWS

- Control
 - Windows EC2s
- Extended scalability
- Addresses limitation in AWS
- VM started and stopped outside of FortiSandbox

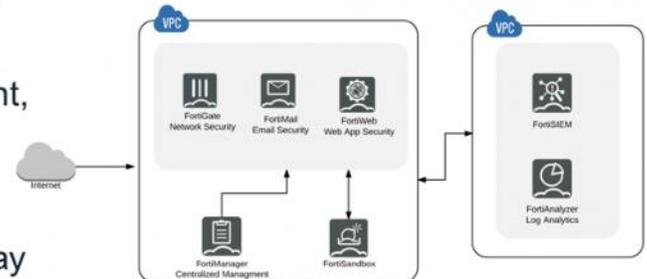


Now, you will learn about one of the AWS-supported Fortinet products, FortiSandbox. FortiSandbox is not a hypervisor in AWS—it is simply a manager and analyzes the results of the sandboxing process. FortiSandbox deploys new EC2 instances with the custom Windows VMs, and then it sends malware, runs it, and captures the results for analysis. FortiSandbox for AWS does not need more resources because it performs management and analysis tasks only. Note that the cost varies based on the number of EC2 instances deployed, size of the instances, and duration of the running time.

DO NOT REPRINT
© FORTINET

FortiSandbox for AWS (Contd)

- FortiSandbox for AWS enables organizations to defend against advanced threats natively in the cloud
- Automated zero-day, advanced malware detection and mitigation
- Works alongside network, email, endpoint, and other security, or as an extension to on-premises security architectures to leverage scale with complete control
- Can be installed as a standalone zero-day malware behavior analysis system
- Integrates with existing FortiGate, FortiMail, or FortiWeb AWS instances



FORTINET

© Fortinet Inc. All Rights Reserved.

35

FortiSandbox for AWS enables organizations to defend against advanced threats natively in the cloud.

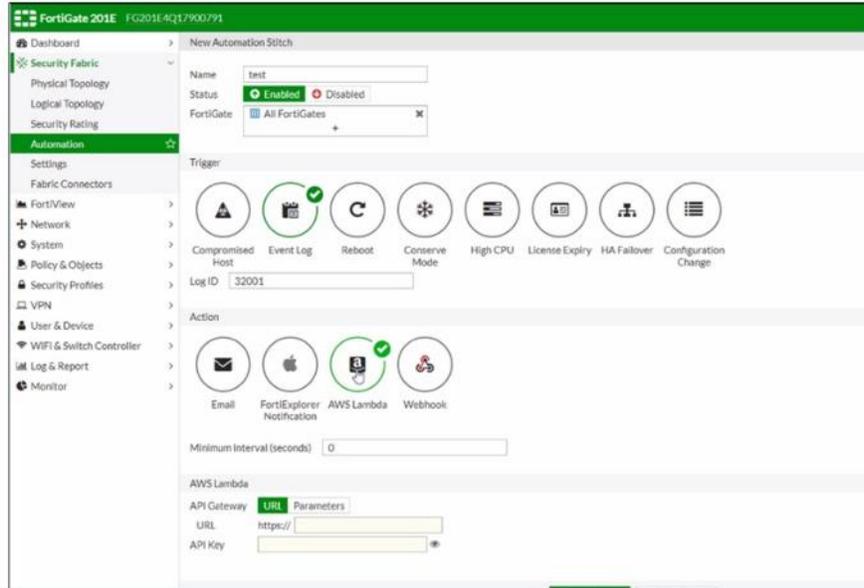
FortiSandbox provides several important benefits, including:

- Automated zero-day, advanced malware detection and mitigation
- An addition to network, email, endpoint, and other security, or an extension to on-premises security architectures that leverages scale with complete control

FortiSandbox can be installed as a standalone zero-day malware behavior analysis system. Also, FortiSandbox can be integrated with existing FortiGate, FortiMail, and FortiWeb AWS instances.

DO NOT REPRINT
© FORTINET

Automation Using AWS Lambda and FortiGate



FORTINET

© Fortinet Inc. All Rights Reserved.

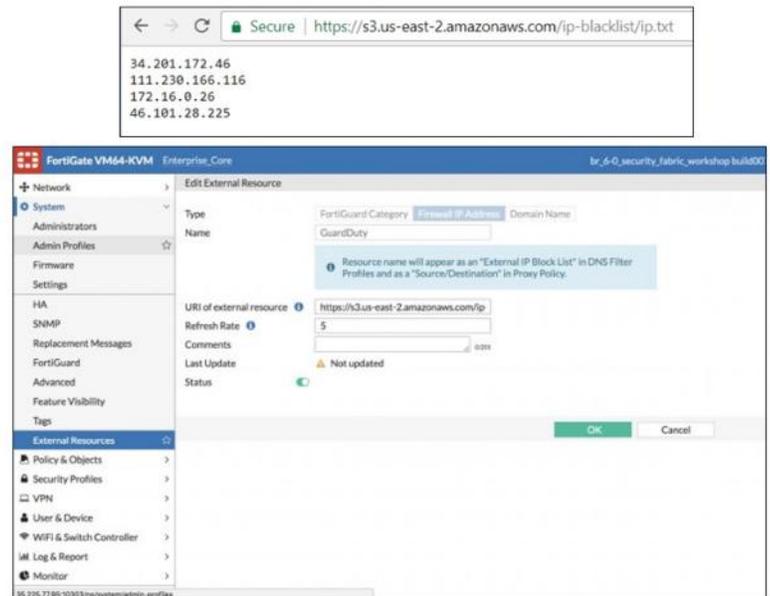
36

FortiGate has an automation stitches feature that can be combined with AWS Lambda or other vendors that invoke automation rules in the Fortinet Security Fabric. For example, you can use the Fortinet compromised host trigger feature with AWS Lambda to automatically quarantine any identified infected hosts in the network. There are many automation triggers that can be used with AWS Lambda.

DO NOT REPRINT
© FORTINET

GuardDuty Integration with FortiGate

- Automates security remediation for workloads running in AWS
- Accelerates time-to-protection for threats detected by the AWS service and automates the creation of network firewall rules in FortiGate to mitigate threats
- Reduces dependency on manual incident response and human intervention



FORTINET

© Fortinet Inc. All Rights Reserved.

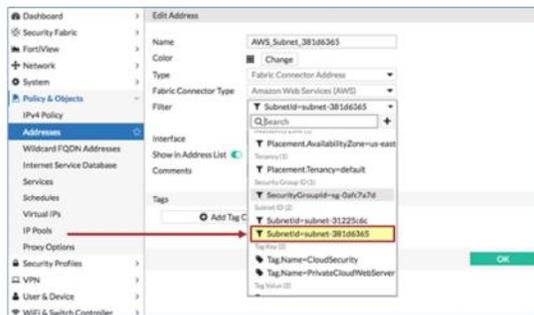
37

Amazon GuardDuty integration with FortiGate automates security remediation for workloads running in AWS. It accelerates time-to-protection for threats detected by the AWS service, and automates the creation of network firewall rules in FortiGate to mitigate threats. It also reduces the dependency on manual incident response and human intervention. You can use the URL of the GuardDuty blacklisted IP addresses found on the FortiGate **External Resources** page, in the **URL of external resource** field.

DO NOT REPRINT
© FORTINET

SDN Connector for AWS

- Dynamic address learning
- Scale up or scale down automatically



FORTINET

© Fortinet Inc. All Rights Reserved.

38

Fortinet Fabric Connectors help automate security operations and policies through one-click integrations with partners, including AWS. You can pull information from AWS, addresses, VM names, and subnets, and then use this information to create firewall policies. Compared to Azure, you need less information to configure this in AWS.

DO NOT REPRINT
© FORTINET

Fortinet WAF Cloud Offering

- Fortinet managed rules for AWS WAF
- FortiWeb-VM
- FortiWeb Cloud

FORTINET

© Fortinet Inc. All Rights Reserved.

39

There are different Fortinet offerings that can provide WAF protection in AWS. For example, you can deploy a FortiWeb VM inside the VPC. One of the drawbacks in this scenario is that you can protect only applications going through inside the VPC.

You can also use FortiWeb Cloud, which is a WAF-as-a-service hosted by Fortinet, but it runs in AWS. You can use FortiWeb Cloud to protect applications that are Internet-facing. For example, you can have your DNS records pointing to the service, and then allow only web application traffic coming from FortiWeb Cloud and block all other traffic.

DO NOT REPRINT
© FORTINET

Fortinet Managed Rules for AWS WAF

- Focus on building and delivering applications, not managing security rules



FORTINET

© Fortinet Inc. All Rights Reserved.

40

FortiWeb rule sets are additional security signatures that you can use to enhance the protections included in the base AWS WAF product. They are based on FortiWeb security service signatures, and are updated on a regular basis to include the latest threat information from FortiGuard Labs.

DO NOT REPRINT
© FORTINET

Fortinet Managed Rule Sets

FORTINET SQLI/XSS	FORTINET MALICIOUS BOTS	FORTINET GEN+KNOWN EXPLOITS	FORTINET OWASP TOP 10
<ul style="list-style-type: none"> Basic protection rules SQL injection Cross site scripting (XSS) <hr/> <ul style="list-style-type: none"> Foundational rules Additive to AWS XSS and SQLi protection 	<ul style="list-style-type: none"> Malicious bots Content scrapers Vulnerability scanners <hr/> <ul style="list-style-type: none"> Specialized protections Protects from known unwanted automated clients 	<ul style="list-style-type: none"> Advanced ruleset General attacks Known exploits <hr/> <ul style="list-style-type: none"> FortiGuard proprietary protections Injection attacks URL redirects HTTP response splitting 	<ul style="list-style-type: none"> SQLi/XSS General attacks Bots Known exploits <hr/> <ul style="list-style-type: none"> Complete set of all rules Discount over purchasing separately FortiGuard proprietary protections

- Four separate packaged rule sets
- Based on FortiGuard FortiWeb WAF signatures
- Available on AWS Marketplace
- Customer benefits:
 - Nearly the same level of protection as WAF signatures on FortiWeb WAF appliances (when combined and all rules used)
 - Latest threat intelligence from FortiGuard
 - Optimized rules for AWS environment
 - Simplified billing through AWS Marketplace
 - Pay only for what is used

FORTINET

© Fortinet Inc. All Rights Reserved.

41

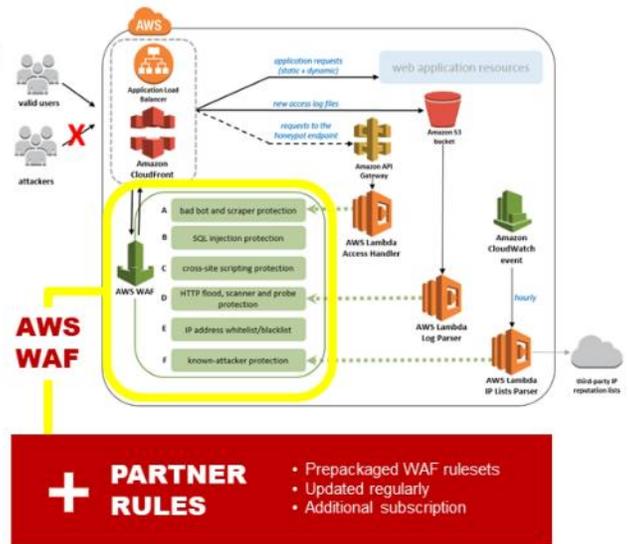
You can also purchase additional rule packages. There are four separate packaged rule sets based on FortiGuard FortiWeb WAF signatures, which are available on AWS Marketplace. These rule sets offer the same level of protection as WAF signatures on FortiWeb WAF appliances (when combined, and all rules are used). Some of the benefits of Fortinet managed rule sets include:

- Latest threat intelligence from FortiGuard
- Optimized rules for the AWS environment
- Simplified billing through AWS Marketplace
- Pay only for what is used

**DO NOT REPRINT
© FORTINET**

AWS WAF Partner Rule Basics

- AWS offers basic SQLi and XSS in their current WAF offering; (not their strength)
- AWS WAF lacks known exploits and vulnerabilities, and many attacks go unprotected
- Additional service to augment AWS WAF
- AWS partners with WAF vendors to offer prepackaged rule sets
- Can subscribe up to three times the partner rule sets
- Actions at rule set level: log, alert, block
- Customer benefits:
 - Additional WAF protections from leading WAF vendors
 - Ensures protection is up-to-date with latest signatures
 - Simplifies WAF setup and management
 - Conveniently available on AWS Marketplace



FORTINET

© Fortinet Inc. All Rights Reserved.

42

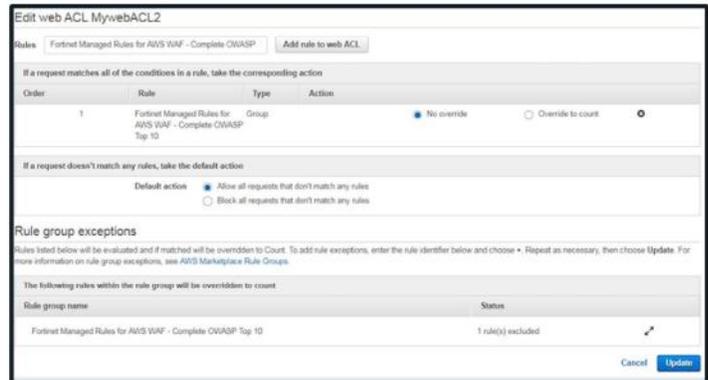
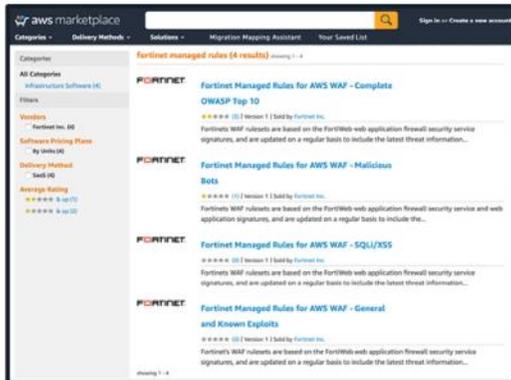
AWS WAF partner rule groups are subscription-based, web application firewall signatures offered by third-party vendors to augment the basic WAF protections offered by the Amazon WAF product. These new rule groups allow AWS WAF customers to choose prepackaged WAF rules from leading IT security providers. Until now, AWS offered only SQL injection and cross-site scripting (XSS) protection. With partner rule groups, vendors now offer protection from a wide variety of application layer attacks packaged in a variety of security rule sets. Some customer benefits include the following:

- Additional WAF protections from leading WAF vendors
- Ensures protection is up-to-date with the latest signatures
- Simplifies WAF setup and management
- Conveniently available on AWS Marketplace

DO NOT REPRINT
© FORTINET

Fortinet Managed Rules for AWS WAF

- Configurable from the AWS WAF console
- Listings accessible from AWS Marketplace



FORTINET

© Fortinet Inc. All Rights Reserved.

43

This slide shows how AWS WAF appears on the AWS WAF console and AWS Marketplace. You can purchase WAF packages from AWS Marketplace and enable them on the WAF configuration.

DO NOT REPRINT
© FORTINET

FortiWeb vs. Fortinet AWS WAF Rules

Feature	FortiWeb	AWS WAF partner rules
Web App Attack Signatures	Yes	Yes
WAF Subscription (FortiGuard)	Yes	Yes
IP Reputation (FortiGuard subscription)	Yes	No
Layer 7 DoS Protection	Yes	No
Bot and known search engine identification/protection	Yes	Yes (Partial)
Captcha	Yes	No
HTTP RFC Validation	Yes	No
Cookie Security	Yes	No
Antivirus/Antimalware	Yes	No
Behavioral Web App Attack Detection	Yes	No
Attack Correlation (protection from scanners, crawlers, scrapers)	Yes	No
Web App Vulnerability Scanner	Yes	No
Attack Alert Tuning	Yes	No
Web Defacement Protection	Yes	No
User and Device Identification	Yes	No
Brute Force Protection	Yes	No
Authentication Offload	Yes	No
Site Publishing and SSO	Yes	No
Meets PCI 6.6 Compliance	Yes	Yes
SSL Inspection	Yes	Yes

FORTINET

© Fortinet Inc. All Rights Reserved.

44

This slide shows a comparison between FortiWeb and AWS WAF partner rules. As you can see, there are some limitations to the AWS WAF partner rules. For example, there is no malware protection in AWS WAF partner rules because there is no engine to protect malware. So, if you need more rules, you can purchase Fortinet managed rule sets in addition to AWS WAF partner rules to get full protection.

DO NOT REPRINT
© FORTINET

WAF Product Positioning

	AWS WAF Partner Rules	FortiWeb
Primary function and focus	Skinny, simplified WAF for applications hosted on AWS using AWS WAF	Dedicated WAF (full feature set including behavior detection, customizable signatures, correlation)
Basic WAF (signatures, IP reputation, and so on)	Yes	Yes
Advanced WAF (behavioral scanning, correlation)	No	Yes
Up-to-date WAF signatures (FortiGuard)	Yes (optimized signatures)	Yes (subscription)
Customizable rules and white listing	No (negative security model)	Yes (positive and negative model)
Sample use cases	<ul style="list-style-type: none"> 1-2 small applications Mid-sized enterprise Application hosted on AWS Must use AWS WAF as base 	<ul style="list-style-type: none"> Mission critical web applications All segments including carrier/MSSP Applications hosted any location
When to position as best alternative	<i>Next step up</i> WAF protection for AWS applications using AWS WAF. Simplified deployment with better protections than standard AWS WAF rules.	Complete protection for applications including zero-day. WAF is primary focus of project. Needs full-fledge WAF for critical applications.
Pros	<ul style="list-style-type: none"> Easy to deploy and manage; convenient Pay for what is used Optimized FortiGuard signatures 	<ul style="list-style-type: none"> Dedicated WAF solution Zero-day protections Advanced features
Cons	<ul style="list-style-type: none"> Expensive for large applications No zero-day protection Only available for AWS WAF No rule customizations 	<ul style="list-style-type: none"> Separate appliance Increased investment Increased setup and management
Availability	<ul style="list-style-type: none"> AWS Marketplace only 	<ul style="list-style-type: none"> HW, VM, AWS (BYOL and On Demand), Azure (BYOL)

FORTINET

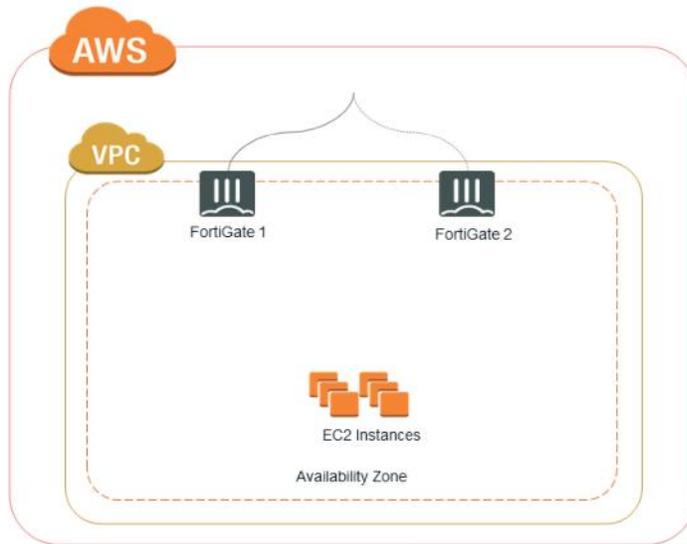
© Fortinet Inc. All Rights Reserved.

45

This slide shows WAF product positioning. It compares services between AWS WAF partner rules and FortiWeb.

DO NOT REPRINT
© FORTINET

Active-Passive FortiGate HA for AWS



- Single AZ
- Native active-passive FortiGate cluster
- Data plane and management HA
- Configuration synchronization
- Session synchronization
- CloudFormation template available on GitHub

FORTINET

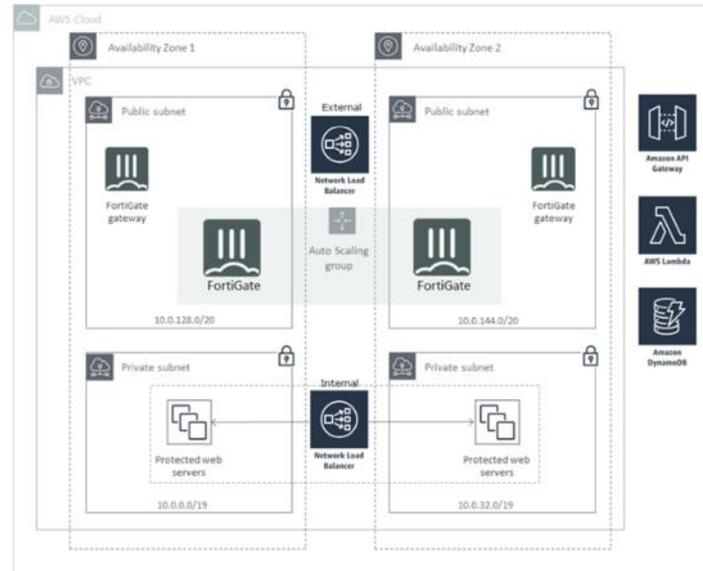
© Fortinet Inc. All Rights Reserved.

46

This slide shows an example of a FortiGate active-passive high availability scenario for AWS. This scenario is based on a single AZ. You will do an active-passive configuration in the lab. If you like, you can also try multiple AZs in the lab.

DO NOT REPRINT
© FORTINET

FortiGate Autoscaling for AWS



FORTINET

© Fortinet Inc. All Rights Reserved.

47

This is the example of FortiGate autoscaling for AWS. There are multiple FortiGate devices deployed in two different AZs. Also, there are two load balancers. You will do this configuration in the lab.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand AWS basic concepts
- ✓ Understand AWS components
- ✓ Understand AWS networking and security
- ✓ Understand Fortinet Security Fabric for AWS
- ✓ Understand Fortinet products on AWS Marketplace
- ✓ Understand FortiGate native active-passive HA
- ✓ Understand FortiGate active-active HA with AWS ELB
- ✓ Understand FortiGate autoscaling

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned the fundamentals of AWS and how to use Fortinet solutions with them.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about the Fortinet solution for Microsoft Azure.

**DO NOT REPRINT
© FORTINET**

Azure Fundamentals

Objectives

- Understand Azure basic concepts
- Understand Azure components
- Understand Azure networking
- Understand Azure security

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

By demonstrating competence in understanding Microsoft Azure fundamentals, you will be able to successfully use Microsoft Azure with the Fortinet solution.

DO NOT REPRINT
© FORTINET

Azure Products and Services

The screenshot displays the Microsoft Azure portal interface, organized into several service categories:

- Compute:** Virtual Machines, Virtual Machine Scale Sets, Azure Container Service, Azure Container Registry, Functions, Batch, Service Fabric, Cloud Services.
- Networking:** Virtual Network, Load Balancer, Application Gateway, VPN Gateway, Azure DNS, Traffic Manager, ExpressRoute, Network Watcher.
- Storage:** Storage Blobs, Tables, Queues, Files, Disks, Data Lake Store, StorSimple, Azure Backup, Site Recovery.
- Monitoring & Management:** Azure Portal, Azure Resource Manager, Azure Advisor, Azure Monitor, Log Analytics, Automation, Scheduler.
- Web & Mobile:** Web Apps, Mobile Apps, Logic Apps, API Apps, Content Delivery Network, Media Services, Search.
- Databases:** SQL Database, SQL Data Warehouse, SQL Server Stretch Database, DocumentDB, Redis Cache, Data Factory, HDInsight, Machine Learning, Cognitive Services, Azure Bot Service*, Data Lake Analytics, Power BI Embedded, Azure Analysis Services.
- Intelligence & Analytics:** (This category is merged into the Databases section in the image).
- Internet of Things & Enterprise Integration:** Azure IoT Hub, Event Hubs, Stream Analytics, Notification Hubs, BizTalk Services, Service Bus, Data Catalog.
- Security + Identity:** Security Center, Key Vault, Azure Active Directory, B2C, Domain Services, Multi-Factor Authentication.
- Developer Services:** Visual Studio Team Services, Azure DevTest Labs, VS Application Insights, API Management, HockeyApp, Developer Tools, Service Profiler*.

FORTINET

© Fortinet Inc. All Rights Reserved.

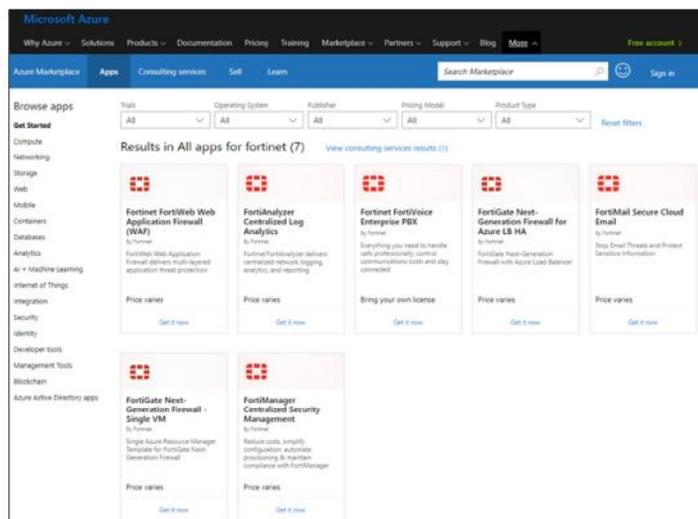
3

When you visit the Microsoft Azure portal, you will see many different services available. Depending on your requirements, you can choose only services that you require for your business. In the labs, you will use only four services, including virtual machines, VNET, Azure active directory (Azure AD), and load balancers.

DO NOT REPRINT
© FORTINET

Azure Marketplace

- Azure Marketplace is the premier destination for software needs
 - Software is certified and optimized to run on Azure
- Online applications and services marketplace
- Enables startups and independent software vendors to offer their solutions to Azure customers around the world



FORTINET

© Fortinet Inc. All Rights Reserved.

4

As shown on this slide, you can choose your software needs from the Azure Marketplace website. Azure Marketplace is the premier destination for software needs. The software is certified and optimized to run on Azure. The difference between Azure Marketplace and AWS Marketplace is that, in Azure, you can find FortiGate devices as templates. For example, you can find a FortiGate active-passive template as a load balancer instead of a single virtual machine. There are no CloudFormation templates directly on AWS Marketplace. Note that only officially supported templates can be found on Azure Marketplace. Azure Marketplace enables startups and independent software vendors to offer their solutions to Azure customers around the world.

DO NOT REPRINT**© FORTINET**

Azure Resource Manager (ARM)

- Deploy, manage, and monitor all the resources of a solution as a group, rather than handling these resources individually
- Benefits:
 - Repeatedly deploy solutions throughout the development lifecycle
 - Deploy resources in a consistent state
 - Manage your infrastructure through declarative templates, rather than scripts
 - Define dependencies between resources, so they are deployed in the correct order
 - Apply access control to all services in a resource group
 - Clarify your organization's billing by viewing costs for a group of resources that share the same tag
 - Use JSON to define the infrastructure of a solution
 - The JSON file is known as an ARM template

FORTINET

© Fortinet Inc. All Rights Reserved.

5

ARM is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure subscription. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

Some of the tasks that you can perform using ARM include:

- Repeatedly deploy solutions throughout the development lifecycle
- Deploy resources in a consistent state
- Manage your infrastructure through declarative templates, rather than scripts
- Define the dependencies between resources, so they are deployed in the correct order
- Apply access control to all services in a resource group
- Clarify your organization's billing by viewing costs for a group of resources that share the same tag
- Use JSON to define the infrastructure of a solution
 - The JSON file is known as a ARM template, and it tells ARM how to deploy in a specific environment

DO NOT REPRINT
© FORTINET

Azure SDKs and Tools

The screenshot displays the Azure SDKs and Tools page, organized into three main sections:

- Languages & Frameworks:**
 - Azure for .NET Developers: Get started, API reference
 - Azure for Python Developers: Get started, API reference
 - Azure for Node.js Developers: Get started, API reference
 - Azure for Java Developers: Get started, API reference
 - Azure for Go Developers: Get started, API Reference
 - Azure REST APIs: API Reference
- Command-Line Interface (CLI):**
 - Azure CLI: Get Started, Reference
 - Azure PowerShell: Get Started, Reference
- Tools & Extensions:**
 - Visual Studio Code: App Service, Azure Functions, Storage, Cosmos DB
 - Python Tools: Visual Studio, Visual Studio Code
 - Service Fabric SDK and Tools: Download for Windows, Download for Linux, Download Mac OS X, Download Service Fabric CLI
 - Docker: Visual Studio tools for Docker, Download for Visual Studio, Download for Visual Studio Code, Download for Team Services
 - Java Tools: Maven plugins, IntelliJ and Eclipse, Visual Studio Code
 - SQL Tools: SQL Operations Studio (PREVIEW), SQL Server Management Studio (SSMS), SQL Server Data Tools (SSDT), See all SQL tools
 - Storage Explorer: Get Started, Download for Linux, Download for Mac, Download for Windows

FORTINET

© Fortinet Inc. All Rights Reserved.

6

The Azure SDKs help developers build apps for Azure. As shown on this slide, there are different SDKs and tools, such as APIs and CLIs.

DO NOT REPRINT © FORTINET

Azure CLI

- The Azure CLI 2.0 is Azure's command-line experience for managing Azure resources
- You can use it in your browser with Azure Cloud Shell, or you can install it on macOS, Linux, or Windows, and run it from the command line
- Azure CLI 2.0 is optimized for managing and administering Azure resources from the command line, and for building automation scripts that work for the ARM

```
PowerShell
PS Azure> #If required, set the following variable to your own environment
PS Azure> $subscriptionName = "Free Trial"
PS Azure> $resourceGroup = "Lab01"
PS Azure> $servicePrincipalName = "Lab01app"
PS Azure>
PS Azure> #Do not modify the following part.
PS Azure> $password = "00000000"
PS Azure> $subscription = Get-AzSubscription -SubscriptionName $subscriptionName
PS Azure> $subscriptionId = $subscription.Id
PS Azure> $tenantId = $subscription.TenantId
PS Azure> $credentials = New-Object Microsoft.Azure.Commands.ActiveDirectory.PADPasswordCredential -Property @{StartDate: Get-Date; Password: $password}
PS Azure> $sp = New-AzServicePrincipal -DisplayName $servicePrincipalName -PasswordCredential $credentials
PS Azure> #Wait 100 seconds in between these two commands
PS Azure> Start-Sleep -s 100
PS Azure> $role = Get-AzRoleDefinition -RoleName $roleName -ResourceGroup $resourceGroup
PS Azure> $roleId = $role.Id
PS Azure> $resourceId = (Get-AzResourceGroup -Name $resourceGroup).ResourceId
PS Azure> #Print the results
PS Azure> Write-Host "`n Save the following information for your template parameters: " $tenantId $subscriptionId $sp.AppSecret $roleName $resource_group $resourceGroup`n
Save the following information for your template parameters:
Tenant_id: 2036478-3660-453f-8531-48364550119f
Subscription_id: 2297641b-9e3d-4911-ac04-70a64d111a7
Resource_group: 2036478-3660-453f-8531-48364550119f
App_secret: N8E7c1ou0P
Resource_group: Lab01
PS Azure>
```

The Azure CLI 2.0 is Azure's command-line experience for managing Azure resources. Azure CLI 2.0 is optimized for managing and administering Azure resources from the command line, and for building automation scripts that work for the ARM. There are two command line tool options available to you during the lab: Batch and PowerShell. You can use the tool in your browser with Azure Cloud Shell, or you can install it on macOS, Linux, and Windows, and run it from the command line. It is very convenient to have command line access within the Azure portal—you can easily copy and paste commands without having to log in to the CLI.

DO NOT REPRINT
© FORTINET

Azure Regions



FORTINET

© Fortinet Inc. All Rights Reserved.

8

Azure operates in multiple data centers around the world. These data centers are grouped into geographic regions, giving you flexibility in choosing where to build your applications. Within each region, multiple data centers exist to provide for redundancy and availability. This approach gives you flexibility as you design applications to create VMs closest to your users and to meet any legal, compliance, or tax purposes.

Region pairs: This approach allows for the replication of resources, such as VM storage, across a geography that should reduce the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.

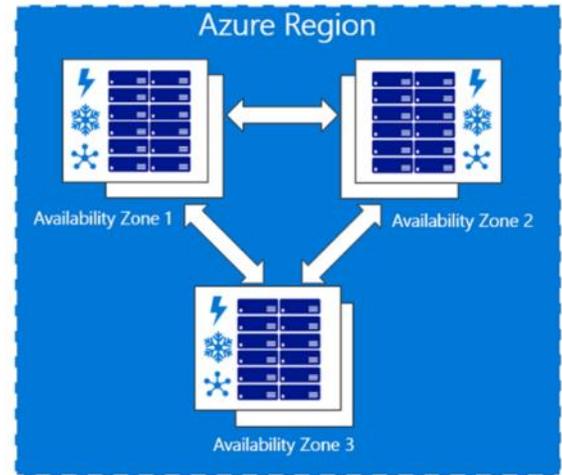
Feature availability: Some services or VM features are available only in certain regions, such as specific VM sizes or storage types.

Global Azure services that do not require a particular region: Azure AD, Azure Traffic Manager, or Azure DNS.

DO NOT REPRINT
© FORTINET

Azure Availability Zones

- Availability zones helps to protect against failures at the data center level
- Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking
- For resiliency, there are a minimum of three separate zones in all enabled regions
- The physical and logical separation of Availability zones within a region protects applications and data from zone-level failures

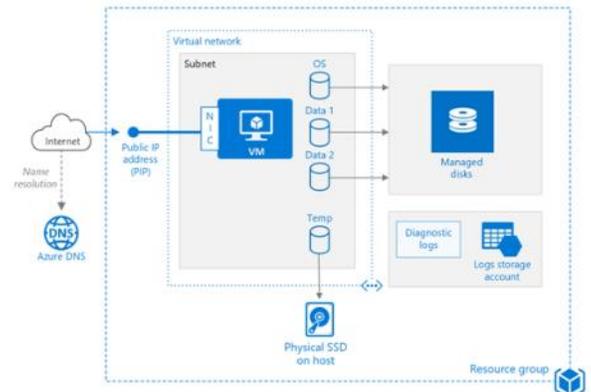


Azure Availability zones is a high-availability offering that protects your applications and data from data center failures. Availability zones are unique physical locations within an Azure region. Each Availability zone is made up of one or more data centers equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate Availability zones in all enabled regions. The physical separation of availability zones within a region protects applications and data from data center failures.

**DO NOT REPRINT
© FORTINET**

Virtual Machines (VMs)

- Azure VMs is one of several types of on-demand, scalable computing resources
- An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it
- VMs have outbound Internet connectivity by default



Azure VMs is one of several types of on-demand, scalable computing resources that Azure offers. An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the VM by performing tasks, such as configuring, patching, and installing the software that runs on it. As shown on this slide, the OS running inside Azure has storages, network interfaces. VMs have outbound Internet connectivity, by default.

DO NOT REPRINT
© FORTINET

Azure VM Series

+ General purpose	D	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
+ Compute optimized	F	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
+ Memory optimized	G	High memory-to-core ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
+ Storage optimized	L	High disk throughput and IO. Ideal for Big Data, SQL, and NoSQL databases.
+ GPU	N	Specialized virtual machines targeted for heavy graphic rendering and video editing available with single or multiple GPUs.
+ High performance compute	H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

FORTINET

© Fortinet Inc. All Rights Reserved.

11

There are different types of VMs available in Azure. Azure VM series components:

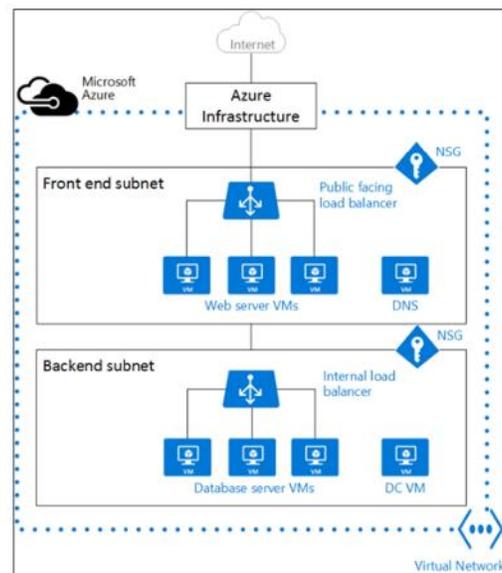
- A Series: Entry-level economical VMs for development and testing
- D Series: General purpose computing
- Dv2 Series: Next-generation, general-purpose computing
- F Series: Computing-optimized VMs
- G Series: Memory and storage-optimized virtual machines
- H Series: High-performance VMs
- L Series: Storage-optimized VMs
- N Series: GPU-enabled VMs

FortiGate or FortiWeb should be deployed in a computer-optimized VM series with more CPU resource availability, for better performance.

DO NOT REPRINT
© FORTINET

Azure VNet

- Azure virtual network (Vnet) capabilities
 - Isolation
 - Internet connectivity
 - Azure resource connectivity
 - VNet connectivity
 - On-premises connectivity
 - Traffic filtering
 - Routing



FORTINET

© Fortinet Inc. All Rights Reserved.

12

The Azure VNet service securely connects Azure resources to each other using VNets. A VNet is a representation of your own network in the cloud. You can also connect VNets to your on-premises networks. VNets group all the subnets within a region. During the lab, you will deploy the VNet as shown on this slide.

Isolation: VNets are isolated from one another. You can create separate VNets for development, testing, and production that use the same CIDR address blocks. Conversely, you can create multiple VNets that use different CIDR address blocks and connect networks together. You can segment a VNet into multiple subnets. Azure provides internal name resolution for VMs and Cloud Services role instances connected to a VNet. You can optionally configure a VNet to use your own DNS servers, instead of using Azure internal name resolution.

Internet connectivity: By default, all Azure VMs and Cloud Services role instances connected to a VNet have access to the Internet. You can also enable inbound access to specific resources, as needed.

Azure resource connectivity: Azure resources such as Cloud Services and VMs can be connected to the same VNet. The resources can connect to each other using private IP addresses, even if they are in different subnets. Azure provides default routing between subnets, VNets, and on-premises networks, so you don't have to configure and manage routes.

VNet connectivity: VNets can be connected to each other, enabling resources connected to any VNet to communicate with any resource on any other VNet.

On-premises connectivity: VNets can be connected to on-premises networks through private network connections between your network and Azure, or through a site-to-site VPN connection over the Internet.

Traffic filtering: You can filter VM and Cloud Services role instances network traffic by inbound and outbound by source IP address and port, destination IP address and port, and protocol.

Routing: You can optionally override Azure's default routing by configuring your own routes, or using BGP routes through a network gateway.

DO NOT REPRINT
© FORTINET

Azure VNet (Contd)

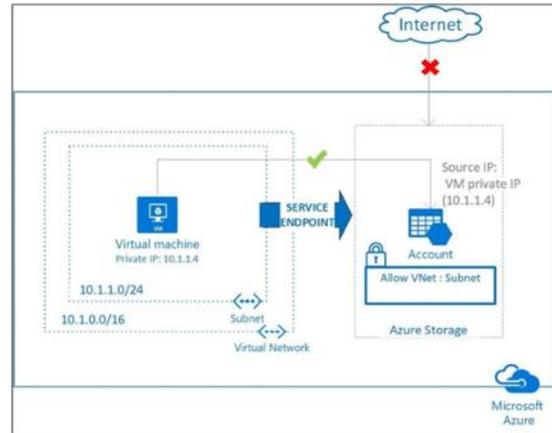
- Azure networking is built around the concept of VNets
- A VNet is a logical, isolated network within the Azure fabric
- By default, VNets are completely isolated from each other
- A VNet must be configured with at least one IP address space
- VMs are deployed into a subnet
- Private IP addresses can be allocated either dynamically or statically
- Public IP addresses can be basic or standard
 - A VM can have a public IP address assigned to it; it will be accessible from the Internet
 - Standard public IP addresses are zone redundant
- VMs in different subnets within a VNet can route to each other directly

It is possible for a VNet to have more than one address space assigned to it. With dynamic assignment, addresses are automatically allocated by the DHCP server when the VM starts and may not remain the same when the VM reboots. Static assignment means that you can manually specify the address and it will be set as a reservation by DHCP. The public IP address actually exists as a network address translation (NAT) entry on the Azure fabric that gets mapped to the VM. If you are attaching a standard SKU public IP address to a VM interface, you *must* apply a network security group; otherwise, you will not be able to reach that VM.

DO NOT REPRINT
© FORTINET

Connected Azure Resources

- You can connect several Azure resources to a VNet, such as:
 - VMs
 - Cloud services
 - App service environments
 - VM scale sets
- VMs connect to a subnet within a VNet through a network interface

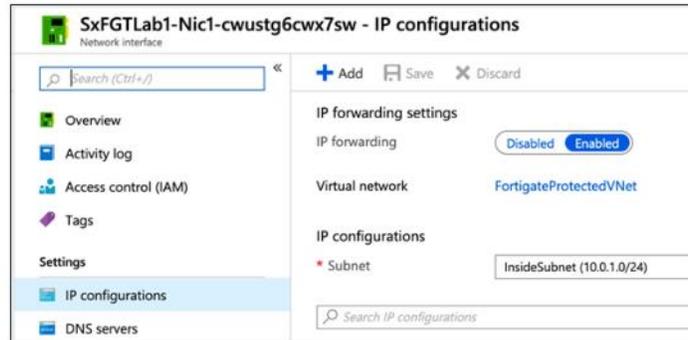


You can connect several Azure resources to a VNet, such as VMs, cloud services, application service environments, and VM scale sets. VMs connect to a subnet within a VNet through a network interface.

DO NOT REPRINT
© FORTINET

IP Forwarding

- Set by network interface
- Allows forwarded source IPs different from the assigned IP of the interface
- Required on *private* FortiGate interface when routing traffic to other networks like the Internet



When you deploy a network device, It is important to have the correct IP forwarding settings of Azure virtual network card. For example, IP forwarding allows FortiGate to generate traffic using source IP address different from the IP address which is assigned to the virtual network interface. If this feature is not enabled, packet will be identified as a spoofing packet, because the reply packet from the Internet forwarded from FortiGate to the client uses the public IP address of Internet service and is identified as a spoofing packet. So you have to make sure that this feature is enabled from the network interface to avoid it. In AWS, this feature works the opposite way, so you will need disable this feature in AWS.

**DO NOT REPRINT
© FORTINET**

Connected to the Internet

- By default, all resources connected to a VNet have outbound connectivity to the Internet
- The private IP address of the resource is source network address translated (SNATed) to a public IP address by the Azure infrastructure
 - You can change the default connectivity by implementing custom routing and traffic filtering
- To communicate inbound to Azure resources from the Internet, or to communicate outbound to the Internet without SNAT, a resource must be assigned a public IP address

By default, all resources connected to a VNet have outbound connectivity to the Internet. You can have a public IP addresses assigned to network interface or an assigned private IP address can connect to the internet using a route defined in the routing table. The private IP address of the resource is SNATed to a public IP address by the Azure infrastructure. You can change the default connectivity by implementing custom routing and traffic filtering. To communicate inbound to Azure resources from the Internet, or to communicate outbound to the Internet without SNAT, a resource must be assigned a public IP address.

DO NOT REPRINT

© FORTINET

Routing

- By default, Azure creates route tables that enable resources connected to any subnet in any VNet to communicate with each other
- You can implement either or both of the following options to override the default routes Azure creates:
 - User-defined routes
 - BGP routes

By default, Azure creates route tables that enable resources connected to any subnet in any VNet to communicate with each other. You can implement either or both user-defined routes or BGP routes to override the default routes Azure creates.

DO NOT REPRINT
© FORTINET

Azure Routes Priority

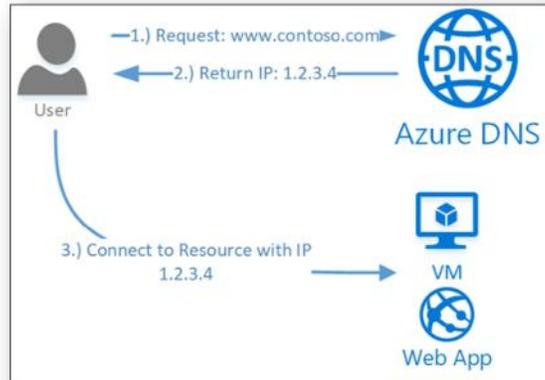
1. User-defined routes (UDR)
 2. BGP routes
 3. System routes
- However, the most specific route always wins
 - 10.0.3.0/24 system route would precede 10.0.0.0/16 BGP route
 - If routes are equally specific, then above applies: 10.0.3.0/24 UDR wins

It is important to know the route priority in Azure. As shown on the slide, if all the routes in route table are equally specific, then the preferred route is UDR followed by BGP and system routes. However, the most specific route always wins. For example, 10.0.3.0/24 system route would precede 10.0.0.0/16 BGP route. If routes are equally specific, then priority order applies and UDR wins. UDRs are very powerful in Azure.

DO NOT REPRINT
© FORTINET

Azure DNS

- Responsible for translating (or resolving) a website or service name to its IP address
- A hosting service for DNS domains, providing name resolution using the Microsoft Azure infrastructure
- Features:
 - Reliability and performance
 - Seamless integration
 - Security



Azure DNS is a hosting service for DNS domains that provides name resolution using the Microsoft Azure infrastructure. Azure DNS is responsible for translating (or resolving) a website or service name to its IP address. It provides reliability, performance, seamless integration, and security. DNS service can be configured for public DNS or internal DNS.

DO NOT REPRINT
© FORTINET

Azure Load Balancer

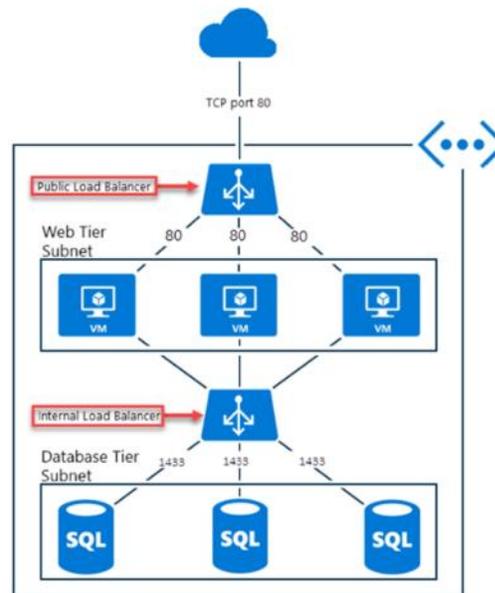
- Delivers high availability and network performance to your applications
- It is a Layer 4 (TCP, UDP) load balancer:
 - Distributes incoming traffic among healthy instances of services defined in a load-balanced set
- Azure Load Balancer can be configured to:
 - Load balance incoming Internet traffic to virtual machines
 - Load balance traffic between virtual machines in a virtual network, between virtual machines in cloud services, or between on-premises computers and virtual machines in a cross-premises virtual network
 - Forward external traffic to a specific virtual machine
- Standard load balancer adds support for zone redundancy

Azure Load Balancer can scale your applications and create high availability for your services. Azure Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications. Azure Load Balancer can be configured to load balance incoming Internet traffic to virtual machines, traffic between virtual machines in a virtual network, traffic between virtual machines in cloud services, or traffic between on-premises computers and virtual machines in a cross-premises virtual network. Azure Load Balancer can also be configured to forward external traffic to a specific virtual machine. The standard load balancer adds support for zone redundancy.

DO NOT REPRINT
© FORTINET

Azure Load Balancer (Contd)

- Load balancer types
 - Basic and standard
 - Public and internal
 - Layer 4 and application gateway (HTTP/HTTPS)
- Direct server return (also called floating IP) load balancer rules
 - No DNAT
- Backend pool member
 - VMs
 - VM scale set
 - VM availability set



FORTINET

© Fortinet Inc. All Rights Reserved.

21

There are different types of load balancers. A standard load balancer can load balance traffic across multiple availability zones. A basic load balancer can load balance only inside the availability zone. A public load balancer has public IP addresses and shows internal load balancer has a private IP address in an external facing interface. This slide shows two load balancers, a public load balancer for applications, and an internal load balancer for the database layer. For IPsec load balancing, you can use a Layer 4 load balancer. You can use an application gateway load balancer to load balance all your applications.

Direct server returns (or floating IP) is the Azure feature that prevents destination NAT (DNAT) from being translated. So, traffic received to the destination VM must reply directly to the source IP address. Basically, the destination VM does not send traffic back to the load balancer; the load balancer only redirects traffic.

For backend pool members, you can add VMs, and scale set or availability set. Any devices that you add to the availability set are automatically added to the target members of the load balancer.

DO NOT REPRINT
© FORTINET

Traffic Manager

- A DNS-based global load balancing service
- Azure Traffic Manager can also work with non-Azure-based endpoints
- Azure Traffic Manager has four routing methods:
 1. Priority routing
 2. Weighted routing
 3. Performance routing
 4. Geographic routing



FORTINET

© Fortinet Inc. All Rights Reserved.

22

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to optimally distribute traffic to services across global Azure regions, while providing high availability and responsiveness. Azure Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic routing method and the health of the endpoints. An endpoint is any Internet-facing service that is hosted inside or outside of Azure. Azure Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models.

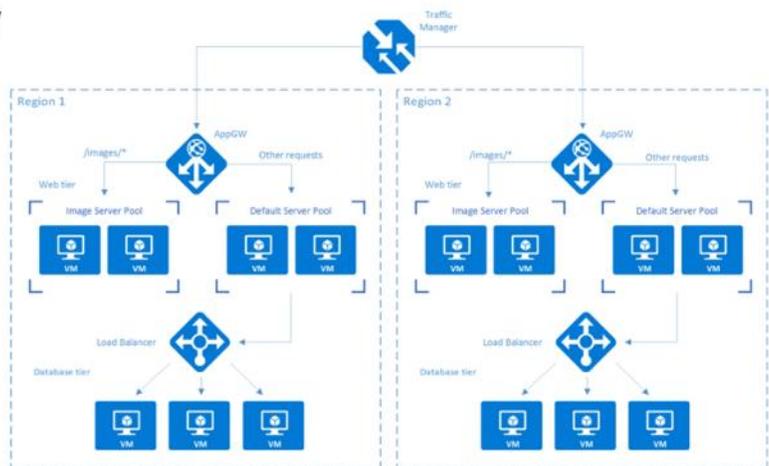
Azure Traffic Manager has four routing methods:

- Priority routing
- Weighted routing
- Performance routing
- Geographic routing

DO NOT REPRINT
© FORTINET

High Resilience Deployments

- Azure Traffic Manager for lower latency and multi-geo redundancy
- Azure Application Gateway to scale various request workloads
- Internal load balancers to deliver connections to the healthy HA cluster backend nodes



FORTINET

© Fortinet Inc. All Rights Reserved.

23

This slide shows an examples of a high resilience deployment. In the example, DNS traffic is going to the traffic manager and the traffic manager decides which region to send the traffic to. Each region has a public load balancer or application gateway load balancer that load balances traffic between VMs in different availability zones. Also, there is an internal load balancer for load balancing traffic between internal VMs.

Azure Traffic Manager helps to lower latency and provide multi-geo redundancy between regions. Azure Application Gateway scales various request workloads and internal load balancers deliver connections to the healthy HA cluster backend nodes.

**DO NOT REPRINT
© FORTINET**

Connecting VNets

- You can connect virtual networks (VNets) to each other, enabling resources connected to either VNet to communicate with each other across VNets
- There are two main ways to achieve connectivity between different VNets:
 - VNet peering
 - VPN gateways

There are multiple ways to connect VNets to each other: you can connect an existing virtual network to another VNet, you can use FortiGates VMs with IPSec between two Vnets, or you can use Azure VNet peering or Azure VPN gateways.

DO NOT REPRINT**© FORTINET**

Peering and VNet-to-VNet

- Peering:
 - Enables resources connected to different Azure VNets within the same Azure location to communicate with each other
 - The bandwidth and latency across the VNets is the same as if the resources were connected to the same VNet
- VNet-to-VNet connection:
 - Enables resources connected to different Azure VNets within the same, or different, Azure locations
 - Bandwidth is limited between VNets because traffic must flow through an Azure VPN gateway

VNet peering enables you to seamlessly connect Azure VNets. After they are peered, the VNets appear as one, for connectivity purposes. The traffic between VMs in the peered VNets is routed through the Microsoft backbone infrastructure, much like traffic is routed between VMs in the same VNet, through private IP addresses only. VNet peering enables resources connected to different Azure VNets within the same Azure location to communicate with each other. The bandwidth and latency across the VNets is the same as if the resources were connected to the same VNet.

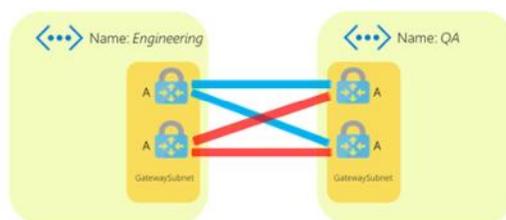
VNet-to-VNet connection enables the connection of resources connected to different Azure VNets within the same, or different, Azure locations. Bandwidth is limited between VNets because traffic must flow through an Azure VPN gateway.

DO NOT REPRINT

© FORTINET

VPN Gateways

- VPN gateways can be used to connect two VNets, or between on-premises networks and Azure VNets:
 - To connect two VNets, you must create a VPN gateway in each VNet
 - VPN gateways always connect to a special subnet, called GatewaySubnet (this name is mandatory)
 - To create a connection, specify the two VPN gateways and configure a shared key
 - VPN gateways consist of two instances in an active-standby configuration
 - It is also possible to create VPN gateways in an active-active configuration, which will use a full mesh of IPsec tunnels



FORTINET

© Fortinet Inc. All Rights Reserved.

26

VPN gateways can be used to connect two VNets, or between on-premises networks and Azure VNets. In order to connect two VNets together, you must create a VPN gateway in each VNet, VPN gateways always connect to a special subnet, called GatewaySubnet (this name is mandatory). To create a connection, specify the two VPN gateways and configure a shared key. VPN gateways consist of two instances in an active-standby configuration. It is also possible to create VPN gateways in an active-active configuration, which will use a full mesh of IPsec tunnels. Failure of a gateway will result in the standby taking over. (The worst case scenario is 90 seconds of failover time.)

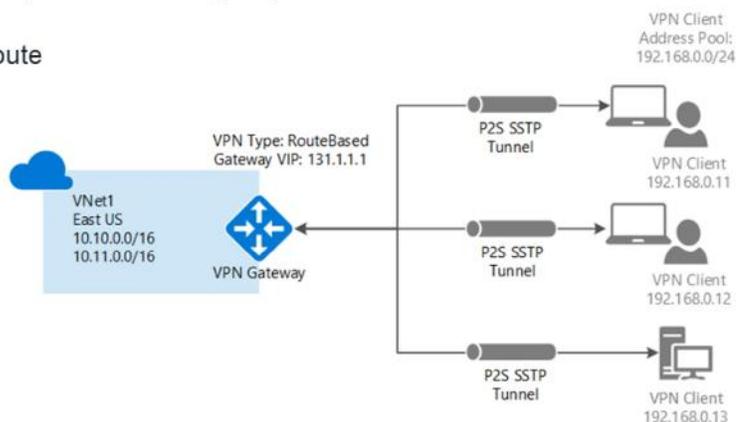
You can also have a FortiGate on one side and Azure VPN gateway on the other side.

DO NOT REPRINT
© FORTINET

Connecting to On-Premises Networks

- You can connect your on-premises network to a VNet using any combination of the following options:

- Point-to-site virtual private network (VPN)
- Site-to-site VPN
- Azure ExpressRoute



FORTINET

© Fortinet Inc. All Rights Reserved.

27

You can connect your on-premises network to a VNet using any combination of the following options:

Point-to-site VPN: Established between a single PC connected to your network and the VNet. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The connection uses the SSTP protocol to provide encrypted communication over the Internet between the PC and the VNet. The latency for a point-to-site VPN is unpredictable and encrypted, because the traffic traverses the Internet.

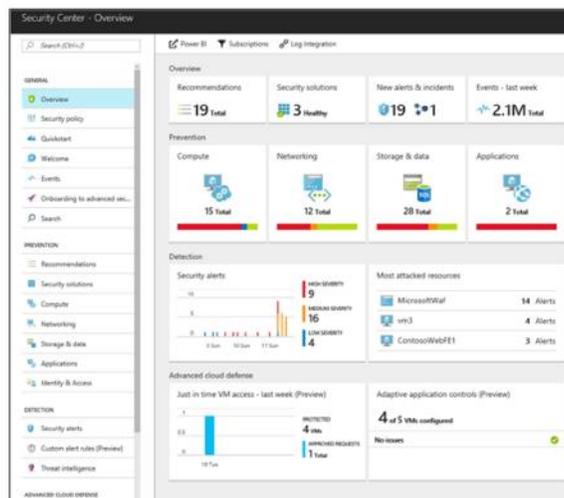
Site-to-site VPN: Established between your VPN device and an Azure VPN Gateway. This connection type enables any on-premises resource you authorize to access a VNet. The connection is an IPsec/IKE VPN that provides encrypted communication over the Internet between your on-premises device and the Azure VPN gateway. The latency for a site-to-site connection is unpredictable, because the traffic traverses the Internet.

Azure ExpressRoute: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not traverse the Internet. The latency for an ExpressRoute connection is predictable, because traffic doesn't traverse the Internet and isn't encrypted.

DO NOT REPRINT
© FORTINET

Azure Security Center

- Azure Security Center helps you prevent, detect, and respond to threats with increased visibility into, and control over, the security of your Azure resources
- It provides integrated security monitoring and policy management across your Azure subscriptions
- It helps detect threats that might otherwise go unnoticed
- It works with a broad ecosystem of security solutions; Fortinet is one of them



FORTINET

© Fortinet Inc. All Rights Reserved.

28

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection (ATP) across your hybrid workloads in the cloud. Security Center helps you prevent, detect, and respond to threats with increased visibility into, and control over, the security of your Azure resources. Some of the benefits of Azure Security Center include, integrated security monitoring and policy management across Azure subscriptions, and detection of threats that might otherwise go unnoticed. Azure Security Center works with a broad ecosystem of security solutions, including Fortinet.

DO NOT REPRINT
© FORTINET

Azure Security Center Recommendations

The screenshot displays the Azure Security Center interface. The top section shows an overview with 10 total recommendations, 1 security solution, 0 new alerts & incidents, and 71.1K events in the last week. A red box highlights the 'Recommendations' section. Below this, a table lists several recommendations, with 'Add a Next Generation Firewall' highlighted in blue and circled in red. To the right, a detailed view of this recommendation is shown, featuring a 'Create New' button circled in red and a list of vendor options including Fortinet.

DESCRIPTION	RESOURCE	STATE	SEVERITY
Enable advanced security for subscriptions	1 subscriptions	Open	High
Add a Next Generation Firewall	UbuntuSubnet3-ip	Open	High
Enable Network Security Groups on subnets	53 subnets	Open	High
Enable Network Security Groups on virtual machines	44 virtual machines	Open	High
Apply a Just-In-Time network access control (preview)	28 virtual machines	Open	High

© Fortinet Inc. All Rights Reserved. 29

Azure Security Center can give you some recommendations based on your deployment. As shown on this slide, Azure highly recommends adding a next generation firewall (NGFW) to your deployment. In order to satisfy the populated recommendations, you must deploy the recommended devices from this menu. All the vendor names are displayed in alphabetical order.

DO NOT REPRINT
© FORTINET

Network Traffic Filtering

- You can filter network traffic between subnets using one or more of the following options:
 - Network security groups (NSG)
 - Azure firewall
 - Network virtual appliances (NVA)

You can filter network traffic between subnets using one or more of the following options:

- NSG
- Azure firewall
- NVA

DO NOT REPRINT © FORTINET

NSG

- Lock down access to a subnet or VM
- Provide a list of access control rules, permitting or denying traffic based on various criteria
- Can be applied either at the NIC level or at the subnet level
- Works only if a resource is connected to a VNet—they do not work for other resources (like PaaS services)



NSG is a list of access control rules that permit or deny traffic based on various criteria. NSG can be applied either at the NIC level or at the subnet level. NSGs work only if a resource is connected to a VNet—they do not work for other resources (like PaaS services). NSG can be applied to network interfaces or to a full subnet. Note that NSGs are stateful and no bidirectional policies are needed.

DO NOT REPRINT
© FORTINET

NVA

- A VM running software that performs a network function, such as:
 - FortiGate
 - FortiWeb
- Available to provide WAN optimization and other network traffic functions
- Typically used with UDR or BGP
- Can be used to filter traffic between VNets

An NVA is a VM running software that performs a network function, such as FortiGate and FortiWeb. NVAs can provide WAN optimization and other network traffic functions. NVAs are typically used with UDR or BGP. You can also use an NVA to filter traffic between VNets.

**DO NOT REPRINT
© FORTINET**

Fortinet Solutions for Azure

Objectives

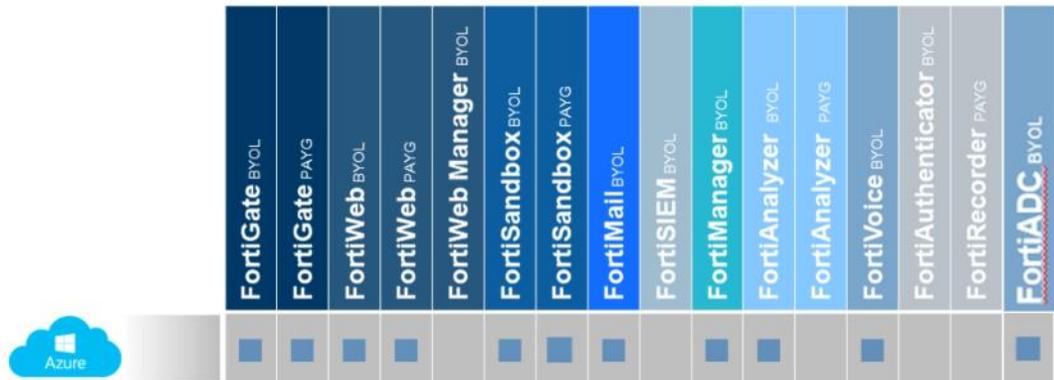
- Understand Fortinet on Azure Marketplace: sizing and PAYG-BYOL table
- Understand FortiGate Fabric Connector for Azure
- Understand FortiWeb on Azure
- Understand FortiGate native active-passive HA
- Understand FortiGate active-active HA with Azure Load Balancer
- Understand FortiGate autoscaling (VMSS, CosmosDB, FunctionApp)

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

By demonstrating competence in Fortinet solutions for Azure, you will be able to successfully deploy and use Fortinet products in Azure Marketplace.

DO NOT REPRINT
© FORTINET

Fortinet Products in Azure Marketplace



FORTINET

© Fortinet Inc. All Rights Reserved.

34

This diagram shows Azure Marketplace availability for Fortinet products. Keep in mind that the information shown in this diagram could change, based on the new support availability for Fortinet products.

DO NOT REPRINT
© FORTINET

SDN Connector for Azure

- Part of FortiOS 6.0 multicloud Security Fabric support
- Updates dynamic address elements

FORTINET

© Fortinet Inc. All Rights Reserved.

35

Fortinet provides different ways to communicate with the Azure. Public connectors called Fortinet SDN connectors can be used to connect with Azure. As shown on this slide, you can use different parameters to connect. For example, you do not need to configure a VM with the IP address on the FortiGate. The VM IP address is obtained automatically through APIs. This is the reason why you should keep the FortiGate configuration as dynamic as possible, without assigning parameters statically. You will learn how to obtain all the parameters during the lab.

DO NOT REPRINT
© FORTINET

SDN Connector for Azure

- Before you can configure this, you need to identify:
 - Azure tenant ID (Directory ID)
 - Azure client ID (Application ID)
 - Azure subscription ID
 - Azure client secret (Application key)
 - Azure resource group

FORTINET

© Fortinet Inc. All Rights Reserved.

36

When you are configuring FortiGate settings, you will need to get all the parameters from the Azure portal. However, determining the correct name for the settings can be challenging. FortiGate names are identical to the API names; however, Azure uses different names in their portal. For example, the Azure tenant ID is called the directory ID in Azure, and the Azure client ID is called the application ID.

DO NOT REPRINT
© FORTINET

SDN Connector for Azure (Contd)

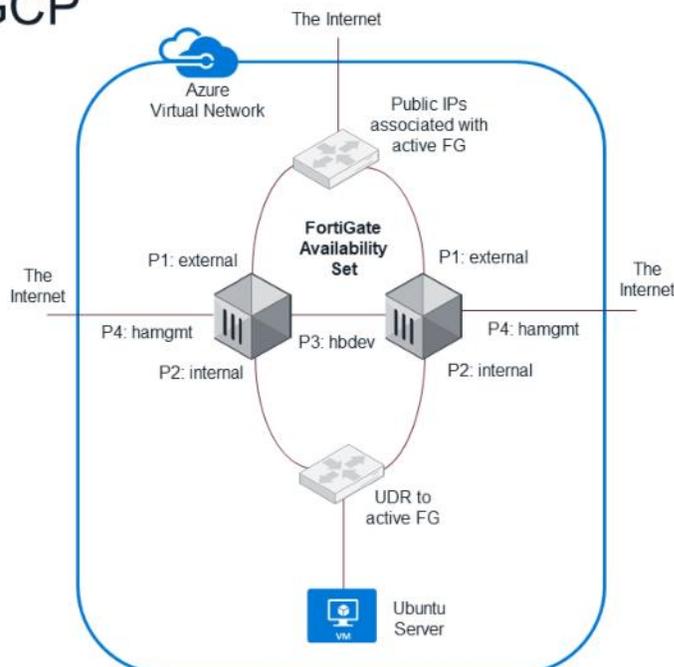
- Supported filters:
 - set filter 'vm=<vm id>'
 - set filter 'securitygroup=<nsg id>'
 - set filter 'vnet=<virtual network id>'
 - set filter 'subnet=<subnet id>'
 - set filter 'vmss=<vmss id>'
 - set filter 'tag.<key>=<value>'
- There are many types of tags in Azure; currently, Fortinet supports only the tag set in VM
- The current implementation limits use to **one subscription and one resource group only** and to only resources in use and associated with running VMs

As shown on this slide, there are several types of filters that you can use. There are also many types of tags in Azure. Currently, Fortinet supports the tag set in VM only. For example, you can create a tag called security policy and setup a value as DMZ. When a new VM is deployed by IT staff in DMZ, the security policy tag can be added for the DMZ server from FortiGate. FortiGate automatically pulls the IP addresses related to the tag and added to the DMZ outgoing policy, without making any changes to FortiGate. Current implementation will limit use to one subscription and one resource group only, and only resources that are in use and associated with running VMs will be allowed.

DO NOT REPRINT
© FORTINET

Active-Passive Unicast FGCP

- Inside one Azure Region
- Minimum three interfaces, but four is better
- Heartbeat and management interfaces in system VDOMs, unusable for productive traffic
- Management interface (port4) for accessing firewalls and reaching out to Azure Management for failover API commands



FORTINET

© Fortinet Inc. All Rights Reserved.

38

There is no traditional FortiGate Clustering Protocol (FGCP) to use in high availability (HA) on cloud computing. The solution is to use HA active passive unicast FGCP which is modified version of the traditional Fortinet clustering protocol. In this scenario, there is no multicast traffic between heart beat interfaces, instead, only unicast traffic. In order to form two FortiGate devices in HA, the peer IP address needs to be configured in each FortiGate device. Also, there is a management interface (port4) which is unique to each cluster member and has a subnet with Internet access. Each cluster member can be accessed separately through management interfaces. There are two interfaces processing the traffic—external and internal—and both heartbeat and management interfaces are system VDOMs, which are hidden and unusable for processing production traffic.

**DO NOT REPRINT
© FORTINET**

SDN Connector—Additional Configuration for Active-Passive Unicast FGCP

- Add to:

```
config system sdn-connector
  edit <connector-name>
```
- Be careful, entries are node-specific!

```
config nic
  edit "FGHAX-Z-Nic1"
  config ip
    edit "ipconfig1"
    set public-ip "FGTXClusterPublicIP"
    next
  end
  next
end
config route-table
  edit "FGTDefaultAPRouteTable"
  config route
    edit "toDefault"
    set next-hop "10.X.2.Y"
    next
  end
  next
end
```

Azure **node-specific** network interface name

Azure ipconfig name, associated with public IP

Azure public IP **name, not IP**

Azure UDR name

Azure route name

Node-specific next hop = firewall port IP

FORTINET

© Fortinet Inc. All Rights Reserved.

39

This slide shows how to configure an API for an active-passive cluster. When you configure fabric connectors on FortiGate, you can add the settings shown on this slide. You will be using this configuration during the lab. For example, FortiGate NIC is pointing to the Azure public IP address, which redirects traffic to the slave device. You will also modify the routing table, as shown on this slide. Note that this configuration is unique to each cluster member. This is the desired configuration if the slave becomes the master in the cluster.

DO NOT REPRINT**© FORTINET**

Active-Passive Unicast FGCP Tips

- Static IP addresses are required
 - Keep config in sync in Azure and FortiOS
- `config nic` under `config system sdn-connector` settings are not synced and require node-independent settings for NIC and UDR next-hop IP
- Inbound traffic requires two virtual IP elements or 0.0.0.0 as external
 - Interface IP address config is not synced
- Use `set override disable` to avoid unnecessary failovers

FORTINET

© Fortinet Inc. All Rights Reserved.

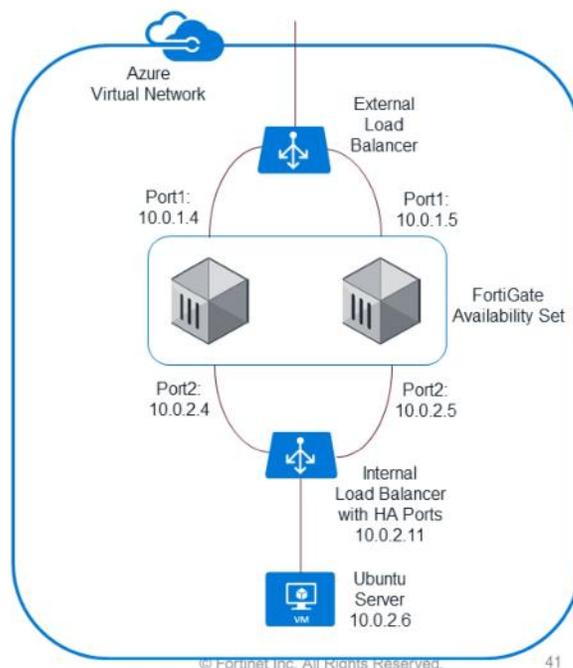
40

This slide shows some useful tips that you can use when configuring active-passive unicast cluster. It is very important to disable the override settings to avoid unnecessary failovers. Setting specific devices to always take the same role in the cloud is not recommended. For example, setting a particular device as master. If a failover happens, another API must be called and may take some time to finish the process. How virtual IP (VIP) addresses work depends on the cloud vendor. FGCP uses the same IP address on both FortiGate devices when traffic passes. Also, you will see a unique primary IP address and secondary IP address. The secondary IP address can move from one device to another. So, you have to know which IP address to use as an external IP address. For this reason, it is recommended that you use 0.0.0.0 as the external VIP address, instead of using multiple IP addresses.

DO NOT REPRINT
© FORTINET

Active-Active FortiGate Devices with Azure Load Balancer

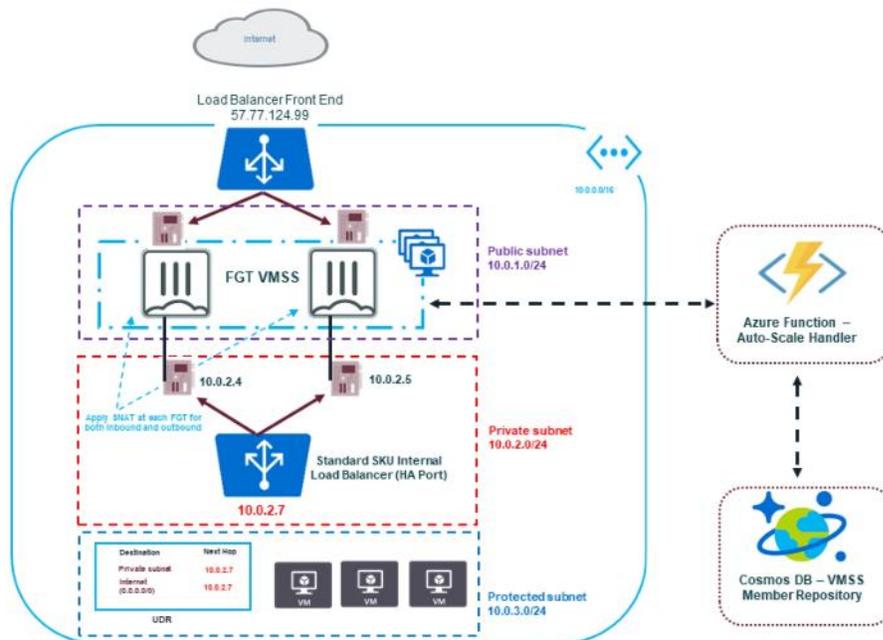
- Azure Load Balancer **can** be used for outbound and east/west connections
- Use an Azure Marketplace or GitHub account to retrieve the current load balancer template
- Load balancer failover depends on the health probes
- FGSP connection sync can't keep connections alive, if SNAT is applied
- FGSP can't provide config sync, you may use FortiManager



This slide shows an active-active load balancing scenario. In this scenario, there are two load balancers: external load balancer and internal load balancer. There are also two FortiGates in the same availability set. The port1 interfaces on both FortiGate devices must be paired with the public external load balancer. The internet traffic first goes to the public load balancer. The public load balancer load balances the traffic to two FortiGates. Then the traffic goes to the internal load balancer, and finally to the VMs. Every cloud vendor has their own load balancing solutions.

DO NOT REPRINT
© FORTINET

FortiGate AutoScale with Azure VMSS and Load Balancer



© Fortinet Inc. All Rights Reserved.

42

This slide shows FortiGate auto scale with Azure. You can deploy FortiGate VMs to support Azure Autoscale. This requires a manual deployment incorporating one or more Virtual Machine Scale Sets (VMSS) and network related components, as well as Azure Function App scripts. Fortinet provides a FortiGate Autoscale for Azure deployment package to facilitate the deployment. Multiple FortiGate-VM instances form a VMSS to provide highly efficient clustering at times of high workloads. FortiGate-VM instances are scaled out automatically according to predefined workload levels. Autoscaling is achieved by using FortiGate-native high availability (HA) features such as config-sync, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events. In this scenario, a combination of two load balancers, load balance traffic, and Cosmos DB determines which FortiGate device is selected as the master. You will work with this scenario in a lab exercise.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand Azure basic concepts
- ✓ Understand Azure components, networking, and security
- ✓ Deploy FortiGate Fabric Connector for Azure
- ✓ Deploy FortiWeb on Azure
- ✓ Understand FortiGate native active-passive HA
- ✓ Deploy FortiGate active-active HA with Azure Load Balancer
- ✓ Deploy FortiGate autoscaling (VMSS, CosmosDB, FunctionApp)

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

By mastering the objectives covered in this lesson, you learned Azure basic concepts, networking, security, and how to use Fortinet solutions with Azure.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about the Fortinet solution for Google Cloud Platform (GCP).

**DO NOT REPRINT
© FORTINET**

GCP Fundamentals

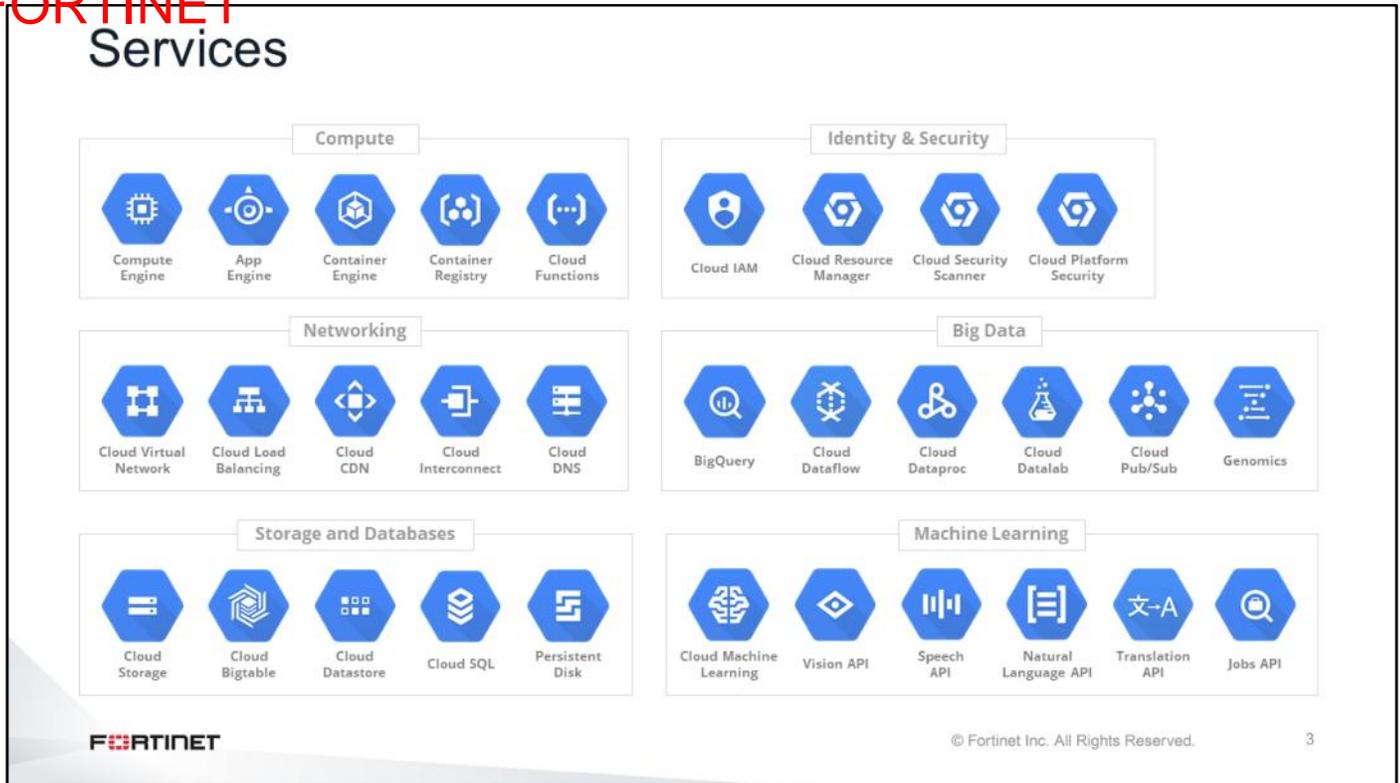
Objectives

- Understand basic concepts
- Understand components
- Understand networking
- Understand security

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

By demonstrating competence in GCP fundamentals, you will be able to understand GCP concepts and security.

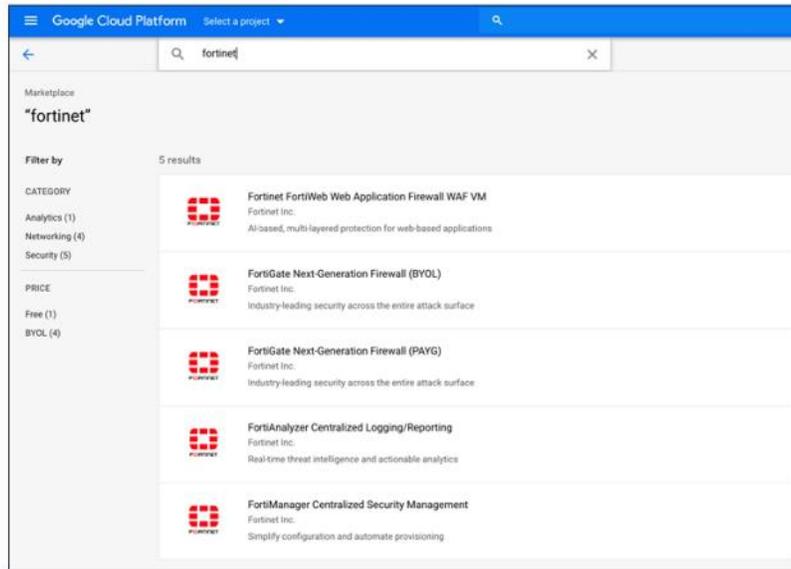
DO NOT REPRINT
© FORTINET



This slide shows GCP services. However, GCP offers fewer services than AWS and Azure. The machine learning section is the important part of GCP, and the reason why some customers use GCP instead of AWS or Azure.

DO NOT REPRINT
© FORTINET

Marketplace



FORTINET

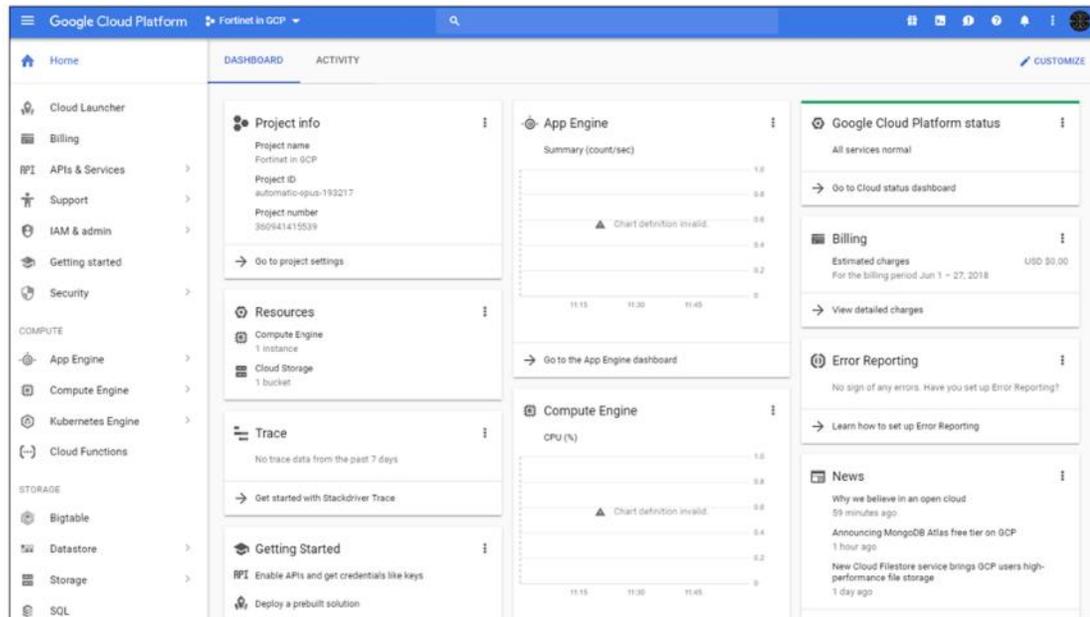
© Fortinet Inc. All Rights Reserved.

4

As shown on this slide, there are a limited number of Fortinet solutions that can be found in the GCP Marketplace.

DO NOT REPRINT
© FORTINET

Console



FORTINET

© Fortinet Inc. All Rights Reserved.

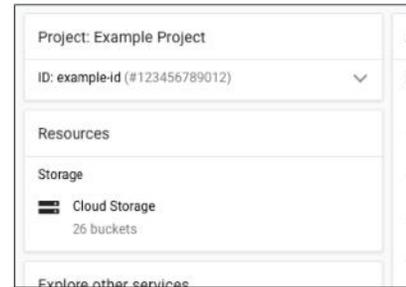
5

This is the Google Cloud Platform (GCP) Console, which is the web-based GUI used to manage GCP projects and resources. When you use the GCP Console, you create a new project or choose an existing project, and use the resources that you create in the context of that project. You can create multiple projects, so you can use projects to separate your work in whatever way makes sense for you. For example, you might start a new project if you want to make sure only certain team members can access the resources in that project, while all team members can continue to access resources in another project.

DO NOT REPRINT
© FORTINET

Projects

- A project is the organizing entity for what you're building
- Any GCP resources that you allocate and use must belong to a project
- Each project ID is unique across GCP
- Each GCP project has:
 - A project name, which you provide
 - A project ID, which you can provide or GCP can provide for you
 - A project number, which GCP provides
- As you work with GCP, you'll use these identifiers in specific command lines and API calls



- *Example Project* is the project name
- *example-id* is the project ID
- *123456789012* is the project number

FORTINET

© Fortinet Inc. All Rights Reserved.

6

Each project ID is unique across GCP. Once you create a project, you can delete the project, but its ID can never be used again. When billing is enabled, each project is associated with one billing account. Multiple projects can have their resource usage billed to the same account. A project serves as a namespace. This means every resource within each project must have a unique name, but you can usually reuse resource names if they are in separate projects. Some resource names must be globally unique. For more information, see the documentation for the resource.

A project is the organizing entity for what you're building. Any GCP resources that you allocate and use must belong to a project. A project is made up of the settings, permissions, and other metadata that describe your applications. Resources within a single project can work together easily—for example by communicating through an internal network, subject to the regions-and-zones rules. The resources that each project contains remain separate across project boundaries; you can only interconnect them through an external network connection.

Each GCP project has the following identifiers:

- A project name, which you provide
- A project ID, which you can provide or GCP can provide for you
- A project number, which GCP provides

As you work with GCP, you'll use these identifiers in certain command lines and API calls.

DO NOT REPRINT
© FORTINET

SDK

- Google Cloud SDK is developed in Python and used to manage the resources in your project
- It is available for Windows, Linux, Debian/Ubuntu, Red Hat/Centos, Mac OS X, and Windows
- Cloud SDK provides various CLI utilities to manage and interact with multiple services on GCP
- Three of the CLIs available in Cloud SDK are:
 - *gcloud* : CLI utility to interact with all other services on GCP
 - *gsutil* : CLI utility to interact with Google Cloud Storage
 - *bq* : CLI utility to interact with Google BigQuery



FORTINET

© Fortinet Inc. All Rights Reserved.

7

Google Cloud SDK is a set of tools for GCP. It contains *gcloud*, *gsutil*, and *bq* command line tools, which you can use to access Compute engine, Cloud Storage, BigQuery, and other products and services from the command line. You can run the tools interactively or in your automated scripts.

Cloud SDK is developed in Python and used to manage the resources in your project. It is available for Windows, Linux, Debian/Ubuntu, Red Hat/Centos, Mac OS X, and Windows. Cloud SDK provides various CLI utilities to manage and interact with multiple services on GCP. Python v2.7.9 (\$ `python -V` Python 2.7.13) is a prerequisite for installing Cloud SDK.

DO NOT REPRINT
© FORTINET

Infrastructure Details

- Live migration
 - Instances can be moved to nearby hosts while active
- Custom machine types
 - Let you configure the right combination of memory and virtual CPU
- Global load balancers that highly scale users instantly:
 - The same system that supports Google products, like Maps, Gmail, and Search

FORTINET

© Fortinet Inc. All Rights Reserved.

8

Live migration: Google Compute Engine instances can be moved to nearby hosts while active—even while under extreme load—complete with their working SSD storage (up to 1.5 TB). Since your VMs don't need to be rebooted for host software updates or other standard operational tasks, uptimes are superb. This ensures predictable performance across all the different parts of your application.

Custom machine types: These let you configure the right combination of memory and virtual CPU for your workload.

Global load balancers: A built-in load balancer is part of a worldwide distributed system for delivering customers to infrastructure, the same system that supports Google products, like Maps, Gmail, and Search.

DO NOT REPRINT
© FORTINET



As of 2019, GCP is available in multiple regions, zones, and network edge locations in more than two hundred countries and territories. However, this number is less than what AWS and Azure offer. A region is a specific geographical location where users can deploy cloud resources. Each region is an independent geographic area that consists of zones.

DO NOT REPRINT
© FORTINET

Global, Regional, and Zonal Resources

- Some resources can be accessed by any other resource, across regions and zones
 - These global resources include preconfigured disk images, disk snapshots, and networks
- Some resources can be accessed only by resources that are located in the same region
 - These regional resources include static external IP addresses
- Other resources can be accessed only by resources that are located in the same zone
 - These zonal resources include VM instances, their types, and disks

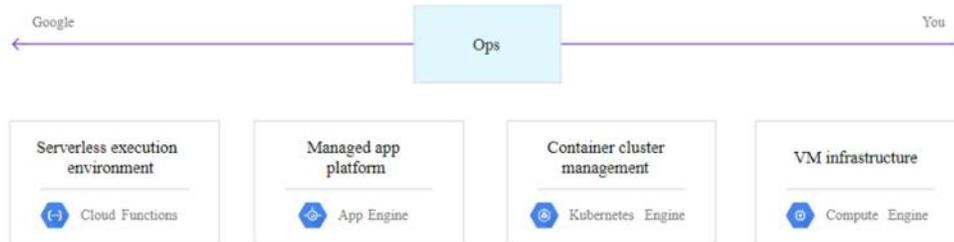


There are three main resources available in GCP, global, regional and zonal resources. For example, creating a network is a global operation, because a network is a global resource, while reserving an IP address is a regional operation, because the address is a regional resource. As you start to optimize your GCP, it's important to understand how these regions and zones interact. For example, even if you could, you wouldn't want to attach a disk in one region to a computer in a different region because the latency you'd introduce would make for very poor performance. Thankfully, GCP won't let you do this; disks can only be attached to computers in the same zone.

DO NOT REPRINT
© FORTINET

Computing and Hosting Services

- You can choose to:
 - Work in a serverless environment
 - Use a managed application platform
 - Leverage container technologies to gain lots of flexibility
 - Build your own cloud-based infrastructure to have the most control and flexibility



FORTINET

© Fortinet Inc. All Rights Reserved.

11

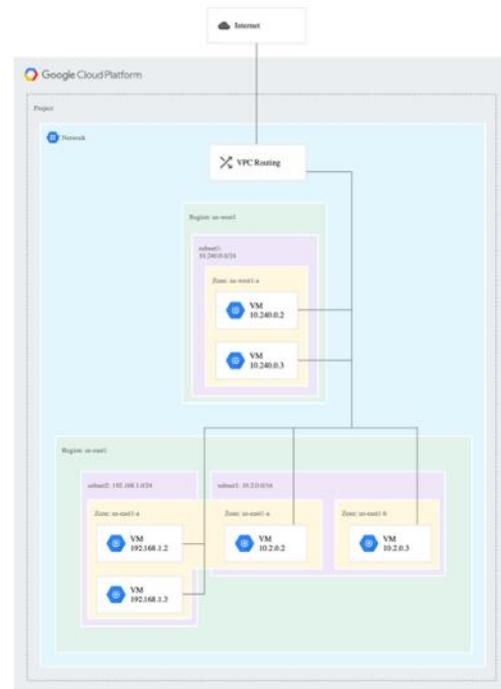
Virtual machines (VMs) are called Google Compute Engine in GCP. Also, there are other options, such as a serverless execution environment, which is equivalent to AWS Lambda or Azure functions. The following are some of the benefits:

- Work in a serverless environment
- Use a managed application platform
- Leverage container technologies to gain lots of flexibility
- Build your own cloud-based infrastructure to have the most control and flexibility

DO NOT REPRINT
© FORTINET

VPC

- VPC, subnets, and VMs
 - Each VM has a primary interface that connects to one subnet
 - The VM can optionally have multiple network interfaces, with each additional interface connecting to a different subnet in the same zone
 - Additional subnets can be created in your VPC, but subnets cannot be shared between projects
 - A route specifies how packets leaving a VM should be directed



© Fortinet Inc. All Rights Reserved.

12

VPCs are created per region within a project, similar to how Azure works. The difference here is that you can have a subnet that is spread across multiple availability zones. Each VM has a primary interface that connects to one subnet. The VM can optionally have multiple network interfaces, with each additional interface connecting to a different subnet in the same zone. Additional subnets can be created in your VPC, but subnets cannot be shared between projects. A route specifies how packets leaving a VM should be directed.

**DO NOT REPRINT
© FORTINET**

Google Cloud DNS

- Publish and maintain domain name system (DNS) records by using the same infrastructure that Google uses
- You can use the GCP Console, the command line, or a REST API to work with managed zones and DNS records

Google Cloud DNS is a global load balancing service that helps to publish and maintain DNS records by using the same infrastructure that Google uses. You can use the GCP console, the command line, or a REST API to work with managed zones and DNS records.

**DO NOT REPRINT
© FORTINET**

Load Balancers

- Global external load balancing
 - HTTP(S) load balancing
 - SSL proxy load balancing
 - TCP proxy load balancing
- Regional external load balancing
 - Distributes traffic among a pool of instances within a region
 - Network load balancing can balance any kind of TCP/UDP traffic
- Regional internal load balancing
 - Distributes traffic from GCP virtual machine instances to a group of instances in the same region

There are multiple load balancers in GCP. The global external load balancer can load balance Layer 7 traffic among regions such as HTTP, HTTPS, SSL proxy, and TCP proxy. The regional external load balancer distributes traffic among a pool of instances within a region. The regional internal load balancer distributes traffic from GCP VM instances to a group of instances in the same region. By default, all the GCP load balancers are denial of service (DoS) protected.

DO NOT REPRINT
© FORTINET

Connectivity

- Google Cloud Interconnect offers three options for advanced connectivity:
 - Carrier interconnect
 - Direct peering connection
 - Cloud VPN

If you have an existing network that you want to connect to GCP resources, Google Cloud Interconnect offers three options for advanced connectivity.

- **Carrier interconnect:** Connects your infrastructure to Google's network edge through highly available, lower-latency connections using service providers. You can also extend your private network into your private compute engine network over carrier interconnect links by using a VPN tunnel between the networks.
- **Direct peering connection:** Exchanges Internet traffic between your network and the Google network at one of Google's broad-reaching edge network locations.
- **Cloud VPN:** Connects your existing network to your compute engine network using an IPsec connection. You can use VPN to connect two compute engine VPN gateways to each other.

DO NOT REPRINT
© FORTINET

GCP Model

- Google Cloud Platform security is a shared responsibility model
- Google secures the compute or container engine from GCP
- Customer responsibility:
 - Keep the security for VM OS
 - Keep applications secure



GCP security models are the same as other vendors. It is a shared responsibility model between the vendor and the customer. Google secures the compute or container engine from GCP, and the customer is responsible for securing VM OS and applications.

DO NOT REPRINT
© FORTINET

Firewall

- Each VPC has its own firewall rules associated controlling access
- Firewall rules are enforced at the instance level
- GCP firewall rules can be modified through the Google Cloud Platform Console, gcloud command line tool, and REST API

Google Cloud Platform							
VPC network							
Firewall rules							
Ingress							
Name	Targets	Source filters	Protocols / ports	Action	Priority	Network	
default-allow-http	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default	
default-allow-https	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default	
default-allow-icmp	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default	

FORTINET

© Fortinet Inc. All Rights Reserved.

17

GCP firewall rules let you allow or deny traffic to and from your VM instances, based on a configuration you specify. Enabled GCP firewall rules are always enforced, protecting your instances regardless of their configuration and operating system, even if they have not started up. Each VPC has its own firewall rules. Controlling access and firewall rules are enforced at the instance level. GCP firewall rules can be modified through the GCP console, gcloud command line tool, and REST API. Firewall rules can be applied to the whole VPC, subnet, VM, and network interfaces.

**DO NOT REPRINT
© FORTINET**

Fortinet Solutions for GCP

Objectives

- Understand Fortinet on GCP Marketplace
- Understand FortiGate Fabric Connector for GCP

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

By demonstrating competence in Fortinet solutions for GCP, you will be able to successfully deploy and use Fortinet products in GCP.

DO NOT REPRINT
© FORTINET

Fortinet Products in GCP Marketplace

Product	Licensing Model	Available in GCP Marketplace
FortiGate	BYOL	Yes
FortiGate	PAYG	Yes
FortiWeb	BYOL	Yes
FortiWeb	PAYG	No
FortiWeb Manager	BYOL	No
FortiSandbox	BYOL	No
FortiSandbox	PAYG	No
FortiMail	BYOL	No
FortiSIEM	BYOL	No
FortiManager	BYOL	Yes
FortiAnalyzer	BYOL	Yes
FortiAnalyzer	PAYG	No
FortiVoice	BYOL	No
FortiAuthenticator	BYOL	No
FortiRecorder	PAYG	No

FORTINET

© Fortinet Inc. All Rights Reserved.

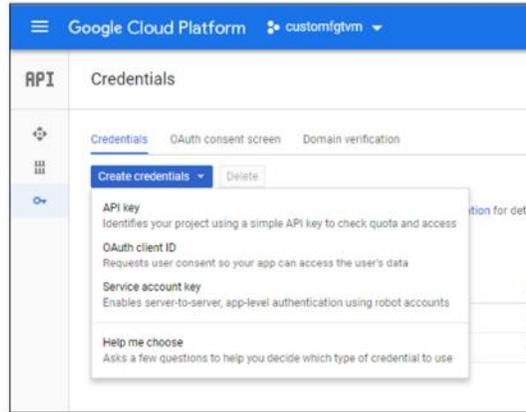
19

As shown on this slide, there are Fortinet solutions in GCP Marketplace. For now, the available Fortinet solutions are FortiGate, FortiWeb, FortiManager, and FortiAnalyzer.

DO NOT REPRINT
© FORTINET

SDN Connector for GCP

- Click **API & Services, Credentials**
- Click **Create credentials, Service account key**



You can access SDN connector for GCP under API and services and then create credentials.

DO NOT REPRINT
© FORTINET

SDN Connector for GCP (Contd)

- In the **Service account** menu, select **New service account**
- Edit the account name
- Select **JSON** for the key type
- Select **Create**

Google Cloud Platform customfgtvm

Create service account key

Service account
New service account

Service account name fortiosconnector Role Editor

Service account ID
fortiosconnector@customfgtvm.iam.gserviceaccount.com

Key type
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.
 JSON Recommended
 P12
For backward compatibility with code using the P12 format

Create Cancel

FORTINET

© Fortinet Inc. All Rights Reserved.

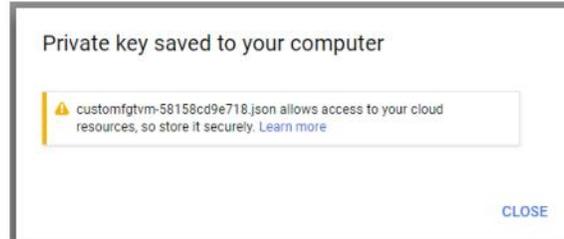
21

As shown on this slide, you can create a user and specify what type of key type that you would use.

**DO NOT REPRINT
© FORTINET**

SDN Connector for GCP (Contd)

- Once created, a file will be downloaded to your PC, and the following message will be displayed:



As shown on this slide, a file will be downloaded to your PC, and this is the private key.

DO NOT REPRINT
© FORTINET

SDN Connector for GCP (Contd)

- Open the downloaded file in a text editor to extract the connector parameters, such as `project_id`, `service_account`, and `private_key`

```
{
  "type": "service_account",
  "project_id": "customfgtvm",
  "private_key_id": "50158cd9e718d39879752ce5022fe9c07b602fe5",
  "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKowggSjAgEAAoIBAQDP6DQI10hMYnfo\nnpIT3spb/LQ1tDOXXpyzt/\n"client_email": "fortiosconnector@customfgtvm.iam.gserviceaccount.com",
  "client_id": "105042549935615524212",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/fortiosconnector%40customfgtvm.iam.gserviceaccount.com"
}
```

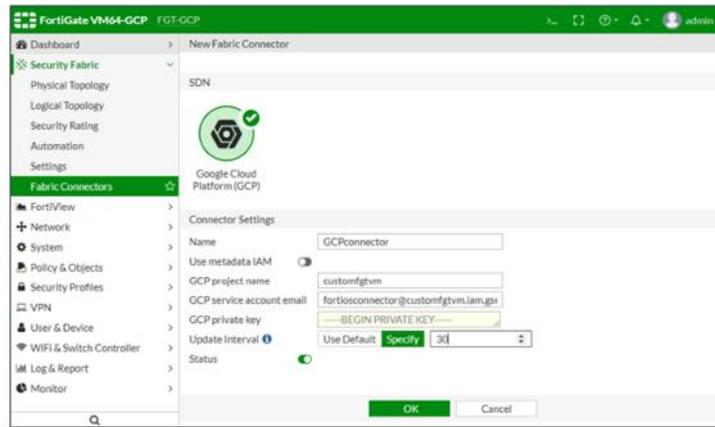
- Arrange the `private_key`, eliminating the symbols `\n` from the string

Once you open the file that you previously downloaded, in a text editor, you will see all connector parameters that are necessary for setting up the FortiGate public connector. You will need to extract the connector parameters such as project id, service account and private key.

DO NOT REPRINT
© FORTINET

SDN Connector for GCP (Contd)

- In the GCP connector configuration, edit the **GCP project name**, **GCP service account email**, and **GCP private key** fields with the data that you obtained from the JSON file, and click **OK**



FORTINET

© Fortinet Inc. All Rights Reserved.

24

To configure the Fabric Connectors on FortiGate, in the GCP connector configuration, edit the **GCP project name**, **GCP service account email**, and **GCP private key** fields with the data that you obtained from the JSON file, and click **OK**.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand basic concepts
- ✓ Understand components
- ✓ Understand networking
- ✓ Understand security
- ✓ Understand Fortinet products on GCP Marketplace
- ✓ Understand FortiGate Fabric Connector for GCP

This slide shows the objectives covered in this lesson. By mastering the objectives covered in this lesson, you learned GCP basic concepts, components, networking, security, Marketplace and FortiGate Fabric Connectors.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about public cloud security with FortiCWP and FortiCASB.

**DO NOT REPRINT
© FORTINET**

FortiCWP

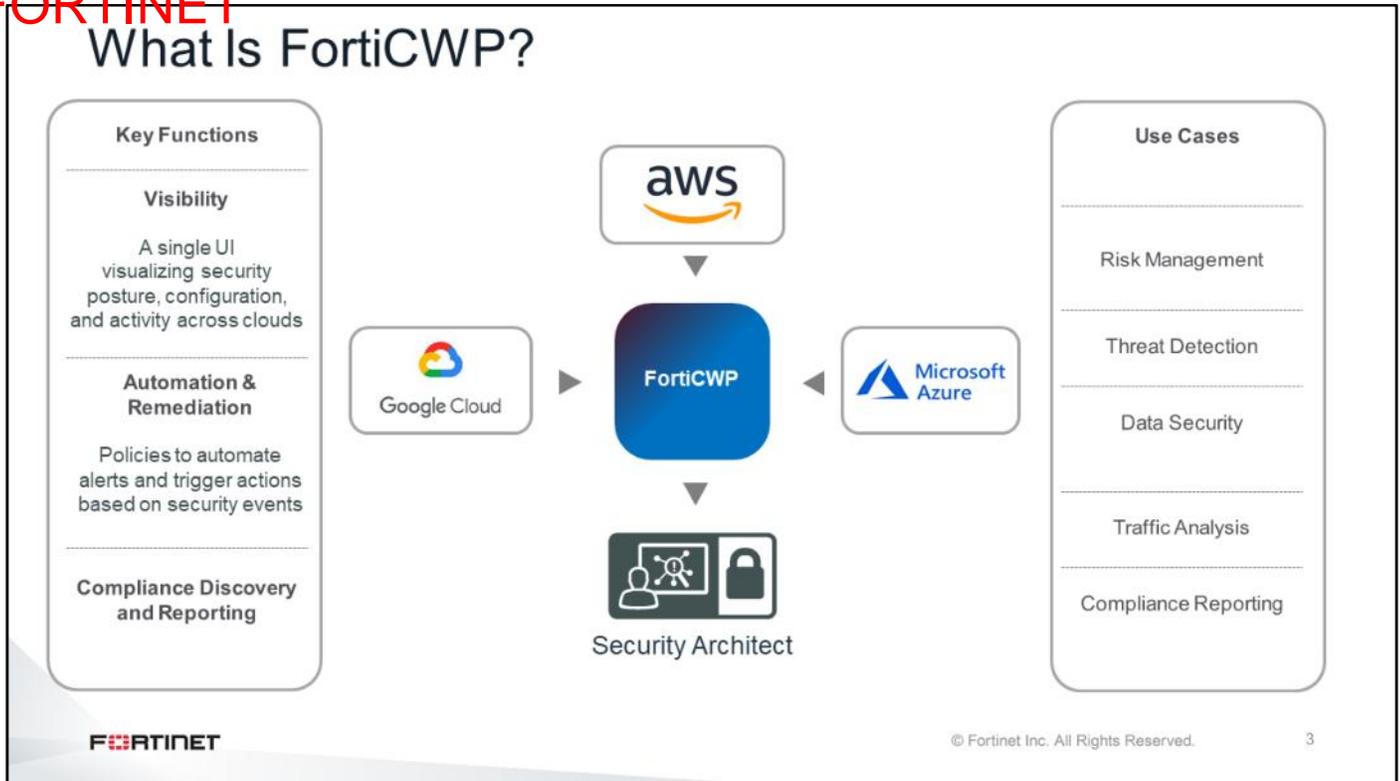
Objectives

- Understand FortiCWP architecture
- Understand FortiCWP supported vendors

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

By demonstrating competence in FortiCWP, you will be able to successfully use it to secure your public cloud.

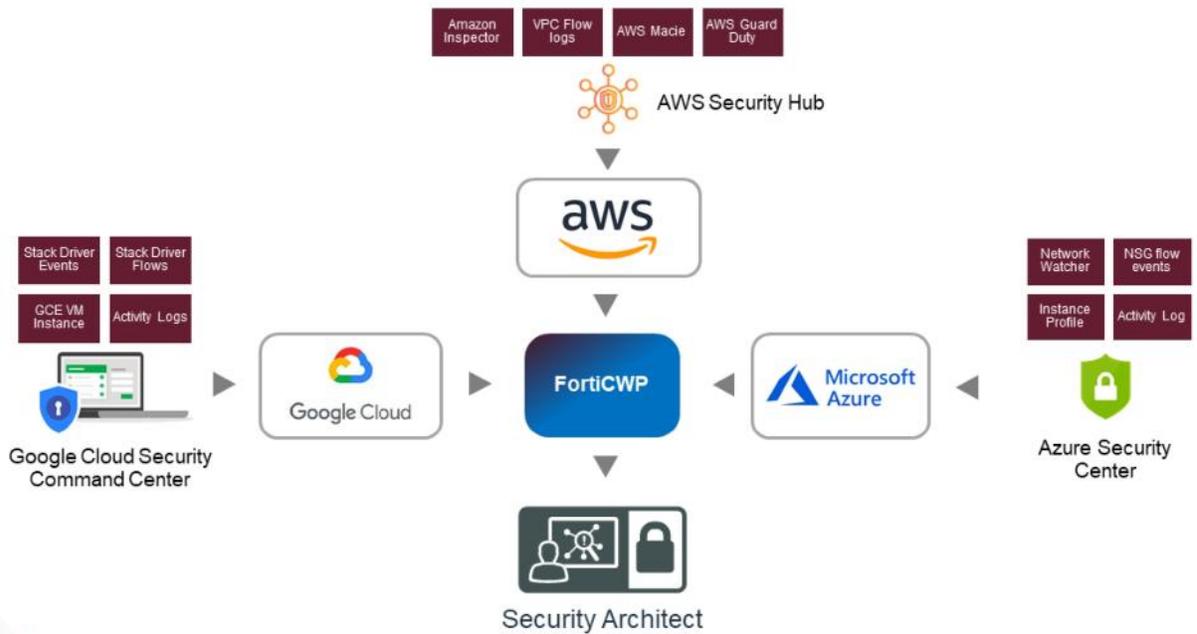
DO NOT REPRINT
© FORTINET



A cloud workload protection (CWP) solution addresses the unique security requirements of infrastructure management in modern multicloud environments. FortiCWP can access the cloud vendor's management console information directly through APIs. Organizations that use FortiCWP can get visibility, achieve compliance, and remediate security risks for their IaaS environments. FortiCWP is a cloud-based service and supports Google Cloud, Amazon Web Services, and Microsoft Azure. The main use cases for FortiCWP are risk management, threat detection, data security, traffic analysis, and compliance reporting.

DO NOT REPRINT
© FORTINET

How Does FortiCWP Interact With the Cloud?

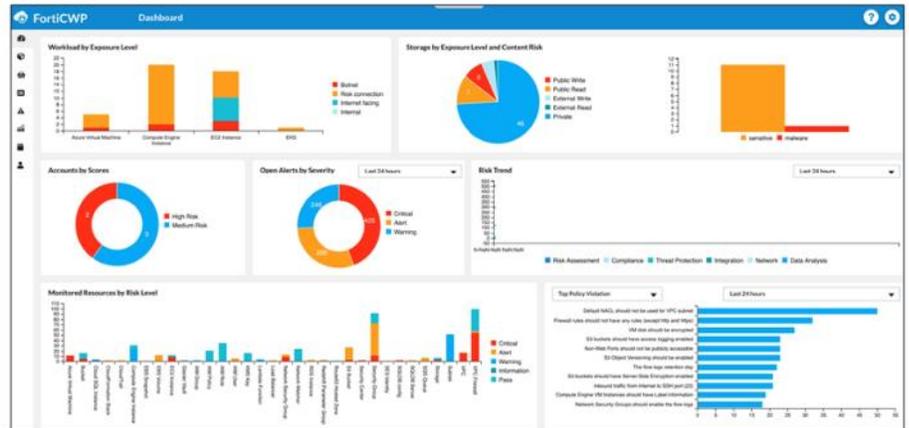


FortiCWP uses each cloud-vendor-specific API to gather information from their different native security features, allowing for risk management of multi cloud environments using a single console. So, security operations teams can perform automated evaluation of their company security posture in large multi cloud environments from the FortiCWP dashboard, instead of going through each account and vendor's native security tools manually.

DO NOT REPRINT
© FORTINET

FortiCWP GUI

- Web-based management portal
- Controls for each supported IaaS vendor
- Dashboards help quickly identify risks
- Advanced reporting and metrics
- Simplified, *up in minutes* implementation



FORTINET

© Fortinet Inc. All Rights Reserved.

5

FortiCWP's intuitive and modern user interface is both easy to use and informative. Administrators log in to the web-based portal and then navigate to the controls and dashboards for each IaaS vendor. Risks are called to the user's attention through the dashboards, and advanced reporting tools provide in-depth information about the event or user. Using the predefined default policies, organizations can be *up in minutes* and then can tailor settings, as desired, over time. This slide shows an example of an IaaS risk dashboard. It shows an assessment of configuration violations across cloud accounts, provides instant visibility into workloads with higher risk, and gives easy drill-down to troubleshoot and gain actionable information.

**DO NOT REPRINT
© FORTINET**

FortiCASB

Objectives

- Understand FortiCASB architecture
- Understand FortiCASB supported applications

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

By demonstrating competence in FortiCASB, you will be able to successfully use it to secure your public cloud.

DO NOT REPRINT
© FORTINET

FortiCASB–Cloud Access Security Broker



- **Enforcement service extended to sanctioned SaaS**
 - Identifies sensitive data and files
 - Extends policies for access and shares
 - Reports on access and usage
- **Protects from cloud-borne threats**
 - Virus and malware propagation
 - Deliberate or accidental distribution of sensitive data
- **Provides compliance and audit tools for SaaS**
 - SOX, PCI, HIPAA, and so on
- Hosted or on-premises solutions
- API, forward proxy, and reverse proxy deployment types

FORTINET

© Fortinet Inc. All Rights Reserved.

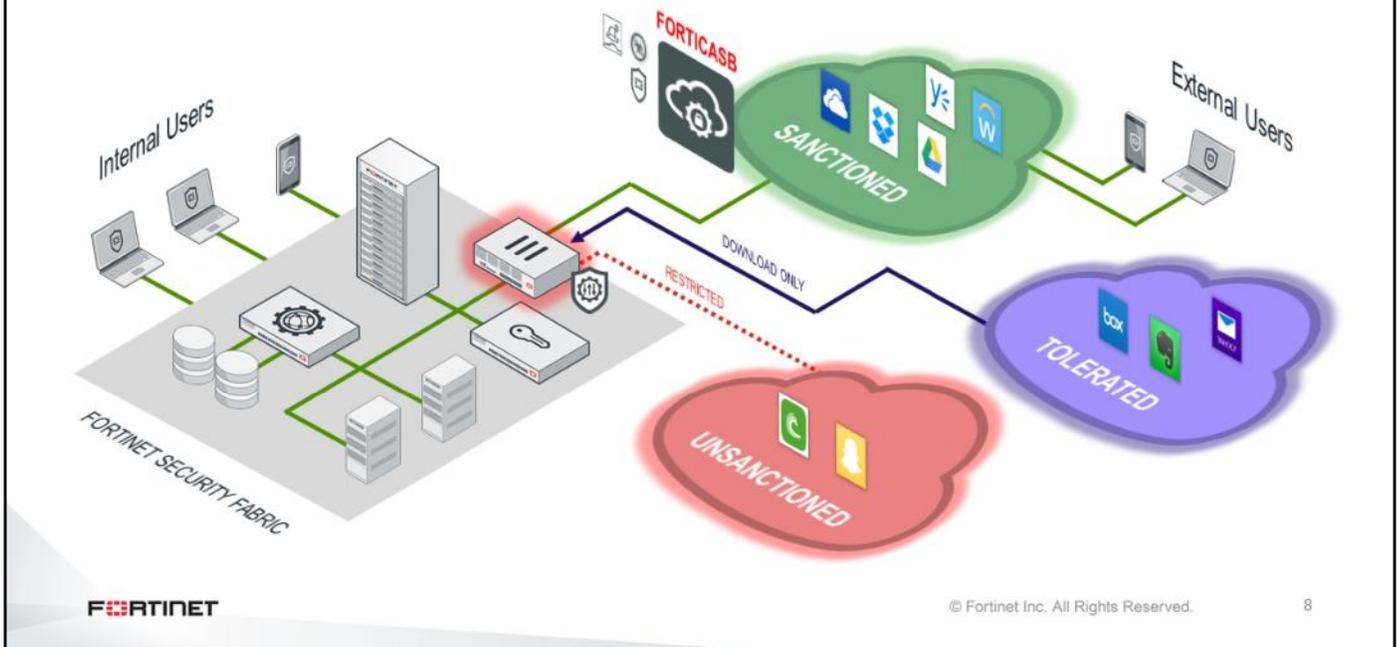
7

Cloud access security brokers (CASBs), in general, are on-premises or cloud-based security policy enforcement points. CASBs are placed between cloud service users and providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. For example, security policies include authentication; single sign-on; authorization; credential mapping; device profiling; data security (content inspection, encryption, tokenization); logging; alerting; and malware detection and prevention.

FortiCASB is Fortinet's cloud-native CASB service that provides visibility, compliance, data security, and threat protection for cloud-based services. Using direct API access to cloud vendors, FortiCASB enables deep inspection and policy management for data stored in SaaS applications. FortiCASB also provides advanced tools that provide detailed user analytics and management tools to ensure policies are enforced, and your organization's data is not getting into the wrong hands.

DO NOT REPRINT
© FORTINET

FortiCASB Solution Overview



Organizations are increasingly adopting software-as-a-service (SaaS) applications for the agility and savings they offer, but find that they don't provide the required visibility and control. FortiCASB is a cloud-native CASB subscription service that is designed to provide visibility, compliance, data security, and threat protection for cloud-based services being used by an organization.

As shown on this slide, FortiCASB can be used as a monitoring and access tool for sanctioned applications by FortiClient or FortiGate application control. Based on the example shown on the slide, applications like Dropbox and One Drive are allowed by application control, but FortiCASB can be used to further inspect specific user actions through the APIs of those providers. Other applications that can't be monitored by FortiCASB and are restricted, can then be blocked with application control.

DO NOT REPRINT
© FORTINET

FortiCASB Extends Application Control




FEATURE	FORTICASB	FORTIOS APP CTRL
SaaS Discovery		Inline
SaaS DLP	Yes	Inline
SaaS Access Control and Policies	Yes	Inline
Policy scanning for stored SaaS data	Yes	
SaaS Access	Direct to Cloud	Inline Proxy
Mobile Direct Access to Cloud	Yes	
SaaS Visibility	Sanctioned Apps	Inline
SaaS Threat scanning	Stored in Cloud	Inline
Manage Tolerated Applications		Yes
Manage Blocked Applications		Yes
Consolidated SaaS Reporting	Sanctioned-only	Limited
Compliance	Sanctioned-only	Yes
Integration	LDAP	IdP, SSO, LDAP

FORTINET

© Fortinet Inc. All Rights Reserved.

9

FortiGate and FortiClient application control provides support for fine-grained control on popular cloud applications, such as YouTube, Dropbox, Baidu, and Amazon. However, in order to have application control protection, traffic must flow through these devices. At the same time, devices with application control cannot inspect the specific user actions within that application, due to hardcoded SSL certificates on their endpoint clients.

The FortiCASB can inspect the user actions of supported applications no matter where the user is, or if those action are being inspected by a FortiGate, because it connects directly to the SaaS provider through the API. By combining FortiCASB and application control, the customer can have the most complete control and inspection of SaaS.

DO NOT REPRINT
© FORTINET

FortiCASB GUI

- Web-based management portal
- Controls for each supported SaaS application
- Dashboards help quickly identify risks
- Advanced reporting and metrics
- Simplified, *up in minutes* implementation



FORTINET

© Fortinet Inc. All Rights Reserved.

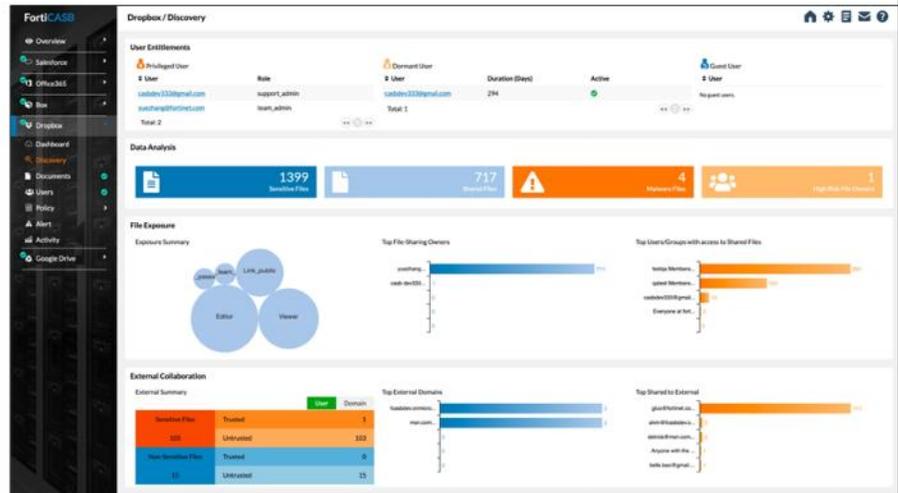
10

FortiCASB's intuitive and modern user interface is both easy to use and informative. Administrators log in to the web-based portal and then navigate to the controls and dashboards for each SaaS application. Risks are called to the user's attention through the dashboards, and advanced reporting tools provide in-depth information about the event or user. Using the predefined default policies, organizations can be *up in minutes*, and then can tailor settings, as desired, over time.

DO NOT REPRINT
© FORTINET

SaaS Applications

- DLP scanning
- Malware analysis with AV scanning and sandbox integration
- Document and user usage and permissions analysis
- Visibility and control into file collaboration
- Threat protection policies, suspicious activity—who, when, where
- Much more



FORTINET

© Fortinet Inc. All Rights Reserved.

11

This slide shows an example of a Dropbox account scanned by the FortiCASB. It shows how many files have been scanned and if FortiCASB found any issues.

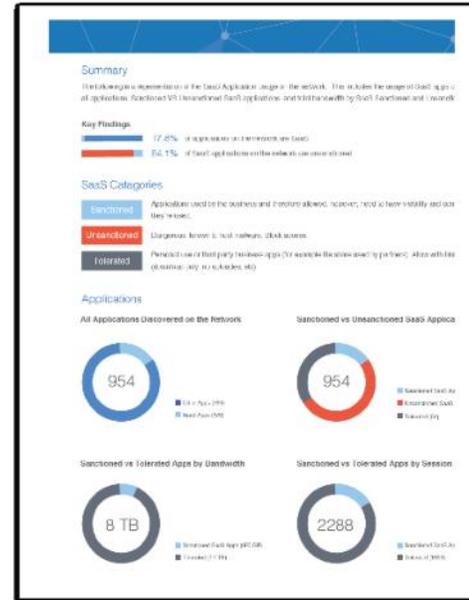
FortiCASB's main features are:

- DLP scanning
- Malware analysis with AV scanning and sandbox integration
- Document and user usage and permissions analysis
- Visibility and control into file collaboration
- Threat protection policies, suspicious activity—who, when, where

DO NOT REPRINT
© FORTINET

SaaS Reporting

- **Sanctioned** apps reported through FortiCASB
- **Tolerated** apps reported through FortiAnalyzer with FortiGate
- **Blocked** apps managed by FortiGate
- Consolidated reporting with FortiAnalyzer
 - Available in future update at no extra cost



12

For compliance purposes, you can use FortiAnalyzer to run a report based on FortiCASB, FortiClient, and FortiGate logs. It will give a report based on consolidated logs for sanctioned applications reported through FortiCASB, tolerated applications, and blocked applications reported through FortiGate and FortiClient logs.

DO NOT REPRINT
© FORTINET

Compliance Reporting

- HIPAA Compliance Report
- PCI Compliance Report
- SOX/COBIT Compliance Report
- GDPR Compliance Report
- ISO 27001
- NIST 800/53 US Federal controls
- NIST 800/171 US Non-Federal controls



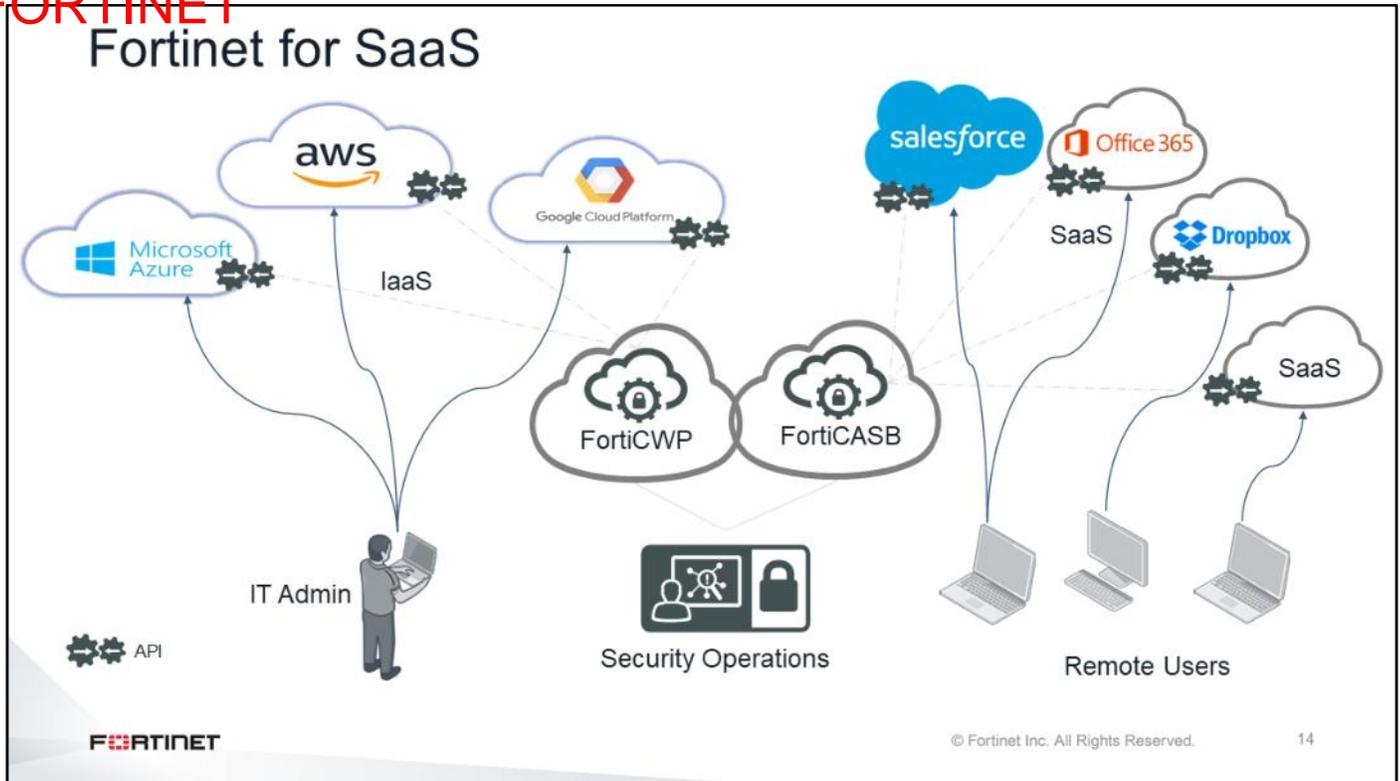
FORTINET

© Fortinet Inc. All Rights Reserved.

13

Organizations are subject to a number of regulatory and standards compliance requirements. For example, payment card industry data security standard (PCI DSS) affects only organizations that do credit card transactions. However, the European Union's general data protection regulation (GDPR), affects every organization with European customers that collects personal data. There are also regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), that affects multiple industries (healthcare, academic, insurance, government entities, and more). Regardless of its reach, Fortinet is committed to ensuring that our products help customers demonstrate compliance with applicable regulatory statutes, as well as internal compliance initiatives.

DO NOT REPRINT
© FORTINET



In summary, FortiCWP secures public cloud infrastructures from unwanted use through the cloud management platform, by connecting directly to cloud infrastructure providers using APIs. FortiCASB secures organizations from improper SaaS usage by directly connecting to the sanctioned applications using APIs, to protect data and manage users in near real time.

As shown in the diagram on this slide, remote users are not behind FortiGate; however, their usage of these applications is equally protected by Fortinet, because these are cloud-based services.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand FortiCWP architecture
- ✓ Understand FortiCWP supported vendors
- ✓ Understand FortiCASB architecture
- ✓ Understand FortiCASB supported applications

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned about public cloud security with FortiCWP and FortiCASB.

DO NOT REPRINT
© FORTINET



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© 2020 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.