

DO NOT REPRINT
© FORTINET

FORTINET
Network
Security
Expert

4

FortiGate Security Study Guide

for FortiOS 6.4



DO NOT REPRINT

© FORTINET

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Network Security Expert Program (NSE)

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Feedback

Email: courseware@fortinet.com



TABLE OF CONTENTS

01 Introduction and Initial Configuration.....	4
02 Security Fabric.....	56
03 Firewall Policies.....	96
04 Network Address Translation (NAT).....	142
05 Firewall Authentication.....	195
06 Logging and Monitoring.....	252
07 Certificate Operations.....	310
08 Web Filtering.....	360
09 Application Control.....	420
10 Antivirus.....	465
11 Intrusion Prevention and Denial of Service.....	514
12 SSL-VPN.....	565

DO NOT REPRINT**© FORTINET****FORTINET**

FortiGate Security

Introduction and Initial Configuration

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.Last Modified 29 May 2020

In this lesson, you will learn about FortiGate administration basics and the components within FortiGate that can be enabled to extend functionality. This lesson also includes details about how and where FortiGate fits into your existing network architecture.

DO NOT REPRINT**© FORTINET**

Lesson Overview



High-Level Features

Setup Decisions

Basic Administration

Built-In Servers

Fundamental Maintenance

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

DO NOT REPRINT**© FORTINET**

High-Level Features

Objectives

- Identify platform design features of FortiGate
- Identify features of FortiGate in virtualized networks and the cloud
- Understand FortiGate security processing units (SPU)

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

By demonstrating competence in identifying the platform design features of FortiGate, features of FortiGate in virtualized networks and the cloud, as well as the FortiGate security processing units, you will be able to describe the fundamental components of FortiGate and explain the types of tasks that FortiGate can do.

DO NOT REPRINT**© FORTINET**

The Modern Context of Network Security

- Firewalls are more than gatekeepers on the network perimeter
- Today's firewalls are designed in response to multi-faceted and multi-device environments with no identifiable perimeter:
 - Mobile workforce
 - Partners accessing your network services
 - Public and private clouds
 - Internet of things (IoT)
 - Bring your own device (BYOD)
- Firewalls are expected to perform different functions within a network
 - Different deployment modes:
 - Distributed enterprise firewall
 - Next-generation firewall
 - Internal segmentation firewall
 - Data center firewall
 - DNS, DHCP, web filter, intrusion prevention system (IPS), and so on



© Fortinet Inc. All Rights Reserved.

4

In the past, the common way of protecting a network was securing the perimeter and installing a firewall at the entry point. Network administrators used to trust everything and everyone inside the perimeter.

Now, malware can easily bypass any entry-point firewall and get inside the network. This could happen through an infected USB stick, or an employee's compromised personal device being connected to the corporate network. Additionally, because attacks can come from inside the network, network administrators can no longer inherently trust internal users and devices.

What's more, today's networks are highly complex environments whose borders are constantly changing. Networks run vertically from the LAN to the Internet, and horizontally from the physical network to a private virtual network and to the cloud. A mobile and diverse workforce (employees, partners, and customers) accessing network resources, public and private clouds, the Internet of Things (IoT), and bring-your-own-device programs all conspire to increase the number of attack vectors against your network.

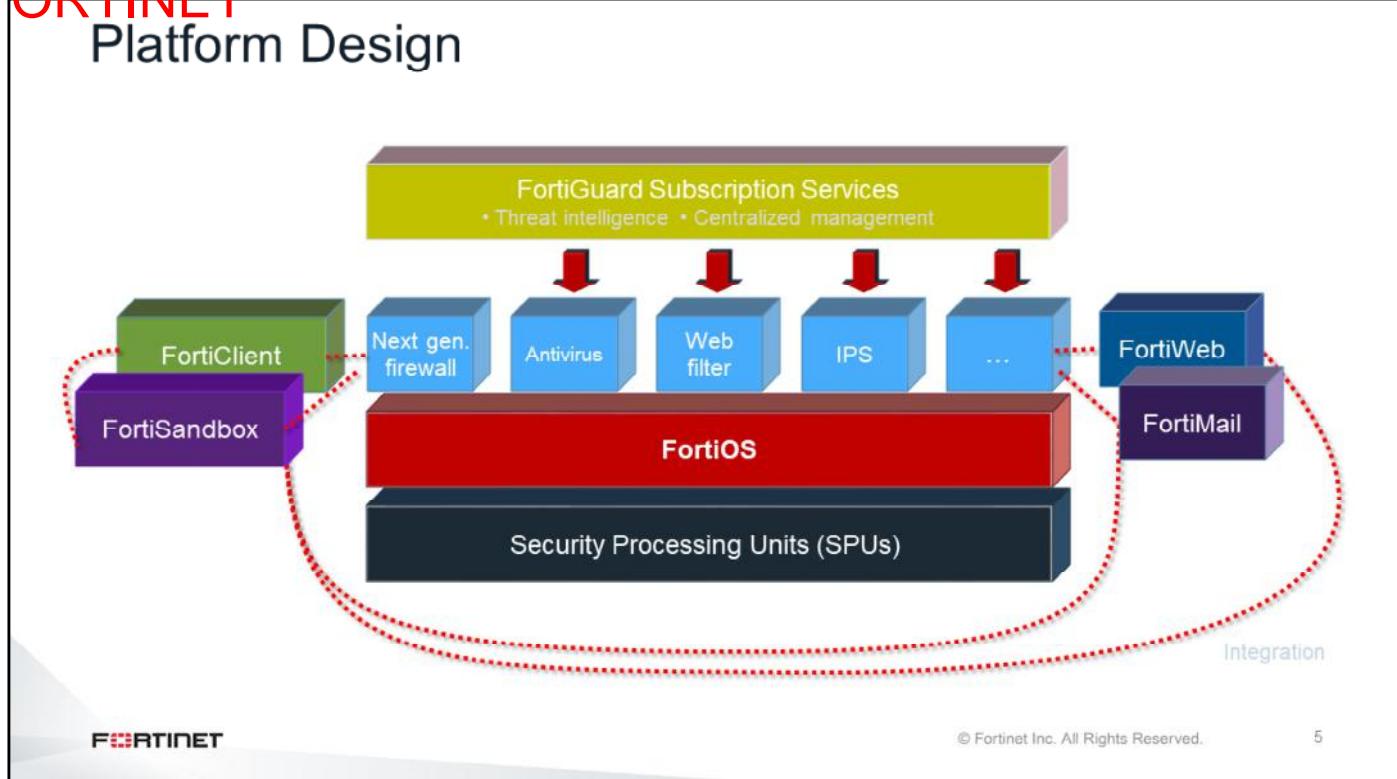
In response to this highly complex environment, firewalls have become robust multi-functional devices that counter an array of threats to your network. Thus, FortiGate can act in different modes or roles to address different requirements. For example, FortiGate can be deployed as a data center firewall whose function is to monitor inbound requests to servers and to protect them without increasing latency for the requester. Or, FortiGate can be deployed as an internal segmentation firewall as a means to contain a network breach.

FortiGate can also function as DNS and DHCP servers, and be configured to provide web filter, anti-virus, and IPS services.

DO NOT REPRINT

© FORTINET

Platform Design



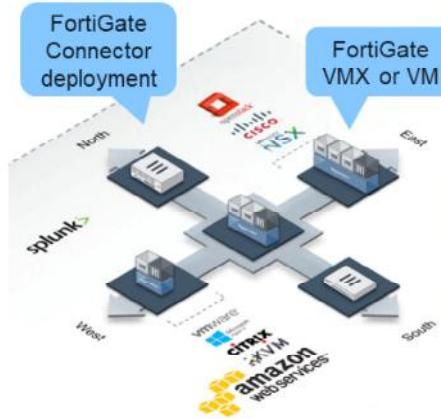
In the architecture diagram shown on this slide, you can see how FortiGate platforms add strength, without compromising flexibility. Like separate, dedicated security devices, FortiGate is still *internally* modular. Plus:

- **Devices add duplication.** Sometimes, dedication *doesn't* mean efficiency. If it's overloaded, can one device borrow free RAM from nine others? Do you want to configure policies, logging, and routing on 10 separate devices? Does 10 times the duplication bring you 10 times the benefit, or is it a hassle? For smaller to midsize businesses or enterprise branch offices, unified threat management (UTM) is often a superior solution, compared to separate dedicated appliances.
- **FortiGate hardware isn't just off-the-shelf.** It's carrier-grade. Most FortiGate models have one or more specialized circuits, called ASICs, that are engineered by Fortinet. For example, a CP or NP chip handles cryptography and packet forwarding more efficiently. Compared to a single-purpose device with only a CPU, FortiGate can have dramatically better performance. This is especially critical for data centers and carriers where throughput is business critical.
(The exception? Virtualization platforms—VMware, Citrix Xen, Microsoft, or Oracle Virtual Box—have general-purpose vCPUs. But, virtualization might be worthwhile because of other benefits, such as distributed computing and cloud-based security.)
- **FortiGate is flexible.** If all you need is fast firewalling and antivirus, FortiGate won't require you to waste CPU, RAM, and electricity on other features. In each firewall policy, UTM and next-generation firewall modules can be enabled or disabled. Also, you won't pay more to add VPN seat licenses later.
- **FortiGate cooperates.** A preference for open standards instead of proprietary protocols means less vendor lock-in and more choice for system integrators. And, as your network grows, FortiGate can leverage other Fortinet products such as FortiSandbox and FortiWeb to distribute processing for deeper security and optimal performance—a total Security Fabric approach.

DO NOT REPRINT**© FORTINET**

Topology in the Cloud

- Deploy FortiGate in **virtualized networks**
 - **FortiGate VM** – Same features as physical appliance except SPUs
 - **FortiGate VMX** – Subset of features for VMware NSX (east-west) data flows
 - **FortiGate Connector for Cisco ACI** – Subset for Cisco ACI (north-south) data flows. Integrates physical or virtual appliance.



FortiGate VM Specifications

Licenses	Max. 1 / 2 / 4 / 8 vCPU
Hypervisor	VMware, Hyper-V, KVM, Citrix Xen Server, Open Source Xen, Azure, Amazon AWS BYOL & on-demand
Memory	Max. 1/4/8/12 GB
10/100/1000 Interfaces	2-4 virtual NICs
Storage Capacity	40+ GB

- **Faster setup and teardown: SDN + VMs**

© Fortinet Inc. All Rights Reserved.

6

FortiGate virtual machines (VMs) have the same features as physical FortiGates, except for hardware acceleration. Why? First, the hardware abstraction layer software for hypervisors is made by VMware, Xen, and other hypervisor manufacturers, *not* by Fortinet. Those other manufacturers don't make Fortinet's proprietary SPU chips. But there is another reason, too. The purpose of generic virtual CPUs and other virtual chips for hypervisors is to abstract the hardware details. That way, all VM guest OSs can run on a common platform, no matter the different hardware on which the hypervisors are installed. Unlike vCPUs or vGPUs that use generic, *non-optimal* RAM and vCPUs for abstraction, SPU chips are specialized *optimized* circuits. Therefore, a virtualized ASIC chip would not have the same performance benefits as a physical SPU chip.

If performance on equivalent hardware is less, you may wonder, why would anyone use a FortiGate VM? In large-scale networks that change rapidly and may have many tenants, equivalent processing power and distribution may be achievable using larger amounts of cheaper, general purpose hardware. Also, trading some performance for other benefits may be worth it. You can benefit from faster network and appliance deployment and teardown.

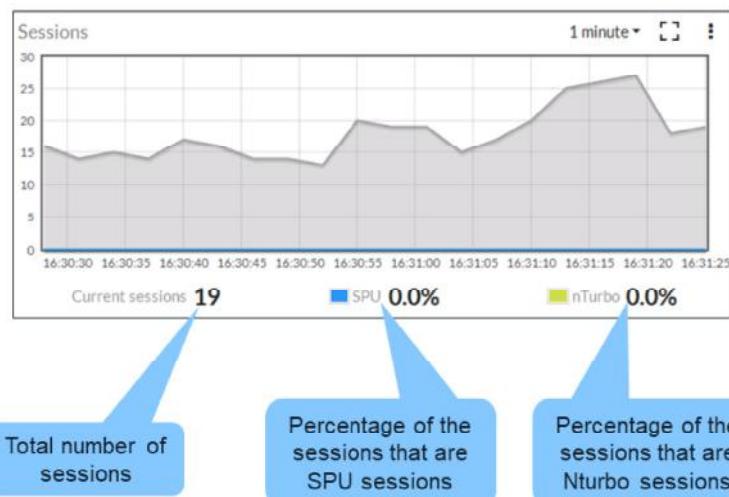
FortiGate VMX and the FortiGate Connector for Cisco ACI are specialized versions of FortiOS and an API that allows you to orchestrate rapid network changes through standards, such as OpenStack for software-defined networking (SDN).

- FortiGate VM is deployed as a guest VM on the hypervisor.
- FortiGate VMX is deployed inside a hypervisor's virtual networks, *between* guest VMs.
- FortiGate Connector for Cisco ACI allows ACI to deploy physical or virtual FortiGate VMs for north-south traffic.

DO NOT REPRINT

© FORTINET SPUs

- Hardware acceleration offload resource intensive processing from CPU
- Processors involved:
 - Content processors (CPs)
 - Security processors (SPs)
 - Network processors (NPs)
- Offloaded NP7 and NP6 sessions can be viewed by enabling per-session accounting



FORTINET

© Fortinet Inc. All Rights Reserved.

7

All Fortinet hardware acceleration hardware has been renamed security processing units (SPUs). This includes NPx and CPx processors.

Most FortiGate models have specialized acceleration hardware, called SPUs that can offload resource intensive processing from main processing (CPU) resources. Most FortiGate devices include specialized content processors (CPs) that accelerate a wide range of important security processes such as virus scanning, attack detection, encryption and decryption. (Only selected entry-level FortiGate models do not include a CP processor.) Many FortiGate models also contain security processors (SPs) that accelerate processing for specific security features such as IPS and network processors (NPs) that offload processing of high volume network traffic.

SPU and nTurbo data is now visible in a number of places on the GUI. For example, the Active Sessions column pop-up in the firewall policy list and the Sessions dashboard widget. Per-session accounting is a logging feature that allows the FortiGate to report the correct bytes/pkt numbers per session for sessions offloaded to an NP7, NP6 or NP6lite processor.

The following example shows the **Sessions** dashboard widget tracking SPU and nTurbo sessions. **Current sessions** shows the total number of sessions, **SPU** shows the percentage of these sessions that are SPU sessions and **Nturbo** shows the percentage that are nTurbo sessions.

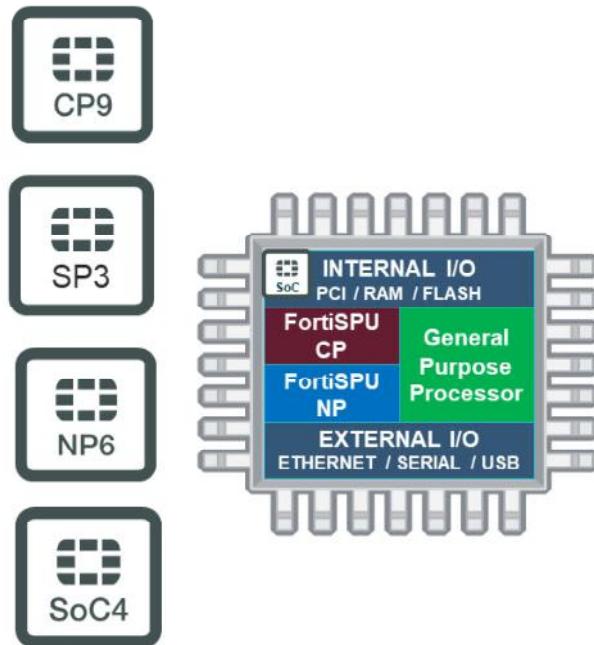
NTurbo offloads firewall sessions that include flow-based security profiles to NP6 or NP7 network processors. Without NTurbo, or with NTurbo disabled, all firewall sessions that include flow-based security profiles are processed by the FortiGate CPU.

DO NOT REPRINT

© FORTINET

SPUs (Contd)

- Content Processor
 - High-speed content inspection
 - Not bound to interface, closer to applications
 - Encryption and decryption (SSL)
 - Antivirus
- Security Processor
 - Directly attached to network interfaces
 - Increase system performance by accelerating IPS
- Network Processor
 - Packet Processing
 - NP6 provided NTurbo
 - Directly attached to network interface
- System-on-a-Chip Processor
 - Optimized performance for entry level
 - SoC4 platforms Include NTurbo



FORTINET

© Fortinet Inc. All Rights Reserved.

8

Fortinet's content processor (CP9) works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services. This frees businesses to deploy advanced security whenever it is needed without impacting network functionality. CP8 and CP9 provide a fast path for traffic inspected by IPS, including sessions with flow-based inspection.

CP processors also accelerate intensive proxy-based tasks:

- Encryption and decryption (SSL)
- Antivirus

FortiGate security processing (SP) modules, such as the SP3 but also including the XLP, XG2, XE2, FE8, and CE4, work at both the interface and system level to increase overall system performance by accelerating specialized security processing. You can configure the SP to favor IPS over firewall processing in hostile high-traffic environments.

FortiSPU network processors work at the interface level to accelerate traffic by offloading traffic from the main CPU. Models which support FortiOS 6.4 contain NP6, NP6lite, and NP7 network processors.

Fortinet integrates content and network processors along with RISC-based CPU into a single processor known as SoC4 for entry-level FortiGate security appliances used for distributed enterprises. This simplifies appliance design and enables breakthrough performance without compromising on security.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which is a more accurate description of a modern firewall?
 - A. A device that inspects network traffic at an entry point to the Internet and within a simple, easily-defined network perimeter
 - B. A multifunctional device that inspects network traffic from the perimeter or internally, within a network that has many different entry points

2. What solution, specific to Fortinet, enhances performance and reduces latency for specific features and traffic?
 - A. Acceleration hardware, called SPUs
 - B. Increased RAM and CPU power



DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions



Basic Administration



Built-In Servers



Fundamental Maintenance

Good job! You now understand some of the high-level features of FortiGate.

Now, you will learn how to perform the initial setup of FortiGate and learn about why you might decide to use one configuration over another.

DO NOT REPRINT

© FORTINET

Setup Decisions

Objectives

- Identify the factory defaults
- Select an operation mode
- Understand FortiGate's relationship with FortiGuard and distinguish between live queries and package updates

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

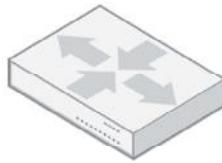
By demonstrating competence in setting up FortiGate, you will be able to use the device effectively in your own network.

DO NOT REPRINT**© FORTINET**

Modes of Operation

NAT

- FortiGate is an OSI Layer 3 **router**
- Interfaces have IP addresses
- Packets are routed by IP
- Configured per VDOM



FORTINET

Transparent

- FortiGate is an OSI Layer 2 **switch** or **bridge**
- Interfaces do *not* have IPs
- Cannot route packets, only forward or block
- Configured per VDOM



© Fortinet Inc. All Rights Reserved.

12

What about the network architecture? Where does FortiGate fit in?

When you deploy FortiGate, you can choose between two operating modes: NAT mode or transparent mode.

- In NAT mode, FortiGate routes packets based on Layer 3, like a router. Each of its logical network interfaces has an IP address and FortiGate determines the outgoing or egress interface based on the destination IP address and entries in its routing tables.
- In transparent mode, FortiGate forwards packets at Layer 2, like a switch. Its interfaces have no IP addresses and FortiGate determines the outgoing or egress interface based on the destination MAC address. The device in transparent mode has an IP address used for management traffic.

Interfaces *can* be exceptions to the router versus switch operation mode, on an individual basis.

When virtual domains (VDOMs) are enabled on FortiGate, each VDOM can be configured for NAT mode or transparent mode, regardless of the operation mode of other VDOMs on FortiGate. By default, VDOMs are disabled on the FortiGate device, but there is still one VDOM active: the *root* VDOM. It is always there in the background. When VDOMs are disabled, the NAT mode or transparent mode relates to the root VDOM.

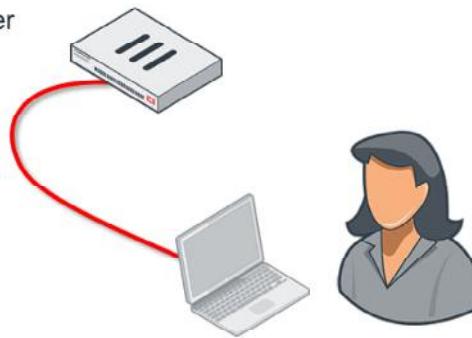
VDOMs are a method of dividing a FortiGate device into two or more virtual devices that function as multiple independent devices. VDOMs can provide separate firewall policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network or organization. In transparent mode, VDOM applies security scanning to traffic and is installed between the internal network and the external network.

By default, a VDOM is in NAT mode when it is created. You can switch it to transparent mode, if required.

DO NOT REPRINT**© FORTINET**

Factory Default Settings

- IP: 192.168.1.99/24
 - MGMT interface on High-End and Mid-Range models
 - Port1 or internal interface on Entry-level models
- PING, HTTP, HTTPS, and SSH protocol management enabled
- Built-in DHCP server is enabled on port1 or internal interface
 - Only on entry-level models that support DHCP server
- Default login:
 - User: admin
 - Password: (blank)
 - Both are case sensitive
 - Modify the default (blank) password
- Can access FortiGate on the CLI
 - Console: without network
 - CLI Console widget and terminal emulator, such as PuTTY or Tera Term



FORTINET

© Fortinet Inc. All Rights Reserved.

13

Network address translation (NAT) mode is the default operation mode. What are the other factory default settings? After you've removed FortiGate from its box, what do you do next?

Now you'll take a look at how you set up FortiGate.

Attach your computer's network cable to port1 or the internal switch ports (entry-level model). For high-end and mid-range models, connect to the MGMT interface. In most entry models, there is a DHCP server on that interface, so, if your computer's network settings have DHCP enabled, your computer should automatically get an IP, and you can begin setup.

To access the GUI on FortiGate or FortiWifi, open a web browser and go to <http://192.168.1.99>.

The default login information is public knowledge. Never leave the default password blank. Your network is only as secure as your FortiGate's admin account. Once you logged in with default login details, you'll see a message to change default blank password for admin user. Before you connect FortiGate to your network, you should set a complex password.

All FortiGate models have a console port and/or USB management port. The port provides CLI access without a network. The CLI can be accessed by the CLI console widget on the GUI or from a terminal emulator, such as PuTTY or Tera Term.

DO NOT REPRINT**© FORTINET**

FortiGuard Subscription Services

- Internet connection and contract required
- Provided by FortiGuard Distribution Network (FDN)
 - Major data centers in the North America, Asia, and Europe
 - Or, from FDN through your FortiManager
 - FortiGate prefers the data center in nearest time zone, but will adjust by server load
- Package updates: FortiGuard antivirus and IPS
 - update.fortiguard.net
 - TCP port 443 (SSL)
- Live queries: FortiGuard web filtering, DNS filtering, and antispam
 - service.fortiguard.net for proprietary protocol on UDP port 53 or 8888
 - securewfw.fortiguard.net for HTTPS over port 443, 53 or 8888



FORTINET

© Fortinet Inc. All Rights Reserved.

14

Some FortiGate services connect to other servers, such as FortiGuard, in order to work. FortiGuard Subscription Services provide FortiGate with up-to-date threat intelligence. FortiGate uses FortiGuard by:

- Periodically requesting packages that contain a new engine and signatures
- Querying the FDN on an individual URL or host name

By default, the FortiGuard server location is set to any where FortiGate will select a server based on server load from any part of the world. However, you have an option to change the FortiGuard server location to USA. In this case, FortiGate will select a USA based FortiGuard server.

Queries are real-time; that is, FortiGate asks the FDN every time it scans for spam or filtered websites. FortiGate queries, instead of downloading the database, because of the size and frequency of changes that occur to the database. Also, you can select queries to use UDP or HTTPs for transport; the protocols are not designed for fault tolerance, but for speed. So, queries require that your FortiGate has a reliable Internet connection.

Packages, like antivirus and IPS, are smaller and don't change as frequently, so they are downloaded (in many cases) only once a day. They are downloaded, using TCP for reliable transport. After the database is downloaded, their associated FortiGate features continue to function, even if FortiGate does not have reliable Internet connectivity. However, you should still try to avoid interruptions during downloads—if your FortiGate must try repeatedly to download updates, it can't detect new threats during that time.

DO NOT REPRINT**© FORTINET**

FortiGuard Subscription Services (Contd)

- FortiGuard third party SSL certificate verification and OCSP stapling check
 - Default FortiGuard access mode is *anycast*
 - Optimize the routing performance to the FortiGuard servers
 - FortiGate gets a single IP address for the domain name of each FortiGuard service
 - FortiGuard servers query the CA's OCSP responder every four hours
 - Enforce a connection to use protocol HTTPS and port 443

Server	Domain name and IP address
Object download	globalupdate.fortinet.net - 173.243.140.6
Querying service (web-filtering, anti-spam)	globalguardservice.fortinet.net - 173.243.140.16
FortiGate Cloud logging	globallogctrl.fortinet.net - 173.243.132.25
FortiGate Cloud management	globalmgrctrl.fortinet.net - 173.243.132.26
FortiGate Cloud messaging	globalmsgctrl.fortinet.net - 173.243.132.27
FortiGate Cloud sandbox	globalaptctrl.fortinet.net - 184.94.112.22
The productapi used by OVPN registration and GUI icon download	globalproductapi.fortinet.net - 66.35.17.252

FORTINET

© Fortinet Inc. All Rights Reserved.

15

In FortiOS 6.4, third party SSL certificate verification and OCSP stapling check has been implemented for all FortiGuard servers. By default, the FortiGuard access mode is *anycast* on the FortiGate to optimize the routing performance to the FortiGuard servers. The FortiGuard server has one IP address to match its domain name. FortiGate connects with a single server address, regardless of where the FortiGate is located.

The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, so that FortiGate can always validate the FortiGuard server certificate efficiently. FortiGate will only complete the TLS handshake with a FortiGuard that provides a *good* OCSP status for its certificate, any other status will result in a failed SSL connection.

The FortiGuard servers query the CA's OCSP responder every four hours and update its OCSP status. If the FortiGuard is unable to reach the OCSP responder, it will keep the last known OCSP status for seven days.

FortiGate aborts connection to the FortiGuard server if:

- The CN in the server's certificate does not match the domain name resolved from the DNS.
- The OCSP status is not good.
- The issuer-CA is revoked by the root-CA.

The FortiGuard access mode *anycast* setting, force the rating process to use protocol HTTPS, and port 443. The table in a slide, shows a list of some the FortiGuard servers and their domain name and IP address.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which protocol does FortiGate use to download antivirus and IPS packages?
A. UDP
 B. TCP

2. How does FortiGate check content for spam or malicious websites?
 A. Live queries to FortiGuard over UDP or HTTPS
B. Local verification using a downloaded web filter database locally on FortiGate



© Fortinet Inc. All Rights Reserved.

16

DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions

Basic Administration

Built-In Servers



Fundamental Maintenance

Good job! You now understand how to perform the initial setup of FortiGate and why you might decide to use one configuration over another. Now, you will learn about basic administration.

DO NOT REPRINT**© FORTINET**

Basic Administration

Objectives

- Manage administrator profiles
- Manage administrative users
- Define the configuration method for administrative users
- Control administrative access to the FortiGate GUI and CLI
- Manage specific aspects of the network interfaces

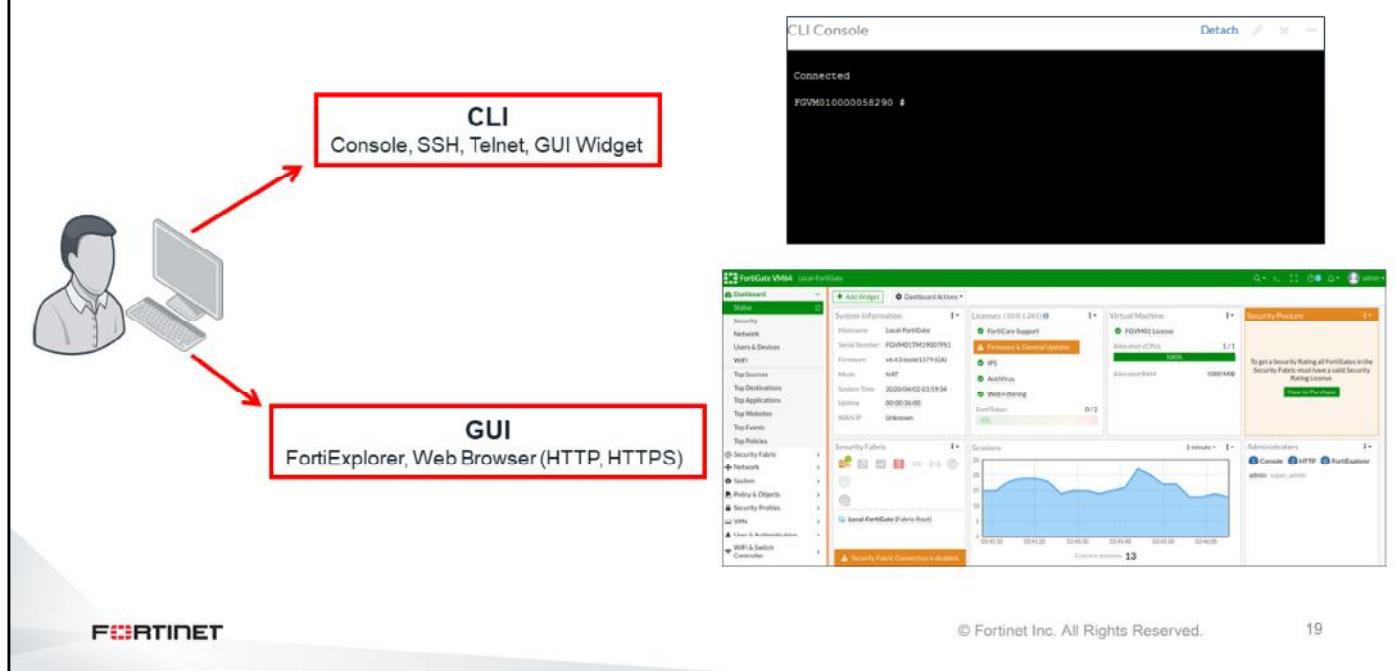
After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic administration, you will be able to better manage administrative users and implement stronger security practices around administrative access.

DO NOT REPRINT

© FORTINET

Administration Methods



Most features are available on both the GUI and CLI, but there are a few exceptions. Reports cannot be viewed on the CLI. Also, advanced settings and diagnostic commands for super users are usually not available on the GUI.

As you become more familiar with FortiGate, and especially if you want to script its configuration, you may want to use the CLI in addition to the GUI. You can access the CLI through either the JavaScript widget in the GUI named **CLI Console**, or through a terminal emulator such as Tera Term (<http://ttssh2.sourceforge.jp/index.html.en>) or PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>). Your terminal emulator can connect through the network—SSH or telnet—or the local console port.

SNMP and some other administrative protocols are also supported, but they are read-only. They can't be used for basic setup.

DO NOT REPRINT**© FORTINET**

Basic CLI Commands

- Use the following commands to check the system status and list all or only non-default attribute values for an interface
- Use <command set> ? to list commands that you can use with it. For example, get ? and list sub-commands under <command set> <command>
 - For example, execute backup ?

What to investigate...	CLI commands to Use...
What is the current status of FortiGate?	get system status
What are all the attribute values for the system interface?	show full-configuration system interface <port>
What are the non-default attribute values for the system interface?	show system interface <port>



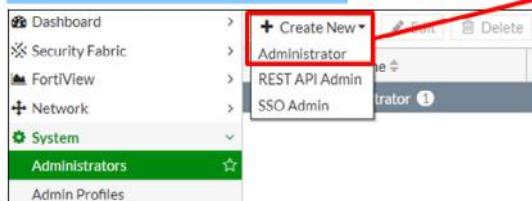
This slide shows some basic CLI commands that you can use to list commands under a command set, check the system status, and list attributes and their values for an interface.

DO NOT REPRINT

© FORTINET

Create an Administrative User

System > Administrators



© Fortinet Inc. All Rights Reserved.

21

Whichever method you use, start by logging in as admin. Begin by creating separate accounts for other administrators. For security and tracking purposes, it is a best practice for each administrator to have their own account.

In the **Create New** drop-down list, you can select either **Administrator** or **REST API Admin**. Typically, you will select **Administrator** and then assign an **Administrator Profile**, which specifies that user's administrative permissions. You could select **REST API Admin** to add an administrative user who would use a custom application to access FortiGate with a REST API. The application would allow you to log in to FortiGate and perform any task that your assigned **Administrator Profile** permits.

Other options not shown here, include:

- Instead of creating accounts on FortiGate itself, you could configure FortiGate to query a remote authentication server.
- In place of passwords, your administrators could authenticate using digital certificates that are issued by your internal certification authority server.

If you do use passwords, ensure that they are strong and complex. For example, you could use multiple interleaved words with varying capitalization, and randomly insert numbers and punctuation. Do not use short passwords, or passwords that contain names, dates, or words that exist in any dictionary. These are susceptible to brute force attack. To audit the strength of your passwords, use tools such as L0phcrack (<http://www.l0phcrack.com/>) or John the Ripper (<http://www.openwall.com/john/>). Risk of a brute force attack is increased if you connect the management port to the Internet.

In order to restrict access to specific features, you can assign permissions.

DO NOT REPRINT

© FORTINET

Administrator Profiles—Permissions

System > Admin Profiles



FORTINET

© Fortinet Inc. All Rights Reserved.

22

When assigning permissions to an administrator profile, you can specify read-and-write, read-only, or none to each area.

By default, there is a special profile named **super_admin**, which is used by the account named **admin**. It cannot be changed. It provides full access to everything, making the **admin** account similar to a root **superuser** account.

The **prof_admin** is another default profile. It also provides full access, but unlike **super_admin**, it only applies to its virtual domain—not the global settings of FortiGate. Also, its permissions can be changed.

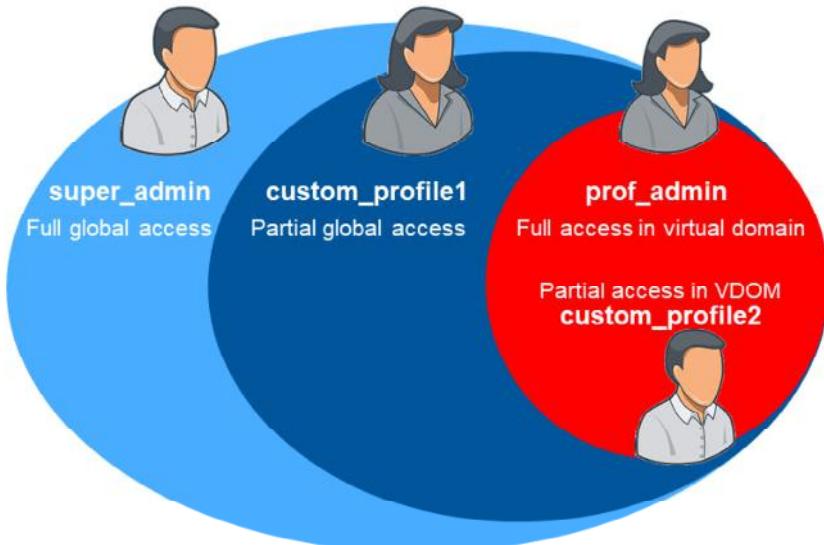
You aren't required to use a default profile. You could, for example, create a profile named **auditor_access** with read-only permissions. Restricting a person's permissions to those necessary for his or her job is a best practice, because even if that account is compromised, the compromise to your FortiGate (or network) is not total. To do this, create administrator profiles, then select the appropriate profile when configuring an account.

The **Override Idle Timeout** feature allows the admintimeout value, under config system accprofile, to be overridden per access profile. Administrator profiles can be configured to increase inactivity timeout and facilitate use of the GUI for central monitoring.

Note that this can be achieved on a per-profile basis, to prevent the option from being unintentionally set globally.

DO NOT REPRINT**© FORTINET**

Administrator Profiles—Hierarchy

**FORTINET**

© Fortinet Inc. All Rights Reserved.

23

What are the effects of administrator profiles?

It's actually more than just read or write access.

Depending on the type of administrator profile that you assign, an administrator may not be able to access the entire FortiGate. For example, you could configure an account that can view only log messages. Administrators may not be able to access global settings outside their assigned virtual domain either. Virtual domains (VDOMs) are a way of subdividing the resources and configurations on a single FortiGate.

Administrators with a smaller scope of permissions cannot create, or even view, accounts with more permissions. So, for example, an administrator using the **prof_admin** or a custom profile cannot see, or reset the password of, accounts that use the **super_admin** profile.

DO NOT REPRINT**© FORTINET**

Two-Factor Authentication



Password (one factor)
+
FortiToken (two factor)

**FORTINET**

© Fortinet Inc. All Rights Reserved.

24

To further secure access to your network security, use two-factor authentication.

Two-factor authentication means that instead of using one method to verify your identity—typically a password or digital certificate—your identity is verified by two methods. In the example shown on this slide, two-factor authentication includes a password plus an RSA randomly generated number from a FortiToken that is synchronized with FortiGate.

DO NOT REPRINT**© FORTINET**

Resetting a Lost Admin Password

User: maintainer

Password: bcpb<serial-number>

All letters in <serial-number> *must* be upper case, for example, FGT60

- All FortiGate appliance models and some other Fortinet device types
- No maintainer procedure in VM, revert to snapshot or reprovision VM
- Only after hard power cycle
 - Soft cycle (reboot) does not work for security reasons.
- Only during first 60 seconds *after boot* (varies by model)
 - Tip: Copy serial number into the terminal buffer, then paste
- Only through hardware console port
 - Requires physical access for security reasons
 - If compliance/risk of physical access requires, maintainer can be disabled

```
config sys global
    set admin-maintainer disable
end
```



© Fortinet Inc. All Rights Reserved.

25

What happens if you forget the password for your `admin` account, or a malicious employee changes it?

This recovery method is available on all FortiGate appliance devices and even some non-FortiGate devices, like FortiMail. There is no maintainer procedure in VM. Administrator must revert to snapshot or reprovision the VM and restore configuration. It's a *temporary* account, only available through the local console port, and only after a hard reboot—disrupting power by unplugging or turning off the power, then restoring it. FortiGate must be physically shut off, then turned back on, not simply rebooted through the CLI.

The `maintainer` login will only be available for login for about 60 seconds after the restart completes (or less time on older models).

If you cannot ensure physical security, or have compliance requirements, you can disable the `maintainer` account. Use caution if you disable `maintainer` and then lose your `admin` password, you cannot recover access to your FortiGate. In order to regain access in this scenario, you will need to reload the device. This will reset to factory default.

DO NOT REPRINT

© FORTINET

Administrative Access—Trusted Sources

The diagram illustrates the configuration and enforcement of trusted hosts for administrative access on a FortiGate device.

Configuration: On the left, the "System > Administrators" configuration screen shows the "Restrict login to trusted hosts" option selected. Under "Trusted Host 1", the IP address 10.0.1.10/32 is listed. A red arrow points from this entry to the "Trusted Hosts" column in the "System Administrator" table on the right, which lists "admin" and "admin1". Both accounts have "10.0.1.10/32" listed under "Trusted Hosts".

Login Failure Message: A blue callout box states: "If admin1 attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message". To the right, a screenshot of the FortiGate login interface shows a red error message box stating "Authentication failure". Below it are fields for "Username" and "Password", and a green "Login" button.

FORTINET

© Fortinet Inc. All Rights Reserved.

26

Another way to secure your FortiGate is to define the hosts or subnets that are trusted sources from which to log in.

In this example, we have configured 10.0.1.10 as the only trusted IP for admin1 from which admin1 log in. If admin1 attempts to log in from a machine with any other IP, they will receive an authentication failure message.

Note that If trusted hosts are configured on all administrators and an administrator is trying to log in from an IP address that is not set on any of the trusted host for any administrators, then the administrator will not get the login page but rather will receive the message: "Unable to contact server".

If you leave any IPv4 address as 0.0.0.0/0, it means that connections from any source IP will be allowed. By default, 0.0.0.0/0 is the configuration for administrator, although you may want to change this.

Notice that each account can define its management host or subnet differently. This is especially useful if you are setting up VDOMs on your FortiGate, where the VDOM's administrators may not even belong to the same organization. Be aware of any NAT that occurs between the desired device and FortiGate. You can easily prevent an administrator from logging in from the desired IP address if it is later NATed to another address before reaching FortiGate, thus defeating the purpose of the trusted hosts.

DO NOT REPRINT**© FORTINET**

Administrative Access—Ports and Password

- Port numbers are customizable.
- Using only secure access (SSH, HTTPS) is recommended.
- Default **Idle timeout** is 5 minutes.

System > Settings

The screenshot shows the 'System > Settings' interface. The 'Administration Settings' section is highlighted with a red box. It includes fields for 'HTTP port' (80), 'Redirect to HTTPS' (selected), 'HTTPS port' (443), 'HTTPS server certificate' (self-sign selected), 'SSH port' (22), 'Telnet port' (23), and 'Idle timeout' (5 minutes). Below this is the 'Password Policy' section, also highlighted with a red box, containing fields for 'Password scope' (Admin selected), 'Minimum length' (8), 'Character requirements' (selected), 'Allow password reuse' (selected), and 'Password expiration' (selected).

FORTINET

© Fortinet Inc. All Rights Reserved.

27

You may also want to customize the administrative protocols' port numbers.

You can choose whether to allow concurrent sessions. This can be used to prevent accidentally overwriting settings, if you usually keep multiple browser tabs open, or accidentally leave a CLI session open without saving the settings, then begin a GUI session and accidentally edit the same settings differently.

For better security, use only secure protocols, and enforce password complexity and changes.

The **Idle timeout** setting specifies the number of minutes before an inactive administrator session times out (default is 5 minutes). A shorter idle timeout is more secure, but increasing the timer can help reduce the chance of administrators being logged out while testing changes.

You can override the idle timeout setting per administrator profile using the **Override Idle Timeout** setting.

You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. The **Override Idle Timeout** setting allows the **admintimeout** value, under **config system accprofile**, to be overridden per access profile.

Note that this can be achieved on a per profile basis, to avoid the option from being unintentionally set globally.

DO NOT REPRINT**© FORTINET**

Administrative Access—Protocols

- Enable acceptable management protocols on each interface independently:
 - Separate IPv4 and IPv6
 - IPv6 options hidden by default
- Also protocols where FortiGate is the destination IP:
 - Security Fabric:
 - CAPWAP
 - FortiTelemetry
 - FMG-Access
 - FTM
 - RADIUS Accounting
- LLDP Support
 - Detecting an upstream Security Fabric FortiGate through LLDP

Network > Interfaces

The screenshot shows the 'Edit Interface' screen for 'port3'. Under 'Address', the 'Addressing mode' is set to 'Manual' with IP/Netmask '10.0.1.254/255.255.255.0'. The 'Administrative access' section is highlighted with a red border. It lists various protocols: HTTPS (checked), FMG-Access (unchecked), TELNET (checked), SSH (checked), HTTP (checked), PING (checked), SNMP (unchecked), FTM (unchecked), and RADIUS Accounting (unchecked). Below this, there are sections for 'Receive LLDP' and 'Transmit LLDP', both with 'Use VDOM Setting' selected.

© Fortinet Inc. All Rights Reserved.

28

You've defined the management subnet—that is, the trusted hosts—for each administrator account. How do you enable or disable management protocols?

This is specific to each interface. For example, if your administrators connect to FortiGate only from port3, then you should disable administrative access on all other ports. This prevents brute force attempts and also insecure access. Your management protocols are HTTPS, HTTP, PING, SSH. By default, the TELNET option is not visible on the GUI.

Consider the location of the interface on your network. Enabling PING on an internal interface is useful for troubleshooting. However, if it's an external interface (in other words exposed to the Internet), then the PING protocol could expose FortiGate to a DoS attack. Protocols that do not encrypt data flow, such as HTTP and TELNET, should be disabled. IPv4 and IPv6 protocols are separate. It's possible to have both IPv4 and IPv6 addresses on an interface, but only respond to pings on IPv6.

Security Fabric connection includes CAPWAP and FortiTelemetry. Protocols like FortiTelemetry are *not* for administrative access, but, like GUI and CLI access, they are protocols where the packets will have FortiGate as a destination IP. The FortiTelemetry protocol is used specifically for managing FortiClients and the Security Fabric. The CAPWAP protocol is used for FortiAP, FortiSwitch, and FortiExtender when they are managed by FortiGate. FMG-Access protocol is used specifically for communicating with FortiManager when that server is managing multiple FortiGate devices. RADIUS accounting protocol is used when FortiGate needs to listen for and process RADIUS Accounting packets for single sign-on authentication. FTM, or FortiToken Mobile push, supports second-factor authentication requests from a FortiToken mobile app.

When you assign the interface roles LAN or WAN to the appropriate interfaces, your FortiGate uses Link Layer Discovery Protocol (LLDP) to detect if there's an upstream FortiGate in your network. If an upstream FortiGate is discovered, you're prompted to configure the FortiGate to join the Security Fabric.

DO NOT REPRINT**© FORTINET**

Features Hidden by Default

- By default, some features like IPv6 are hidden on the GUI
 - Hidden features are not disabled
- In **Feature Visibility**, select whether to hide or show groups of features commonly used together.

System > Feature Visibility

Core Features

- Advanced Routing
- IPv6** (highlighted)
- VPN
- WiFi Controller

Security Features (Feature Set: NGFW)

- AntiVirus
- Application Control
- DNS Filter
- Email Filter
- Endpoint Control
- Explicit Proxy
- Intrusion Prevention
- Web Application Firewall
- Web Filter

Additional Features

- Allow Unnamed Policies
- Certificates
- DNS Database
- Domain & IP Reputation
- Dos Policy
- Email Collection

FORTINET

© Fortinet Inc. All Rights Reserved.

29

FortiGate has hundreds of features. If you don't use all of them, hiding features that you don't use makes it easier to focus on your work.

Hiding a feature on the GUI does not disable it. It is still functional, and still can be configured using the CLI.

Some advanced or less commonly used features, such as IPv6, are hidden by default.

To show hidden features, click **System > Feature Visibility**.

DO NOT REPRINT**© FORTINET**

Interface IPs

- In NAT mode, interfaces cannot be used until they have an IP address:
 - Manually assigned
 - Automatic
 - DHCP
 - PPPoE
- Exception: **One-Arm Sniffer**

Network > Interfaces

Edit Interface

Name: port8
Alias:
Type: Physical Interface
Role: Undefined

Address

Addressing mode: Manual DHCP One-Arm Sniffer
IP/Netmask: 0.0.0.0/0.0.0.0

Note that the **One-Arm Sniffer** is available only when editing an unreferenced interface

Edit Interface

Name: port8
Alias:
Type: Physical Interface
Role: Undefined

Address

Addressing mode: Manual DHCP One-Arm Sniffer
Retrieve default gateway from server:
Distance: 5
Override internal DNS:

© Fortinet Inc. All Rights Reserved.

30

When FortiGate is operating in NAT mode, every interface that handles traffic must have an IP address. When in NAT mode, the IP address can be used by FortiGate to source the traffic, if it needs to start or reply to a session, and can be used as a destination address for devices trying to contact FortiGate or route traffic through it. There are multiple ways to get an IP address:

- Manually
- Automatically, using either DHCP or PPPoE

There is an exception to the IP address requirement: the **One-Arm Sniffer** interface type. This interface is *not* assigned an address.

When **One-Arm Sniffer** is selected as the addressing mode, the interface is not inline with the traffic flow, rather it is receiving a copy of the traffic from a mirrored port on a switch. The interface operates in promiscuous mode scanning traffic that it sees but is unable to make changes as the original packet has already been processed by the switch. As a result, one-arm sniffer mode is mostly used in proof of concept (POC) or in environments where corporate requirements state that traffic must not be changed, only logged.

DO NOT REPRINT**© FORTINET**

Interface Role Compared to Alias

- Role defines interface settings typically grouped together:
 - Avoids accidental misconfiguration
 - Four types:
 - WAN
 - LAN
 - DMZ
 - Undefined (show all settings)
 - Not in list of policies
- Alias is a friendly descriptor for the interface:
 - Used in list of policies to label interfaces by purpose

The screenshot shows two FortiGate management interface windows. The top window, titled 'Edit Interface', displays configuration for 'port3'. It includes fields for 'Name' (port3), 'Alias' (internal_network), 'Type' (Physical Interface), 'Role' (set to 'LAN'), 'Address' (WAN), 'Addressing' (DHCP), and 'IP/Netmask' (10.0.1.254/255.255.255.0). The bottom window, titled 'Policy & Objects > IPv4 Policy', shows a table of security policies. The first policy, 'Full Access', is applied to 'Internal network (port3)' and 'Internet Access Port (port1)', with a source of 'LOCAL SUBNET'. The second policy, 'Implicit Deny', applies to 'any' with a source of 'all'.

ID	Name	From	To	Source
1	Full Access	<input checked="" type="checkbox"/> Internal network (port3)	<input checked="" type="checkbox"/> Internet Access Port (port1)	<input checked="" type="checkbox"/> LOCAL SUBNET
0	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all

FORTINET

© Fortinet Inc. All Rights Reserved.

31

How many times have you seen network issues caused by a DHCP server—not client—enabled on the WAN interface?

You can configure the interface's role. The roles shown in the GUI are the usual interface settings for that part of a topology. Settings that do not apply to the current role are hidden on the GUI (all settings are always available on the CLI regardless of the role). This prevents accidental misconfiguration.

For example, when the role is configured as WAN, there is no DHCP server and device detection configuration available. Device detection is usually used to detect devices internally on your LAN.

If there is an unusual case, and you need to use an option that's hidden by the current role, you can always switch the role to **Undefined**. This displays all options.

To help you remember the use of each interface, you can give them aliases. For example, you could call port3 `internal_network`. This can help to make your list of policies easier to comprehend.

DO NOT REPRINT

© FORTINET

Static Gateway

- Must be at least one default gateway
- If the interface is DHCP or PPPoE, the gateway can be added dynamically



This is a detailed view of the 'New Static Route' dialog box. It includes fields for Destination (Subnet 0.0.0.0/0.0.0.0), Gateway Address (10.200.2.254), Interface (port2), Administrative Distance (10), Comments (empty), and Status (Enabled). Below these are 'Advanced Options' with a Priority field set to 0. At the bottom are 'OK' and 'Cancel' buttons.

FORTINET

© Fortinet Inc. All Rights Reserved.

32

Before you integrate FortiGate into your network, you should configure a default gateway.

If FortiGate gets its IP address through a dynamic method such as DHCP or PPPoE, then it should also retrieve the default gateway.

Otherwise, you must configure a static route. Without this, FortiGate will not be able to respond to packets outside the subnets directly attached to its own interfaces. It probably also will not be able to connect to FortiGuard for updates, and may not properly route traffic.

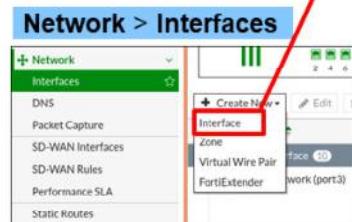
You should make sure that FortiGate has a route that matches all packets (destination is 0.0.0.0/0), known as a default route, and forwards them through the network interface that is connected to the Internet, to the IP address of the next router.

Routing completes the basic network settings that are required before you can configure firewall policies.

DO NOT REPRINT**© FORTINET**

Link Aggregation

- Bundles several physical ports to form a single point-to-point logical channel with greater bandwidth
 - Increases redundancy for higher availability



New Interface

Name	Link_Agg1		
Alias			
Type	802.3ad Aggregate		
Interface members	port6 port7		
Role	LAN		
Address			
Addressing mode	Manual		
IP/Netmask	10.0.5.1/24		
Create address object matching subnet			
Name	Link_Agg1 address		
Destination	10.0.5.1/24		
Secondary IP address			
Administrative access			
IPv4	<input type="checkbox"/> HTTPS <input type="checkbox"/> SSH <input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> PING <input type="checkbox"/> SNMP <input type="checkbox"/> Security Fabric Connection	<input type="checkbox"/> FMG-Access <input type="checkbox"/> FTM
Receive LLDP	Use VDOM Setting	Enable	Disable
Transmit LLDP	Use VDOM Setting	Enable	Disable
DHCP Server			
Network			
Device detection	Enabled		
Security mode	Normal		

© Fortinet Inc. All Rights Reserved.

33

Link aggregation logically binds multiple physical interfaces into a single channel. Link aggregation increases bandwidth and provides redundancy between two network devices.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. How do you restrict logins to FortiGate from only specific IP addresses?
 - A. Change FortiGate management interface IP address
 - B. Configure trusted host

2. As a best security practice when configuring administrative access to FortiGate, which protocol should you disable?
 A. Telnet
 B. SSH



© Fortinet Inc. All Rights Reserved.

34

DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



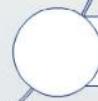
Setup Decisions



Basic Administration



Built-In Servers



Fundamental Maintenance

Good job! You now have the knowledge needed to carry out some basic administrative tasks. Now, you'll learn about built-in servers.

DO NOT REPRINT

© FORTINET

Built-In Servers

Objectives

- Enable the DHCP service on FortiGate
- Enable the DNS service on FortiGate
- Understand the configuration possibilities and some of their implications

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

By demonstrating competence in implementing the DHCP and DNS built-in servers, you will know how to provide these services through FortiGate.

DO NOT REPRINT

© FORTINET

FortiGate as a DHCP Server

The screenshot shows the FortiGate interface with three windows open:

- Edit Interface:** Shows an interface named "port3" with a "Role" of "LAN". The "Addressing mode" is set to "Manual" with IP "10.0.1.254/255.255.255.0".
- DHCP Server:** Shows a configuration for an address range from 10.0.1.1 to 10.0.1.253. It includes options for Default gateway, DNS server, and Lease time.
- Create New IP Address Assignment Rule:** A modal window for creating a new rule. It has fields for Type (set to "MAC Address"), Description (empty), Match Criteria (empty), Action (set to "Assign IP"), and IP (empty). There is also a "Create New" button for rules.

Red arrows point from the "Edit Interface" and "DHCP Server" sections towards the "Create New IP Address Assignment Rule" modal, indicating their relationship.

© Fortinet Inc. All Rights Reserved. 37

Wireless clients are not the only ones that can use FortiGate as their DHCP server.

For an interface (such as port3), select the **Manual** option, enter a static IP, and then enable the **DHCP Server** option. Options for the built-in DHCP server will appear, including provisioning features, such as DHCP options and IP address assignment rules. You can also block specific MAC addresses from receiving an IP address. Note that in the screenshot on the middle of the slide, in the **IP Address Assignment Rule** section, you can create IP address assignment rules.

DO NOT REPRINT**© FORTINET**

DHCP Server—IP Address Assignment Rule

- Assign, block or reserve the IP address to the host
 - To assign, type MAC address and select action type Assign IP or choose from existing DHCP lease
 - To block, type MAC address and select action type to block
 - To reserve, type MAC address, select action type and then add the IP address
- FortiGate uses the host's MAC address to look up its IP address in the reservation table
- Actions if MAC is unknown

Network > Interfaces

The screenshot shows the 'IP Address Assignment Rules' section under 'Network > Interfaces'. A red box highlights the 'Create New' button. Below it, a detailed view of a new rule being created is shown in a separate window:

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0C:29:E1:E0:62	Assign IP	
Implicit	Unknown MAC Addresses	Assign IP	
Networked Devices			

Create New IP Address Assignment Rule

Type: **MAC Address** (selected) | Description: Write a comment... | Match Criteria: MAC address: | Action: Action type: **Assign IP** (selected), Block, Reserve IP | IP: 0.0.0.0 | OK | Cancel

FORTINET

© Fortinet Inc. All Rights Reserved.

38

For the built-in DHCP server, you can reserve specific IP addresses for devices with specific MAC addresses.

The action selected for **Unknown MAC Addresses** defines what FortiGate DHCP server does when it gets a request from a MAC address that is not explicitly listed. The default action is **Assign IP**; however, you can change the default action type to **Assign IP** or **Block**.

- **Assign IP**: Permits the DHCP server to assign from its pool of addresses to the identified MAC address. A device receiving an IP address will always receive the same address provided that its lease has not expired.
- **Block**: The computer with the identified MAC address and the **Block** option will not receive an IP address.
- **Reserve IP**: This allows you to bind a specific IP to a MAC address.

DO NOT REPRINT**© FORTINET**

FortiGate as a DNS Server

- Resolves DNS lookups from the internal network:
 - Enabled per interface
 - Not appropriate for Internet service because of load, and therefore should not be public facing.
- One DNS database can be shared by all FortiGate interfaces:
 - Can be separate per VDOM
- Resolution methods:
 - Forward: Relay requests to the next server (in DNS settings)
 - Non-recursive: Use FortiGate DNS database only to try to resolve queries
 - Recursive: Use FortiGate DNS database first; relay unresolvable queries to next server (in DNS settings)



© Fortinet Inc. All Rights Reserved.

39

You can configure FortiGate to act as your local DNS server. You can enable and configure DNS separately on each interface.

A local DNS server can improve performance for your FortiMail or other devices that use DNS queries frequently. If your FortiGate offers DHCP to your local network, DHCP can be used to configure those hosts to use FortiGate as both the gateway and DNS server.

FortiGate can answer DNS queries in one of three ways:

- Forward: Relays all queries to a separate DNS server (that you have configured in **Network > DNS**); that is, it acts as a DNS relay instead of a DNS server.
- Non-Recursive: Replies to queries for items in FortiGate's DNS databases and does not forward unresolvable queries.
- Recursive: Replies to queries for items in FortiGate's DNS databases and forwards all other queries to a separate DNS server for resolution.

You can configure all modes on the GUI or CLI.

DO NOT REPRINT**© FORTINET**

DNS Forwarding

- Forwarding allows DNS control without the local FQDN database
- Sends query to the external DNS server

Network > DNS Servers

The screenshot shows the FortiGate management interface under the 'Network' tab. The 'DNS Servers' option is selected, highlighted with a red box. The 'DNS Service on Interface' table has a row for 'internal_network (port3)' set to 'Recursive'. The 'DNS Database' table lists three entries: 'remote.lab' (Master, Shadow, TTL 86400), 'student.lab' (Master, Shadow, TTL 86400), and 'training.lab' (Master, Shadow, TTL 86400). A callout box points to the 'Recursive' mode in the service table with the text: 'To view DNS Servers in Network, you must make it visible in System > Feature Visibility > DNS database'.

Double-click the interface field or select and click **Edit**.

Edit DNS Service

Interface	internal_network (port3)
Mode	Recursive Non-Recursive
DNS Filter	<input type="checkbox"/>
OK Cancel	

Forward to System DNS

© Fortinet Inc. All Rights Reserved. 40

If you choose Recursive, FortiGate queries its own database before forwarding unresolved requests to the external DNS servers.

If you choose **Forward to System DNS**, you can control DNS queries within your own network, without having to enter any DNS names in FortiGate's DNS server.

DO NOT REPRINT**© FORTINET**

DNS Database—Configuration

- Add DNS zones:
 - Each zone has its own domain name
 - RFC 1034 and 1035
- Add DNS entries to each zone:
 - Host name
 - IP address it resolves to
 - Types supported:
 - IPv4 address (A) or IPv6 address (AAAA)
 - Name server (NS)
 - Canonical name (CNAME)
 - Mail exchange (MX) server
 - IPv4 (PTR) or IPv6 (PTR)



© Fortinet Inc. All Rights Reserved.

41

If you choose to have your DNS server resolve queries, or you choose a split DNS, you must set up a DNS database on your FortiGate.

This defines the host names that FortiGate will resolve queries for. Note that FortiGate currently supports only the DNS record types listed on this slide.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. When configuring FortiGate as a DHCP server, to restrict access by MAC address, what does the **Assign IP** option do?
 - A. Assigns a specific IP address to a MAC address
 - B. Dynamically assigns an IP to a MAC address

2. When configuring FortiGate as a DNS server, which resolution method uses the FortiGate DNS database only to try to resolve queries?
 - A. Non-recursive
 - B. Recursive

DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions



Basic Administration



Built-In Servers



Fundamental Maintenance

Good job! You now know how to enable DHCP and DNS services on FortiGate, and have some understanding of configuration possibilities. Now, you will learn about fundamental maintenance.

DO NOT REPRINT**© FORTINET**

Fundamental Maintenance

Objectives

- Back up and restore system configuration files
- Understand the restore requirements for plain text and encrypted configuration files
- Identify the current firmware version
- Upgrade firmware
- Downgrade firmware

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

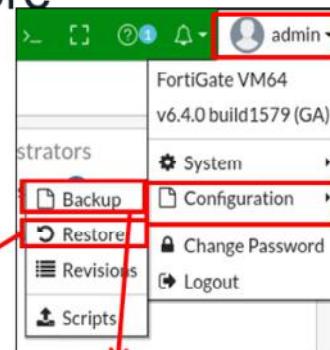
By demonstrating competence in implementing basic maintenance of FortiGate, you will be able to perform the vital activities of back up and restore, upgrade or downgrade firmware, and ensure that FortiGate remains reliably in service throughout its lifecycle.

DO NOT REPRINT

© FORTINET

Configuration File—Backup and Restore

- Configuration can be saved to an external device
 - Optional encryption
 - Can back up automatically
 - Upon logout
 - Not available on all models
- To restore a previous configuration, upload file
 - Reboots FortiGate



Restore System Configuration

Restore from Local PC USB Disk

File

Password

Backup System Configuration

Backup to Local PC USB Disk

Encryption

Password

Confirm password

FORTINET

© Fortinet Inc. All Rights Reserved.

45

Now that FortiGate has basic network settings and administrative accounts, you will learn how to back up the configuration. In addition to selecting the destination of the backup file, you can choose to encrypt or not to encrypt the backup file. Even if you choose not to encrypt the file, which is the default, the passwords stored in the file are hashed, and, therefore, obfuscated. The passwords that are stored in the configuration file would include passwords for the administrative users and local users, and preshared keys for your IPSec VPNs. It may also include passwords for the FSSO and LDAP servers.

The other option is to encrypt the configuration file with a password. Besides securing the privacy of your configuration, it also has some effects you may not expect. After encryption, the configuration file cannot be decrypted without the password and a FortiGate of the same model and firmware. This means that if you send an encrypted configuration file to Fortinet Technical Support, even if you give them the password, they cannot load your configuration until they get access to the same model of FortiGate. This can cause unnecessary delays when resolving your ticket.

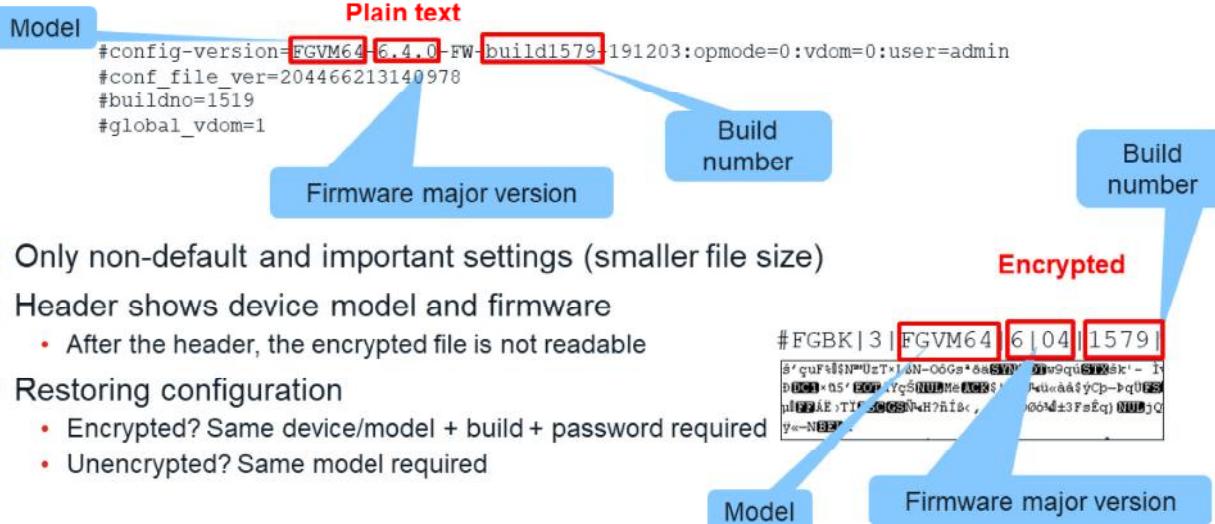
If you enable virtual domains (VDOMs), subdividing the resources and configuration of your FortiGate, each VDOM administrator can back up and restore their own configurations. You don't have to back up the entire FortiGate configuration, however it is still recommended.

Backups are needed to help speed up the return to production in the event of an unforeseen disaster that damages FortiGate. Having to recreate hundreds of policies and objects from scratch takes a significant amount of time, while loading a configuration file on a new device takes much less.

Restoring a configuration file is very similar to backing one up and restarts the FortiGate.

DO NOT REPRINT**© FORTINET**

Configuration File Format

**FORTINET**

© Fortinet Inc. All Rights Reserved.

46

If you open the configuration file in a text editor, you'll see that both encrypted and unencrypted configuration files contain a clear text header that contains some basic information about the device. The example on this slide shows what information is included. To restore an encrypted configuration, you must upload it to a FortiGate of the same model and firmware, then provide the password.

To restore an unencrypted configuration file, you are required to match only the FortiGate model. If the firmware is different, FortiGate will attempt to upgrade the configuration. This is similar to how it uses upgrade scripts on the existing configuration when upgrading firmware. However, it is still recommended to match the firmware on FortiGate to the firmware listed in the configuration file.

Usually, the configuration file only contains non-default settings, plus few default, yet crucial, settings. This minimizes the size of the backup, which could otherwise be several MB in size.

DO NOT REPRINT**© FORTINET**

Upgrade Firmware

- The current firmware version can be viewed on the dashboard or in **System > Firmware** (or on the CLI: get system status)
- If there is an updated firmware version, you will be notified
- Firmware can be updated by clicking **Upload Firmware** or selecting the upgrade option section
- Make sure you read the Release Notes to verify the upgrade path and other details

System > Firmware

FortiGate VM64 Local-FortiGate

Dashboard > Firmware Management

Current version: FortiOS v6.2.0 build0866 (GA)

FortiOS v6.2.3 available

Upload Firmware

Select file

FortiGuard Firmware

Latest: All available

PATCHES

FortiOS v6.2.3 build1066

Release notes

Follow upgrade path Directly update to v6.2.3

v6.2.0 > v6.2.2 > v6.2.3

FortiOS v6.2.2 build1010 will be installed as part of the incremental upgrade process

Backup config and upgrade Upgrade

FORTINET

© Fortinet Inc. All Rights Reserved.

47

You can view the current firmware version in multiple places on the FortiGate GUI. When you first log in to FortiGate, the landing page is the dashboard. You will see the firmware version in the **System** widget. This information is also found at **System > Firmware**. And, of course, you can retrieve the information on the CLI using the command `get system status`.

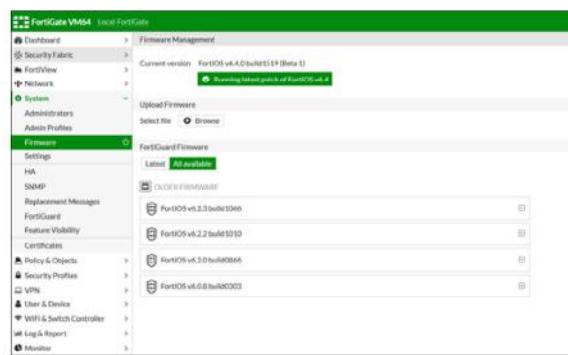
If a new version of the firmware is available, you will be notified on the dashboard and on the **Firmware** page.

Remember to read the *Release Notes* to make sure that you understand the supported upgrade path. The *Release Notes* also provide pertinent information that may affect the upgrade.

DO NOT REPRINT**© FORTINET**

Upgrade Firmware Process

1. Back up the configuration (full config backup on GUI or CLI)
2. Download a copy of the current firmware, in case reversion is needed
3. Have physical access, or a terminal server connected to local console, in case reversion is needed
4. Read the *Release Notes*; they include the upgrade path and other useful information
5. Perform the upgrade



FORTINET

© Fortinet Inc. All Rights Reserved.

48

Upgrading the firmware on FortiGate is simple. Click **System > Firmware**, and then browse to the firmware file that you have downloaded from support.fortinet.com or choose to upgrade online.

If you want to make a clean install by overwriting both the existing firmware and its current configuration, you can do this using the local console CLI, within the boot loader menu, while FortiGate is rebooting. However, this is not the usual method.

DO NOT REPRINT**© FORTINET**

Downgrade Firmware Process

1. Get the pre-upgrade configuration file
2. Download a copy of the current firmware, in case reversion is needed
3. Have physical access, or a terminal server connected to the local console, in case reversion is needed
4. Read the *Release Notes* (Does downgrade preserve configuration?)
5. Downgrade the firmware
6. If required, upload the configuration that matches the firmware version



© Fortinet Inc. All Rights Reserved.

49

You can also downgrade the firmware. Because settings change in each firmware version, you should have a configuration file in the syntax that is compatible with the firmware.

Remember to read the *Release Notes*. Sometimes a downgrade between firmware versions that preserves the configuration is not possible, such as when the OS changed from 32-bit to 64-bit. In that situation, the only way to downgrade is to format the disk, then reinstall.

After you've confirmed that the downgrade is possible, verify everything again, then start the downgrade. After the downgrade completes, restore a configuration backup that is compatible with that version.

Why should you keep emergency firmware and physical access?

Earlier firmware versions do not know how to convert later configurations. Also, when upgrading through a path that is not supported by the configuration translation scripts, you *might* lose all settings except basic access settings, such as administrator accounts and network interface IP addresses. Another rare, but possible, scenario is that the firmware could be corrupted when you are uploading it. For all of those reasons, you should always have local console access during an upgrade. However, in practice, if you read the *Release Notes* and have a reliable connection to the GUI or CLI, it should not be necessary.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. When restoring an encrypted system configuration file, in addition to needing the FortiGate model and firmware version from the time the configuration file was produced, what must you also provide?
 A. The password to decrypt the file
 B. The private decryption key to decrypt the file

2. Which document should you consult to increase the chances of success before upgrading or downgrading firmware?
 A. Cookbook
 B. Release Notes



DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions



Basic Administration



Built-In Servers



Fundamental Maintenance

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify key FortiGate features, services, and built-in servers
- ✓ Identify the differences between the two operating modes, and the relationship between FortiGate and FortiGuard
- ✓ Identify the factory defaults, basic network settings, and console ports
- ✓ Execute basic administration, such as creating administrative users and permissions
- ✓ Execute backup and restore tasks and discuss the requirements for restoring an encrypted configuration file
- ✓ Initiate an upgrade and downgrade of the firmware

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

By mastering the objectives covered in this lesson, you learned how and where FortiGate fits into your network and how to perform basic FortiGate administration.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Security Fabric

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified: 1 June 2020

In this lesson, you will learn about the Fortinet Security Fabric.

DO NOT REPRINT

© FORTINET

Lesson Overview



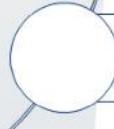
Introduction to the Fortinet Security Fabric



Deploying the Security Fabric



Extending the Security Fabric and Features



Security Fabric Rating and Topology View

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

By demonstrating competence in deploying the Fortinet Security Fabric, using and extending the Security Fabric features, and understanding its topology, you will be able to use the Fortinet Security Fabric effectively in your network.

DO NOT REPRINT

© FORTINET

Introduction to the Fortinet Security Fabric

Objectives

- Define the Fortinet Security Fabric
- Identify why the Security Fabric is required
- Identify the Fortinet devices that participate in the Security Fabric, especially the essential ones

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

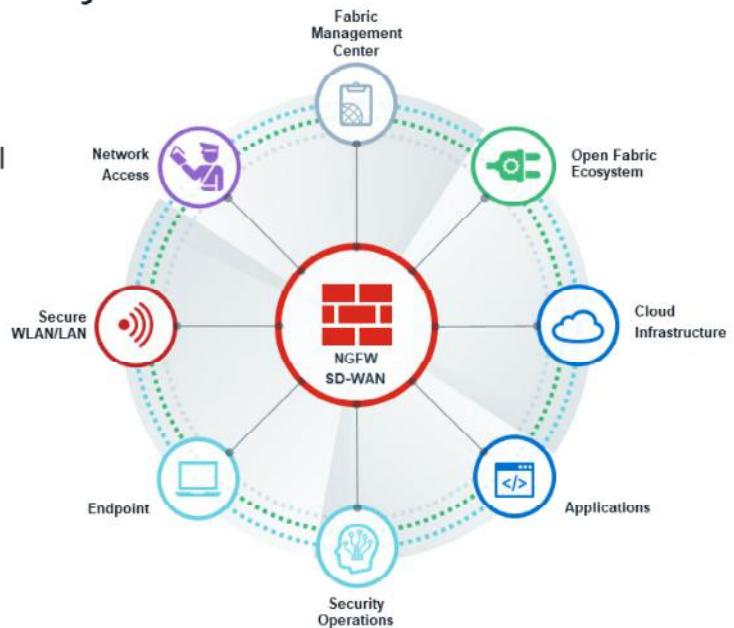
By demonstrating competence in understanding key concepts of the Fortinet Security Fabric, you will better understand the value of the Security Fabric, the servers that comprise it, and how to deploy it.

DO NOT REPRINT

© FORTINET

What is the Fortinet Security Fabric?

- An enterprise solution that enables a holistic approach to network security, whereby the network landscape is visible through a single console and all network devices are integrated into a centrally managed and automated defence
- The Security Fabric has these attributes:
 - Broad
 - Integrated
 - Automated
- The API allows for third-party device integration



FORTINET

© Fortinet Inc. All Rights Reserved.

4

What is the Fortinet Security Fabric?

It is a Fortinet enterprise solution that enables a holistic approach to network security, whereby the network landscape is visible through a single console and all network devices are integrated into a centrally managed and automated defence.

The network devices include all components, from physical endpoints to virtual devices in the cloud. Because devices are centrally managed and are sharing threat intelligence with one another in real time, and are receiving updates from Fortinet at the macro level, your network can quickly identify, isolate, and neutralize threats as they appear.

The Security Fabric has the following attributes:

- **Broad:** It provides visibility of the entire digital attack surface to better manage risk
- **Integrated:** It provides a solution that reduces the complexity of supporting multiple point products
- **Automated:** Threat intelligence is exchanged between network components in real-time allowing for automated response to threats

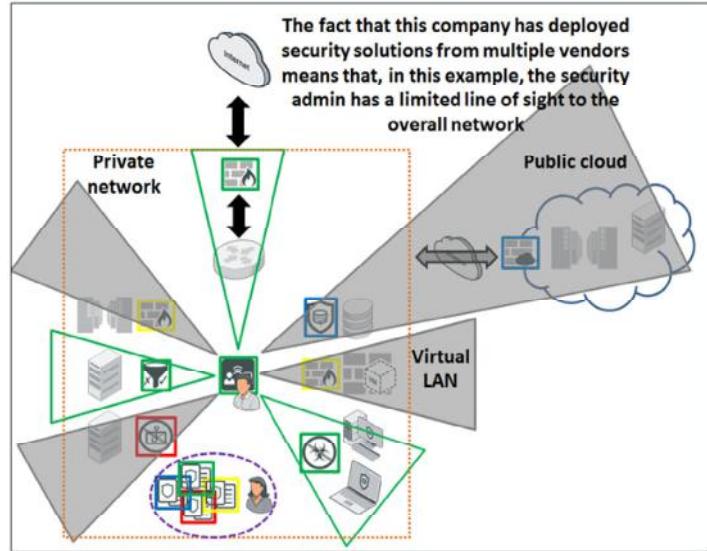
A fourth attribute could be added to this description of the Security Fabric: *open*. The API and protocol are available for other vendors to join and for partner integration. This allows for communication between Fortinet and third-party devices.

DO NOT REPRINT

© FORTINET

Why a Security Fabric?

- Many administrators lack visibility of their network defences, making their networks more susceptible to undetected network infiltration
 - Network complexity and sophisticated malware (soon to be augmented by AI), necessitates a centralized and holistic approach to security



FORTINET

© Fortinet Inc. All Rights Reserved.

5

Why has Fortinet deemed the Security Fabric an essential solution for a robust network defence?

As networks evolved and various new types of threats surfaced, point security products were deployed to address these emerging threats. Oftentimes, these piecemeal solutions were effective, but deploying products using different standards and protocols often meant that defence assets could not be effectively coordinated.

The illustration on the right side of the slide tells a story of a network that has deployed security solutions from four different vendors. The administrator at the center, working from the security console, has visibility into only some of the security solutions. This lack of visibility of the entire network defence is a serious flaw, and could allow a foreign infiltrator to breach network defences undetected.

The sheer complexity of today's networks compounds this problem. In addition, increasingly sophisticated malware has an expanding attack surface on which to exploit, because networks have broken out of the confines of a traditional network perimeter and have expanded to virtualized networks and public clouds. Add to this mix, the ever growing numbers of unmanaged devices, as a result of bring-your-own-device(BYOD) programs, and you have the perfect security storm.

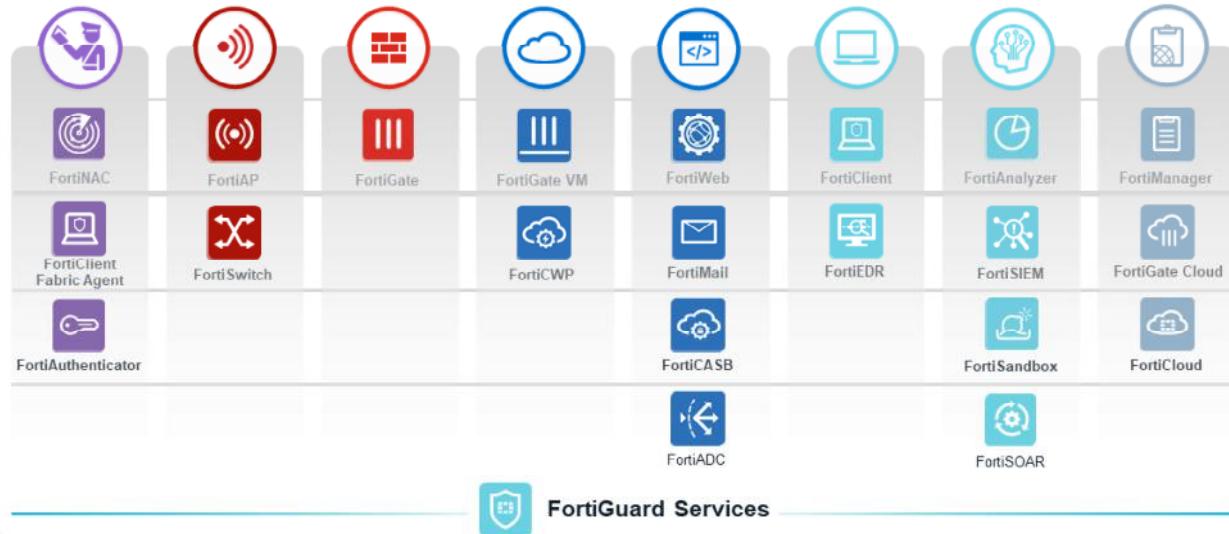
The most feasible solution is to build a centrally managed, holistic approach to security, whereby you have a clear line of sight to all potential infiltration points and can coordinate defences to contain and neutralize network breaches.

DO NOT REPRINT

© FORTINET

Security Fabric Products

- Different consumption models available



FORTINET

© Fortinet Inc. All Rights Reserved.

6

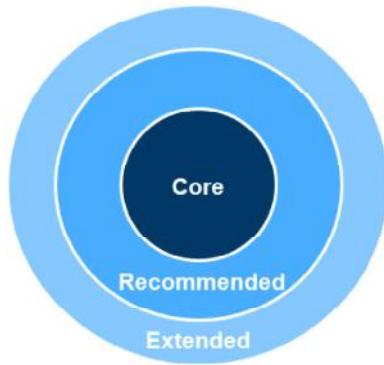
As shown on this slide, the Fortinet Security Fabric offers eight solutions: Network Access, Secure WLAN/LAN, Public and Private Cloud Infrastructure, Applications, Endpoint, Security Operations, Open Fabric Ecosystem, and Fabric Management Center. Each of these solutions is based on specific use cases and involve the integration of specific Fortinet products.

The Fortinet Security Fabric offers network security with FortiGate, IPS, VPN, SDWAN. It also offers multi-cloud strategy across public clouds, private clouds, and hybrid clouds, and SaaS. It also offers quite a sophisticated endpoint offering ranging from the Fabric Agent all the way up to full endpoint protection, email security, web application security, which is growing very fast in the cloud, secure access across more distributed enterprises and SD-WAN environments, advanced threat protection, management and analytics, and SIEM.

All of these are underscored and supported by FortiGuard Services that deliver AI-powered intelligence and protection across the Security Fabric.

DO NOT REPRINT**© FORTINET**

Devices That Comprise the Security Fabric



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



© Fortinet Inc. All Rights Reserved.

7

FortiGate and FortiAnalyzer creates the core of the security fabric. To add more visibility and control, Fortinet recommends adding FortiManager, FortiAP, FortiClient, FortiSandbox, FortiMail, and FortiSwitch. The solution can be extended by adding other network security devices.

DO NOT REPRINT

© FORTINET

Knowledge Check

- 1. What is the Fortinet Security Fabric?**
 A. A Fortinet solution that enables the communication and visibility between devices of your network
 B. A device that can manage all your firewalls

- 2. What combination of devices must participate in the Security Fabric?**
 A. A FortiAnalyzer and two or more FortiGate devices
 B. A FortiMail and two or more FortiGate devices



© Fortinet Inc. All Rights Reserved.

8

DO NOT REPRINT

© FORTINET

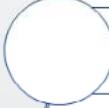
Lesson Progress



Introduction to the Fortinet Security Fabric



Deploying the Security Fabric



Extending the Security Fabric and Features



Security Fabric Rating and Topology View

Good job! You now understand the basics of the Fortinet Security Fabric. Next, you'll learn how to deploy the Security Fabric in your network environment.

DO NOT REPRINT

© FORTINET

Deploying the Security Fabric

Objectives

- Understand how to implement the Security Fabric
- Configure the Security Fabric on root and downstream FortiGate devices
- Understand how device detection works
- Understand how to extend your existing Security Fabric

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

By demonstrating competence in the deployment of the Fortinet Security Fabric, you will better understand the value of the Security Fabric and how it helps to manage all your network devices more efficiently.

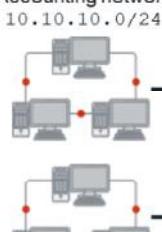
DO NOT REPRINT

© FORTINET

How Do You Implement the Security Fabric?

Here is an example of a simple network using only the core Security Fabric components.

Accounting network
10.10.10.0/24



Accounting ISFW

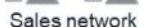
FortiAnalyzer

Marketing network
10.10.200.0/24



Marketing ISFW

Sales network
10.10.35.0/24



Sales ISFW

External
Port 10
Port 11
Port 12

There is a FortiAnalyzer and one next-generation firewall (NGFW). This FortiGate will be configured as the *root* firewall. In this example, the alias for the firewall is *External*.

There are three internal segmentation firewalls (ISFWs) that segregate the WAN into logical components and allow your network to contain a threat, should a breach occur.

© Fortinet Inc. All Rights Reserved.

11

FORTINET

In this simple network that comprises only the core devices of a Security Fabric, there is one FortiAnalyzer and one next-generation firewall (NGFW) FortiGate. This implementation example is intended to be a high-level view only. For more detail, see docs.fortinet.com. The FortiGate device named External is acting as the edge firewall and will also be configured as the *root* firewall within the Security Fabric. Downstream from the root firewall there are three internal segmentation firewalls that compartmentalize the WAN in order to contain a breach and control access to various LANs. In this example, there are Accounting, Marketing, and Sales LANs.

DO NOT REPRINT

© FORTINET

Configure the Security Fabric on Root FortiGate

The screenshot shows the FortiGate UI for configuring the Security Fabric on the root FortiGate. It includes three windows:

- Main Configuration Window:** Shows the "Edit Fabric Connector" screen under "Security Fabric > Fabric Connectors". It has sections for "Status" (Enabled), "Fabric name" (e.g., "Security Fabric"), and "Allow other Security Fabric devices to join". A callout points to the "Status" section with the text "Enable Security Fabric Connection and select interfaces". Another callout points to the "Fabric name" field with the text "Fabric name for the Security Fabric".
- Fabric Analyzer Settings Window:** Shows the "Edit Fabric Connector" screen under "Core Network Security". It has sections for "FortiAnalyzer Settings" (Status, IP address, Upload option, Allow access to FortiGate REST API, Verify FortiAnalyzer certificate) and "FortiAnalyzer Logging" (Real Time, Every Minute, Every 5 Minutes). A callout points to the "IP address" field with the text "FortiAnalyzer IP address".
- Authorization Window:** Shows the "FortiGate Authorization" screen. It lists serial numbers (e.g., FGVM010000077646) and actions (e.g., Accept, Deny). A callout points to the "Action" column with the text "Preauthorizing the downstream FortiGate devices to join the Security Fabric".

At the bottom left is the FORTINET logo. At the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 12.

First, on the root FortiGate, you must enable **Security Fabric Connection** in the interfaces facing any downstream FortiGate. If you select **Serve as Fabric Root**, you also need to configure the FortiAnalyzer IP address. Then, you need to configure a fabric name for the Security Fabric. This FortiAnalyzer configuration will be pushed to all the downstream FortiGate devices. All downstream FortiGate devices send logs directly to FortiAnalyzer.

You can also preauthorize your downstream devices by adding the serial number of the device. When you add the serial number of a Fortinet device to the trusted list on the root FortiGate, the device can join the Security Fabric as soon as it connects. After you authorize the new FortiGate, additional connected FortiAP and FortiSwitch devices automatically appear in the topology tree. On the topology tree, it's easier for you to authorize them with one click.

DO NOT REPRINT

© FORTINET

Configure the Security Fabric on the Downstream FortiGate

Downstream FortiGate Security Fabric > Fabric Connectors

Select Join Existing Fabric

Add Root FortiGate IP address

Enable Security Fabric Connection on downstream FortiGate

Root FortiGate pushes its FortiAnalyzer configuration to all downstream FortiGate devices

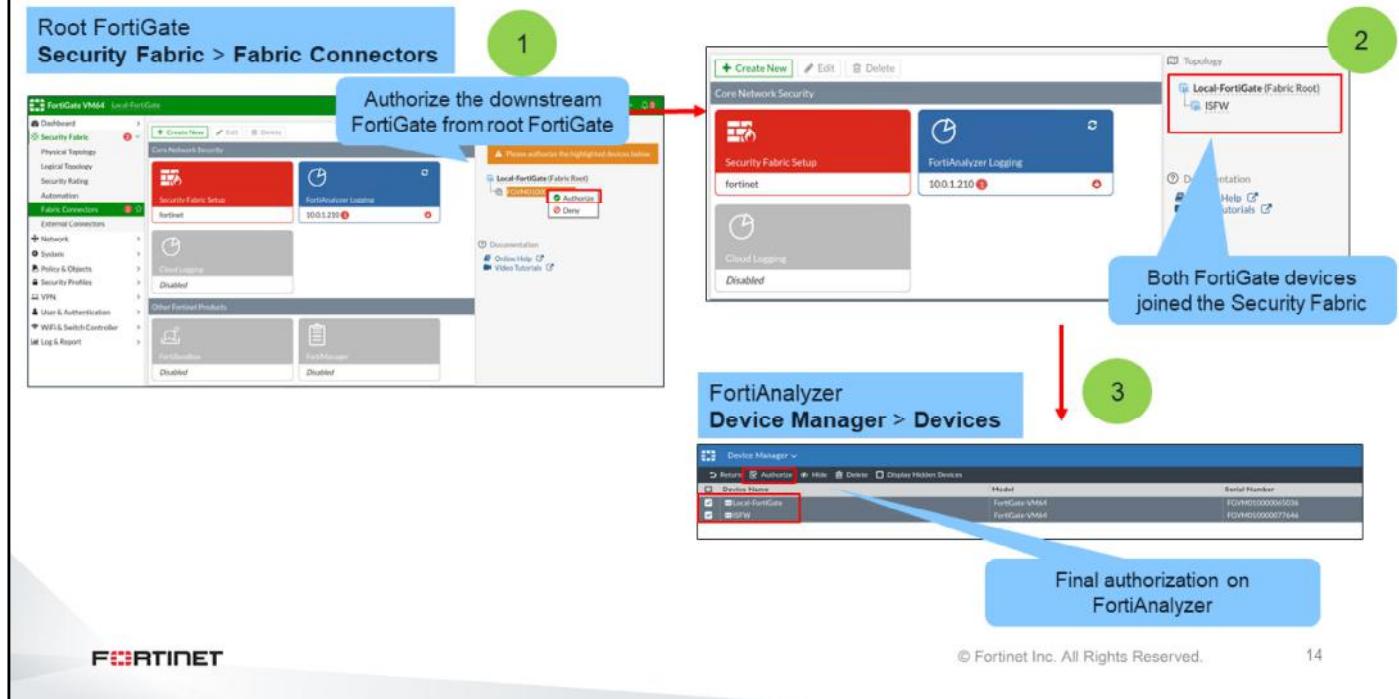
© Fortinet Inc. All Rights Reserved. 13

The second step in implementing the Security Fabric is configuring the downstream Fortinet devices. On the downstream FortiGate devices, you must enable **Security Fabric Connection** and **Device Detection** on the interfaces facing the downstream FortiGate devices. On the **Fabric Connectors** page, select **Join Existing Fabric** and add the root (upstream) FortiGate IP address. The root FortiGate pushes its FortiAnalyzer configuration to all downstream FortiGate devices.

DO NOT REPRINT

© FORTINET

Authorizing Devices



The third step in implementing the Security Fabric is to authorize the downstream FortiGate device on the both root FortiGate and the FortiAnalyzer. Click the serial number of the highlighted downstream FortiGate device and select **Authorize**. After few seconds, the downstream FortiGate will join the Security Fabric. In order to complete the full Security Fabric process, you will need to authorize all your devices on the FortiAnalyzer. From the FortiAnalyzer **Device Manager** section, select all your devices in the Security Fabric and click **Authorize**. After few seconds, you will notice all your authorized devices join the Security Fabric.

DO NOT REPRINT

© FORTINET

Synchronizing Objects Across Security Fabric

Root FortiGate
Security Fabric > Fabric Connectors

1

2

3

4

5

6

One downstream FortiGate device is out of sync

Objects can be synchronized by Automatic or Manual mode

Click "Rename All Objects" to rename objects on Remote-FortiGate using the FortiGate name as a suffix.

© Fortinet Inc. All Rights Reserved. 15

When the Security Fabric is enabled, various objects such as addresses, services, and schedules are synced from the upstream FortiGate to all downstream devices by default.

In this example, the notifications icon displays a message that Firewall objects are not synchronized with all the FortiGates in the Fabric. In the topology tree, **Remote-FortiGate** is highlighted in yellow because it is out of sync.

In the example shown on this slide, you will examine how to resolve a syncing conflict.

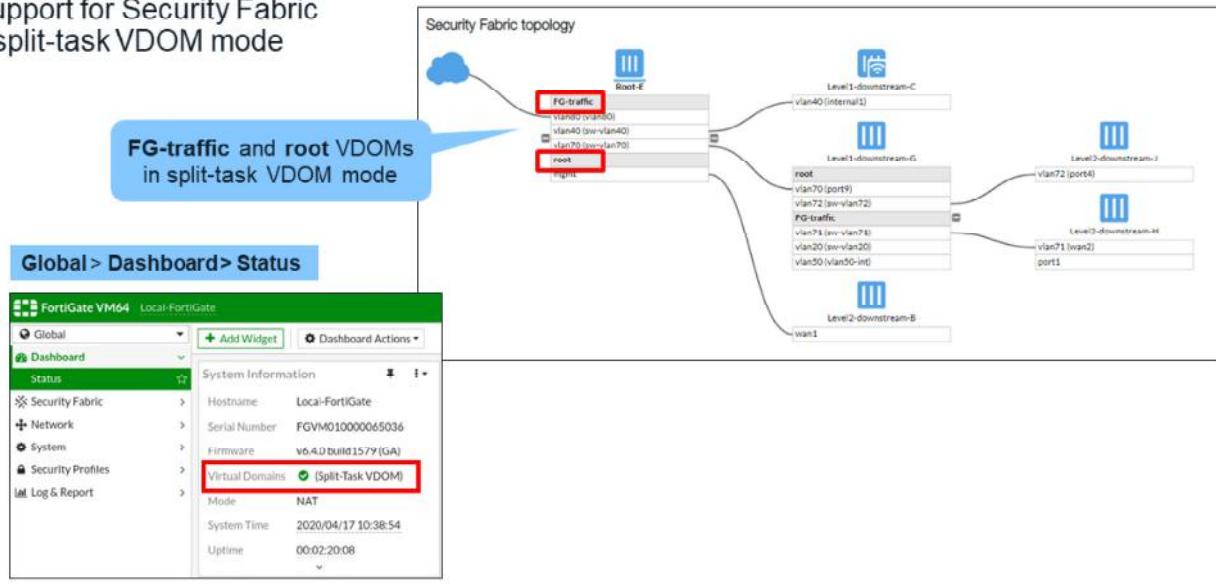
1. The notification icon displays this message: Firewall objects are not synchronized with all FortiGates in the Fabric. Click **Open Synchronization Wizard**
2. On the **Review FortiGates** page, the **Remote-Fortigate** is highlighted in yellow, with status of **Out of sync**. Click **Next**.
3. On the **Review Tables** page, the status of the **Address** object is **Needs manual intervention**. Click **Resolve Conflicts**.
4. On the **Resolve Conflicts** page, you can see that both the root FortiGate and downstream FortiGate devices contain the **Local_Subnet** object (with different IP address/subnet schema on each device), causing a status of **Name Conflict**. In the **Strategy** field, there are two options to resolve the conflict: **Automatic** and **Manual**. If you select **Automatic**, as shown in this example, you can then click **Rename All Objects**.
5. **Remote-FortiGate** is appended to the name of the downstream FortiGate device **Local Subnet** address object and the status has change to **Resolved**.
6. On the last page of the wizard, a message indicates: All FortiGates have been synced.

DO NOT REPRINT

© FORTINET

Split-Task VDOM

- Support for Security Fabric in split-task VDOM mode



FORTINET

© Fortinet Inc. All Rights Reserved.

16

Starting with FortiOS 6.2, you can enable FortiGate security fabric in split-task VDOM mode. If you enable split-task VDOM mode on the upstream FortiGate device, it can allow downstream FortiGate devices to join the Security Fabric in the root and FG-traffic VDOMs. If split-task VDOM mode is enabled on the downstream FortiGate, it can only connect to the upstream FortiGate through the downstream FortiGate interface on the *root* VDOM.

Telemetry settings are shown in both global and VDOM contexts, but in VDOM context, only the topology and FortiTelemetry-enabled interface fields are shown.

DO NOT REPRINT

© FORTINET

Split-Task VDOM (Contd)

The image contains three screenshots of the FortiGate Management Interface (FortiGate UI) illustrating different Physical Topology views:

- Global > Physical Topology:** Shows the global physical topology where all FortiGate devices in the same Security Fabric are visible.
- root > Physical Topology:** Shows the root FortiGate and its downstream devices connected to the root VDOM.
- FG-traffic > Physical Topology:** Shows the root FortiGate and its downstream devices connected to the current selected VDOM.

Annotations provide instructions for each view:

- Click Global > Physical Topology to see the root FortiGate and all downstream FortiGate devices in the same Security Fabric**
- Click FG-Traffic > Physical Topology to see the root FortiGate and all downstream FortiGate devices connected to the current VDOM**
- Click root > Physical Topology to see the root FortiGate and the downstream FortiGate connected to the root VDOM**

At the bottom left is the **FORTINET** logo, and at the bottom right is the copyright notice **© Fortinet Inc. All Rights Reserved.** and page number **17**.

You can click **Global > Physical Topology** to see the root FortiGate and *all* downstream FortiGate devices that are in the same Security Fabric as the root FortiGate. You can click **root > Physical Topology** or **FG-Traffic > Physical Topology** to see the root FortiGate and *only* the downstream FortiGate devices that are connected to the current selected VDOM on the root FortiGate.

DO NOT REPRINT

© FORTINET

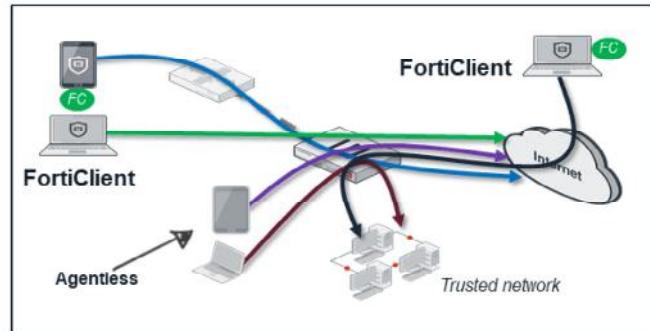
Device Identification—Agentless vs. Agent

Agentless

- Useful feature for the Security Fabric topology view
- Requires *direct* connectivity to FortiGate
- Detection methods:
 - HTTP user agent
 - TCP fingerprinting
 - MAC address vendor codes
 - DHCP
 - Microsoft Windows browser service (MWBS)
 - SIP user agent
 - Link Layer Discovery Protocol (LLDP)
 - Simple Service Discovery Protocol (SSDP)
 - QUIC
 - FortiOS-VM detection
 - FortiOS-VM vendor ID in IKE messages
 - FortiOS-VM vendor ID in FortiGuard web filter and spam filter requests

Agent (FortiClient)

- Location and infrastructure independent



FORTINET

© Fortinet Inc. All Rights Reserved.

18

Device identification is an important component in the Security Fabric. FortiGate detects most of the third-party devices in your network and adds them into the topology view in the Security Fabric. There are two device identification techniques: with an agent and without an agent (agentless).

Agentless identification uses traffic from the device. Devices are indexed by their MAC address and there are various ways to identify devices, such as HTTP user-Agent header, TCP fingerprint, MAC address OUI, and FortiOS-VM detection methods, to name a few. Agentless device identification is only effective if FortiGate and the workstations are directly connected network segments, where traffic is sent directly to FortiGate, and there is no intermediate router or Layer 3 device between FortiGate and the workstations.

Note that FortiGate uses a *first come, first served* approach to determine the device identity. For example, if a device is detected by the HTTP user agent, FortiGate updates its device table with the detected MAC address and scanning stops as soon as the type has been determined for that MAC address.

Agent-based device identification uses FortiClient. FortiClient sends information to FortiGate, and the device is tracked by its unique FortiClient user ID (UID).

DO NOT REPRINT

© FORTINET

Device Identification (Contd)

Enable Device Detection on interface(s)

Network > Interfaces

Edit Interface

Name: port3
Type: Physical Interface
Role: DMZ

Address
Addressing mode: Manual/DHCP
IP Netmask: 10.0.1.254/255.255.255.0

Administrative access
IPv4: HTTPS, FMG-Access, TELNET, Security Fabric Connection, PING, SSH, FTM, SNMP, RADIUS Accounting

Receive LLDP: Use VDOM Setting, Enable/Disable
Transmit LLDP: Use VDOM Setting, Enable/Disable

Network
Device detection:

Security Fabric > Logical Topology

Windows PC
10.0.1.100

Internet → port3 → Local-FortiGate → port1 → Windows PC → port1 → Local-HOST → Remote-FortiGate → To-Remote-HOST → To-Local-HOST

Windows PC detected upon traffic from the PC to the FortiGate

Enable Device Detection

© Fortinet Inc. All Rights Reserved. 19

By default, FortiGate uses device detection (passive scanning), which runs scans based on the arrival of traffic.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What are the two mandatory settings of the Security Fabric configuration?
 A. Fabric name and Security Fabric role
 B. Fabric name and FortiManager IP address

2. From where do you authorize a device to participate in the Security Fabric?
 A. From the downstream FortiGate
 B. From the root FortiGate



© Fortinet Inc. All Rights Reserved.

20

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to the Fortinet Security Fabric



Deploying the Security Fabric



Extending the Security Fabric and Features



Security Fabric Rating and Topology View

Good job! You now know how to deploy the Security Fabric. Next, you'll learn about Security Fabric features and how to extend the Security Fabric in your network environment.

DO NOT REPRINT

© FORTINET

Extending the Fabric and Features

Objectives

- Extend the Security Fabric across your network
- Understand automation stitches and threat responses
- Configure external connectors
- Understand the Security Fabric status widgets

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

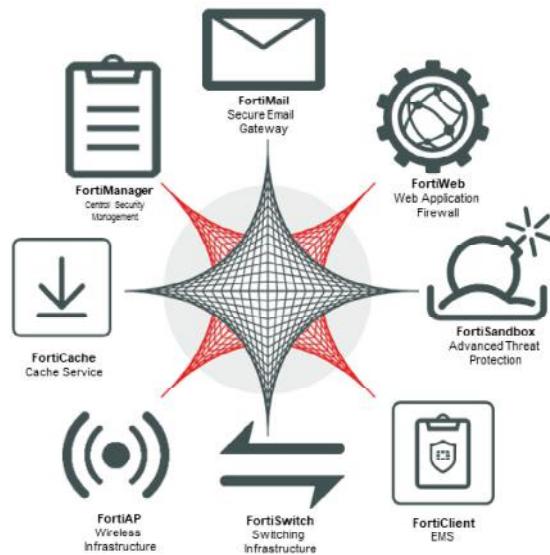
By demonstrating competence in the extending the Fortinet Security Fabric, you will better understand the value of the Security Fabric and how it helps to manage all your network devices from a single point of device.

DO NOT REPRINT

© FORTINET

Extending the Fabric

- Central management integration
 - FortiManager
- FortiMail integration
 - FortiMail
- Web application integration
 - FortiCache
 - FortiWeb
- FortiClient integration
 - FortiClient EMS
- Advanced threat protection integration
 - FortiSandbox
- Access device integration
 - FortiAP
 - FortiSwitch



FORTINET

© Fortinet Inc. All Rights Reserved.

23

Fortinet recommends using a FortiManager for centralized management of all FortiGate devices, and access devices in the security fabric. You can integrate FortiSwitch devices, and FortiAP devices to extend the Security Fabric down to the access layer. You can also extend the Security Fabric by integrating FortiMail, FortiWeb, FortiCache, FortiSandbox, and FortiClient EMS.

DO NOT REPRINT

© FORTINET

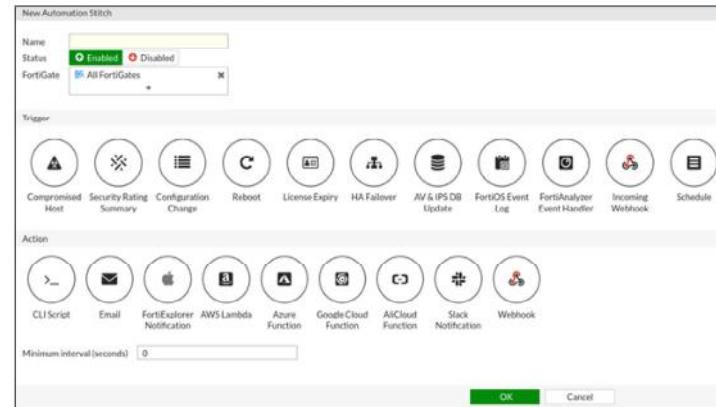
Automation Stitches

AUTOMATION STITCH



- Configure various automated actions based on triggers
- Event trigger and one or more actions
- Configure the **Minimum interval** setting to make sure you don't receive repeat alert notifications about the same event

Security Fabric > Automation



FORTINET

© Fortinet Inc. All Rights Reserved.

24

Administrator-defined automated work flows (called stitches) use if/ then statements to cause the FortiOS to automatically respond to an event in a preprogrammed way. Because this workflow is part of the Security Fabric, you can set up if/then statements for any device in the Security Fabric. However, the Security Fabric is not required to use stitches.

Each automation stitch pairs an event trigger and one or more actions. Automation stitches allow you to monitor your network and take appropriate action when the Security Fabric detects a threat. You can use Automation stitches to detect events from any source in the Security Fabric and apply actions to any destination.

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

DO NOT REPRINT**© FORTINET**

Automated Threat Response



- Configure automated threat response
- Requires FortiAnalyzer IoC reporting
- Various remediation options:
 - Access layer quarantine using FortiSwitch or FortiAP
 - FortiClient quarantine
 - IP ban

**FORTINET**

© Fortinet Inc. All Rights Reserved.

25

You can configure the **Compromised Host** trigger to create an automated threat response stitch. This trigger uses indicator of compromise (IoC) event reporting from FortiAnalyzer. Based on the **Threat level threshold** setting, you can configure the stitch to take different remediation steps:

- Quarantine the compromised host at the FortiSwitch or FortiAP
- Quarantine FortiClient on the compromised host using FortiClient EMS
- Ban the IP

You can also click **Monitor > Quarantine Monitor** to view quarantined and banned IP addresses. Quarantined addresses are automatically removed from quarantine after a configurable period of time. Banned IP addresses can be removed from the list only by administrator intervention.

DO NOT REPRINT

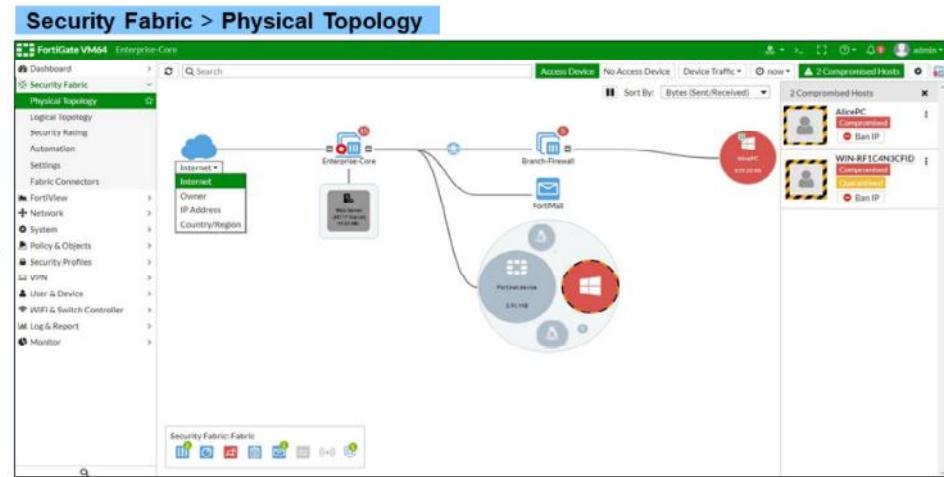
© FORTINET

Automated Threat Response (Contd)

NOTIFICATIONS



- Output notifications in various ways such as iOS Push or on the GUI dashboard
- Integrate with IFTTT and other cloud services



FORTINET

© Fortinet Inc. All Rights Reserved.

26

You can also view compromised hosts on the FortiGate GUI and get output notifications in various ways such as iOS push. This feature is integrated with IFTT.

DO NOT REPRINT**© FORTINET**

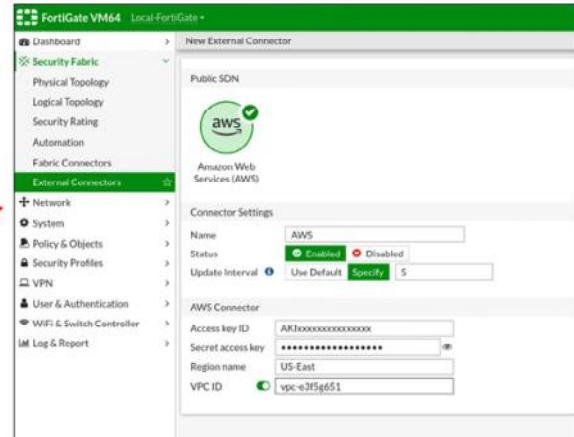
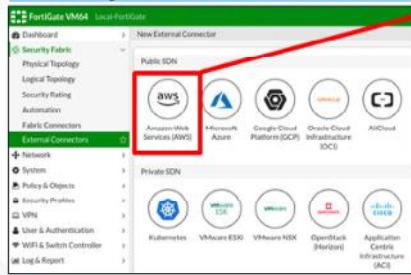
External Connectors

- Security Fabric multi-cloud support adds external connectors to the Security Fabric configuration

Allow you to integrate

- Amazon Web Services (AWS)
- Microsoft Azure
- Oracle Cloud Infrastructure (OCI)
- Google Cloud Platform (GCP)

Security Fabric > External Connectors



© Fortinet Inc. All Rights Reserved.

27

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

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

FortiGate VM for Microsoft Azure also supports cloud-init and bootstrapping.

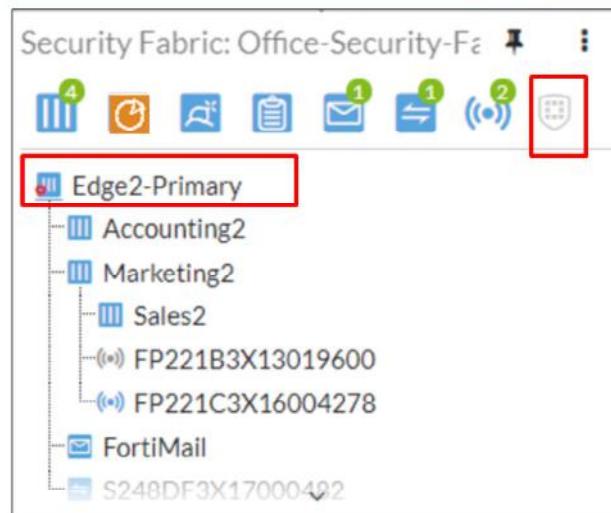
DO NOT REPRINT

© FORTINET

The Security Fabric Status Widget

- The name of your Security Fabric
- Icons indicating the other Fortinet devices that can be used in the Security Fabric
- The names of the FortiGate devices in the Security Fabric

Dashboard > Status > Security Fabric widget



FORTINET

© Fortinet Inc. All Rights Reserved.

28

The **Security Fabric Status** widget shows a visual summary of many of the devices in the Security Fabric. You can hover over the icons at the top of the widget to get a quick view of the status of the Security Fabric, including the status of FortiTelemetry and devices in the Security Fabric. You can click to authorize FortiAP and FortiSwitch devices that are connected to an authorized FortiGate.

Icons represent the other Fortinet devices that can be used in the Security Fabric:

- Devices in blue are connected in your network.
- Devices in gray are unauthorized devices that are connected in your network.
- Devices in red are not detected in your network, but are recommended for the Security Fabric.
- An attention icon indicates a FortiGate or FortiWiFi waiting for authorization.

DO NOT REPRINT

© FORTINET

The Security Posture Widget

- Latest security rating for your Security Fabric
- Security posture score by percentile
- Can be specific to your organization region or all regions
- Must have a valid security rating license



FORTINET

© Fortinet Inc. All Rights Reserved.

29

The **Security Posture** widget shows the latest security rating for your Security Fabric. You can configure the widget to show either how your organization's Security Fabric rating compares to the ratings of other organizations in the same industry, or to organization in all industries. Your organization's industry is determined from your FortiCare account. You can also configure the widget to show scores that are specific to your organization's region or all regions. The widget shows the security rating score by percentile. To receive a security rating score, all FortiGate devices in the Security Fabric must have a valid security rating license.

The security rating license is a FortiGuard service. You must purchase a license to access to all the latest features. Security audit checks from FortiOS 5.6 will continue to run, but the following upgrades are available only when you purchase a security rating license:

- FortiGuard updates
- The ability to run security rating checks across each licensed device or all FortiGates in the Security Fabric from the root FortiGate
- New 6.0 rating checks
- The ability to submit rating scores to FortiGuard and receive security rating scores from FortiGuard for ranking customers by percentile

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Why should an administrator extend the Security Fabric to other devices?
 A. To provide a single pane of glass for management and reporting purposes
B. To eliminate the need to purchase licenses for FortiGate devices in the Security Fabric

2. What is the purpose of Security Fabric external connectors?
 A. External connectors allow you to integrate multi cloud support with the Security Fabric
B. External connectors allow you to connect the FortiGate command line interface (CLI)

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to the Fortinet Security Fabric



Deploying the Security Fabric



Extending the Security Fabric and Features



Rating Service and Topology View

Good job! You now know how to extend the Security Fabric and its features. Next, you'll learn about the Security Fabric Rating service and topology view.

DO NOT REPRINT

© FORTINET

Rating Service and Topology View

Objectives

- Understand the Security Fabric rating service
- View and run the Security rating service
- Understand difference between physical and logical topology views

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

By demonstrating competence in the Fortinet Security rating service and topology views, you should be able to have clear visibility of your network devices.

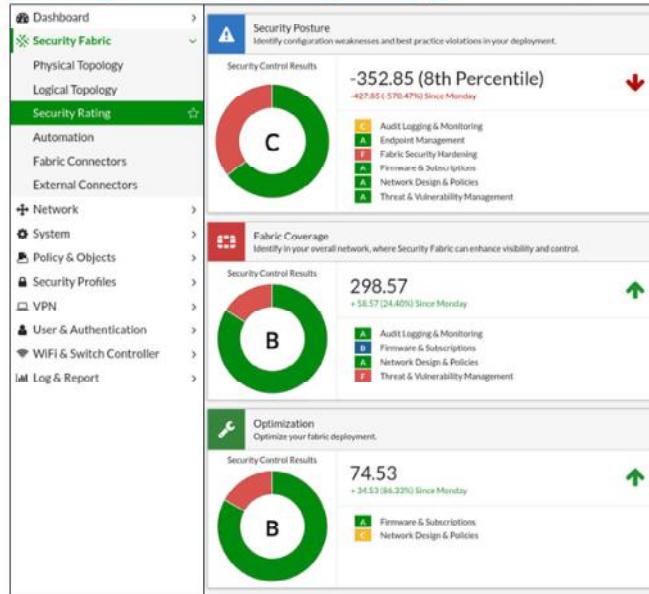
DO NOT REPRINT

© FORTINET

Security Fabric Rating

- Three major scorecards:
 - **Security Posture**
 - **Fabric Coverage**
 - **Optimization**
- Provide executive summaries of the three largest areas of security focus
- Clicking a scorecard drills down to report of itemized results and compliance recommendations

Security Fabric > Security Rating



© Fortinet Inc. All Rights Reserved.

33

FORTINET

Security rating is a subscription service that requires a security rating license. This service now provides the ability to perform many *best practices*, including password checks, to audit and strengthen your network security.

The **Security Rating** page is separated into three major scorecards:

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

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

The scorecards show an overall letter grade and breakdown of the performance in sub-categories. Clicking a scorecard drills down to a detailed report of itemized results and compliance recommendations.

The point score represents the net score for all passed and failed items in that area. The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies. You can click **FSBP** and **PCI** to reference the corresponding standard.

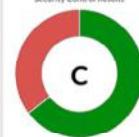
DO NOT REPRINT

© FORTINET

Security Posture

Security Fabric > Security Rating > Security Posture

Security Control Results:



Grades:

- Audit Logging & Monitoring
- Endpoint Management
- Fabric Security Hardening

Security Control	Devices	Score	Result	Compliance
Unsecure Protocol - HTTP	12	100	Failed	FSBP SH01.2
Log Capacity Management (Local Device)	12	100	Failed	FSBP AL05.1
PortClient Vulnerabilities	10	100	Under Development	FSBP EM01.2
Default Port HTTPS	12	100	Failed	FSBP SH01.8

Report Details:

- Score: -352.85 (8th Percentile)
- Last Run: 6 second(s) ago
- Runups: 6
- Trends:

 - High: 295
 - Low: -609
 - Change: -570.47%

Fabric Security Hardening (SH)

Recommendations:

- Backup configuration before applying
- Disable HTTP access on the following interfaces:
 - port1
 - port3

Apply

The Security Rating Score helps you to identify the security issues in your network and to prioritize your tasks

Security issues that are labelled **Apply**, can be resolved immediately

Identifies critical security gaps

© Fortinet Inc. All Rights Reserved.

34

Click on the **Security Posture** scorecard on the **Security Rating** page to expand the scorecard and see more details.

The security posture service now supports the following:

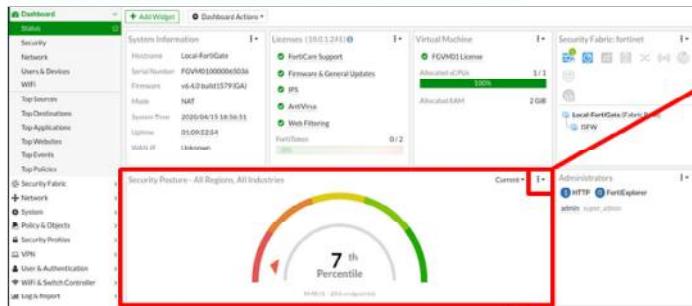
- Customer rankings by percentile using security audit (FortiGuard data): Security rating now supports sending results to FortiGuard, and receiving statistics from FortiGuard. Results are displayed to customer in the form of percentile.
- Security audits running in the background, not just on demand, when an administrator is logged into the GUI. When you view the security audit page, the latest saved security audit data is loaded. From the GUI you can run audits on demand and view results for different devices in the Security Fabric. You can also view all results or just failed test results.
- New security checks that can help you make improvements to your organization's network. These results include enforcing password security, applying recommended login attempt thresholds, encouraging two factor authentication, and more.

DO NOT REPRINT

© FORTINET

FortiGuard Security Rating Service

Dashboard > Status > Security Posture



Different customer FortiGates with improved ratings



- Enable or disable security checks using CLI:

```
config system global
    set security-rating-run-on-schedule [enable/disable]
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

35

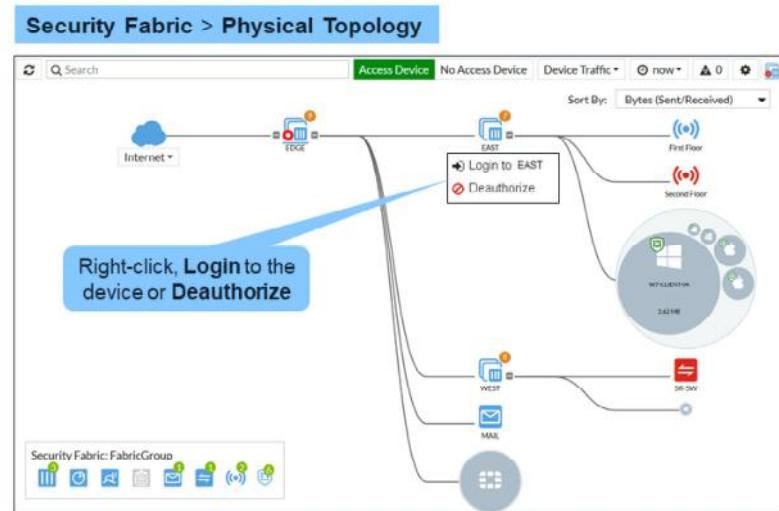
The Security rating service reports the security posture score per the Security Fabric group. FortiGuard Security Rating Service is a subscription-based service that takes the generated report and obtains analysis by FortiGuard. It compares security score results within the industry that the fabric group belongs to. All FortiGate devices in the group need to have FortiGuard Security Rating Service and the score can be obtained only on the Security Fabric root node. The score can be obtained after the security rating report is generated. The scores are presented as percentiles, and are based on the industry, the size of the organization, and the region.

DO NOT REPRINT

© FORTINET

Topology Views

- Authorize or deauthorize access devices (FortiSwitch, FortiAPs)
- Ban or unban compromised clients
- Some device management tasks:
 - Login
 - Deauthrize



FORTINET

© Fortinet Inc. All Rights Reserved.

36

You can view the Security Fabric topology on the FortiGate GUI, from the **Security Fabric** menu. You can select the **Physical Topology** or **Logical Topology** view. To view the complete network, you must access the topology views on the root FortiGate in the Security Fabric.

The **Physical Topology** view displays your network as a bubble chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to resize it and view more information about the device.

The **Logical Topology** view is similar to the **Physical Topology** view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric.

DO NOT REPRINT**© FORTINET**

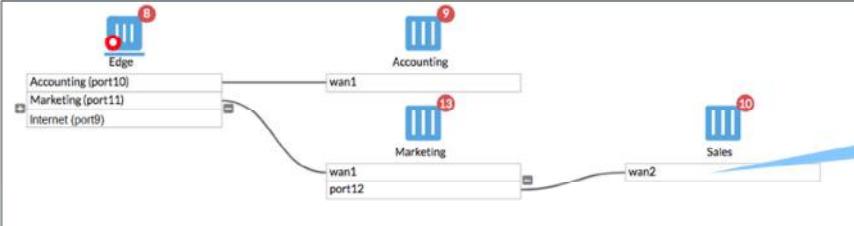
Topology Views (Contd)

Security Fabric > Physical Topology



Visualization of access layer devices in the Security Fabric

Security Fabric > Logical Topology



Information about the interfaces that each device in the Security Fabric connects

FORTINET

© Fortinet Inc. All Rights Reserved.

37

This slide shows the difference between the **Physical Topology** view and the **Logical Topology** view.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which one is a part of the Security Rating scorecard?
 - A. Firewall Policy
 - B. Optimization

2. From which view can an administrator deauthorize a device from the Security Fabric?
 - A. From the physical topology view
 - B. From the Fortiview



© Fortinet Inc. All Rights Reserved.

38

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to the Fortinet Security Fabric



Deploying the Security Fabric



Extending the Security Fabric and Features



Rating Service and Topology View

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Define the Fortinet Security Fabric
- ✓ Identify why the Security Fabric is required
- ✓ Identify the Fortinet devices that participate in the fabric, especially the essential ones
- ✓ Understand how to implement the Security Fabric
- ✓ Configure the Security Fabric on root and downstream FortiGate
- ✓ Understand how the device detection works
- ✓ Understand how to extended your existing Security Fabric
- ✓ Extend the Security Fabric across your network
- ✓ Understand automation stiches and threat responses
- ✓ Configure fabric connectors
- ✓ Understand the Security Fabric status widgets
- ✓ Understand Security Fabric Rating service
- ✓ View and run Security Rating service
- ✓ Understand difference between Physical and Logical topology view

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and use the Fortinet Security Fabric.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Firewall Policies

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified 29 May 2020

In this lesson, you will learn about firewall policies and how to apply them to allow and deny traffic passing through FortiGate. At its core, FortiGate is a firewall, so almost everything that it does to your traffic is linked to your firewall policies.

DO NOT REPRINT

© FORTINET

Lesson Overview



Firewall Policies

Configuring Firewall Policies

Managing Firewall Policies

Best Practices and Troubleshooting

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

DO NOT REPRINT

© FORTINET

Firewall Policies

Objectives

- Identify components of firewall policies
- Identify how FortiGate matches traffic to firewall policies

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

By demonstrating competence in identifying the different components of firewall policies, and recognizing how FortiGate matches traffic with firewall policies and takes appropriate action, you will have a better understanding of how firewall policies interact with network traffic.

DO NOT REPRINT

© FORTINET

What Are Firewall Policies?

- Policies define:
 - Which traffic matches them
 - How to process matching traffic
- When a new IP session packet arrives, FortiGate:
 - Starts at the top of the list to look for a policy match
 - Applies the first matching policy
- Implicit Deny**
 - No matching policy? FortiGate drops packet

The screenshot shows the FortiGate configuration interface under 'Policy & Objects > Firewall Policy'. It displays four rows of policy entries:

- Row 2: LAN (port3) → ISP1 (port1). Conditions: LOCAL_SUBNET, all, always, ALL, ACCEPT, Enabled. Actions: default, deep-inspection.
- Row 3: LAN (port3) → ISP2 (port2). Conditions: LOCAL_SUBNET, all, always, ALL, ACCEPT, Enabled. Actions: default, deep-inspection.
- Row 4: Implicit. Conditions: all, always, ALL, DENY. Actions: default, deep-inspection. Status: Disabled.

A blue callout bubble labeled 'Implicit Deny' points to the fourth row. A red arrow points from the right edge of the slide towards the bottom of the screenshot.

FORTINET

© Fortinet Inc. All Rights Reserved.

4

To begin, you will learn about what firewall policies are.

Firewall policies define which traffic matches them and what FortiGate does when traffic does match.

Should the traffic be allowed? Initially, FortiGate bases this decision on simple criteria, such as the source of the traffic. Then, if the policy does not block the traffic, FortiGate begins a more computationally expensive security profile inspection—often known as unified threat management (UTM)—such as antivirus, application control, and web filtering, if you've chosen it in the policy. Those scans could block the traffic if, for example, it contains a virus. Otherwise, the traffic is allowed.

Will network address translation (NAT) be applied? Authentication required? Firewall policies also determine the answers to these questions. After processing is finished, FortiGate forwards the packet toward its destination.

FortiGate looks for the matching firewall policy from *top to bottom* and, if a match is found, the traffic is processed based on the firewall policy. If no match is found, the traffic is dropped by the default **Implicit Deny** firewall policy.

DO NOT REPRINT**© FORTINET**

Components and Policy Types

Objects used by policies

- Interface and zone
- Address, user, and Internet service objects
- Service definitions
- Schedules
- NAT rules
- Security profiles

Policy types

- IPv4, IPv6
- Virtual wire pair (IPv4, IPv6)
- Proxy
- Multicast
- Local In Policy
(Origin and destination is FortiGate itself)
- DoS (IPv4, IPv6)
- Traffic shaping



Policy & Objects	
Firewall Policy	
Firewall Virtual Wire Pair Policy	
NAT64 Policy	
NAT46 Policy	
Authentication Rules	
Multicast Policy	
Local In Policy	
IPv4 DoS Policy	
IPv6 DoS Policy	
Addresses	
Internet Service Database	
Services	
Schedules	
Virtual IPs	
IP Pools	
Protocol Options	
Traffic Shapers	
Traffic Shaping Policy	
Traffic Shaping Profile	
Virtual Servers	
Health Check	

© Fortinet Inc. All Rights Reserved.

5

Each policy matches traffic and applies security by referring to the objects that you've defined, such as addresses and profiles.

What about other firewall policy types? Do IPv6 or virtual wire policies exist? Yes. These policies use slightly different objects that are relevant to their type. In this lesson, you will learn about IPv4 firewall policies, because they are the most common use case.

DO NOT REPRINT**© FORTINET**

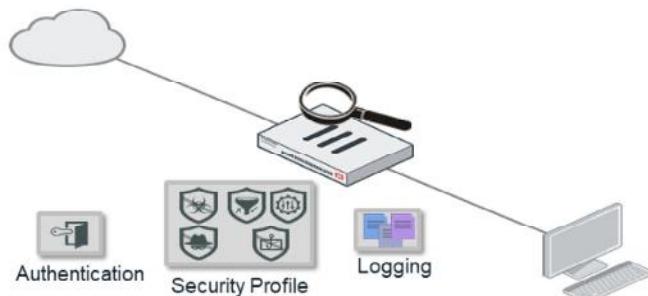
How Are Policy Matches Determined?

Incoming and outgoing interfaces	✓
Source: IP address, user, Internet Services	✓
Destination: IP address or Internet Services	✓
Services	✓
Schedules	✓

Action = **ACCEPT** or **DENY**

Policy & Objects > Firewall Policy

Name	<input type="text"/>
Incoming Interface	<input type="text"/>
Outgoing Interface	<input type="text"/>
Source	<input type="button" value="+"/>
Destination	<input type="button" value="+"/>
Schedule	<input checked="" type="checkbox"/> always
Service	<input type="button" value="+"/>
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY



FORTINET

© Fortinet Inc. All Rights Reserved.

6

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- **Incoming Interface**
- **Outgoing Interface**
- **Source:** IP address, user, Internet services
- **Destination:** IP address or Internet services
- **Service:** IP protocol and port number
- **Schedule:** Applies during configured times

When the traffic matches a firewall policy, FortiGate applies the action configured in the firewall policy.

- If the **Action** is set to **DENY**, FortiGate drops the session.
- If the **Action** is set to **ACCEPT**, FortiGate applies other configured settings for packet processing, such as antivirus scanning, web filtering, or source NAT.

For example, if you want to block incoming FTP to all but a few FTP servers, you would define the addresses of your FTP servers, select those as the destination, and select FTP as the service. You probably *wouldn't* specify a source (often any location on the Internet is allowed) or schedule (usually FTP servers are always available, day or night). Finally, you would set the **Action** setting to **ACCEPT**.

This *might* be enough, but often you'll want more thorough security. Here, the policy also authenticates the user, scans for viruses, and logs blocked connection attempts.

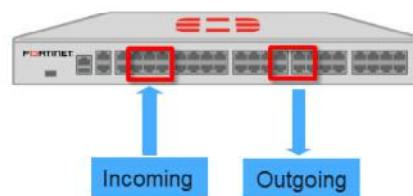
DO NOT REPRINT

© FORTINET

Simplify—Interfaces and Zones

- **Incoming Interface** and **Outgoing Interface** can be interface(s) or a **zone**
 - Zone: Logical group of interfaces
- To match policies with traffic, select one (or more) interfaces or any interface

Network > Interfaces			
<input type="button" value="Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> Search			
Type	Members	IP/Netmask	
Physical Interface		10.0.1.254/255.255.255.0	
port4	Physical Interface	0.0.0.0/0.0.0.0	
port5	Physical Interface	0.0.0.0/0.0.0.0	
port6	Physical Interface	0.0.0.0/0.0.0.0	
port7	Physical Interface	0.0.0.0/0.0.0.0	
port8	Physical Interface	172.16.100.3/255.255.255.0	
<input type="checkbox"/> Zone 1			
DMZ	Zone	port2	0.0.0.0/0.0.0.0
		port8	



© Fortinet Inc. All Rights Reserved.

7

To begin describing how FortiGate finds a policy for each packet, let's start with the interface(s).

Packets arrive on an incoming, or ingress, interface. Routing determines the outgoing, or egress, interface. In each policy, you *must* set a source and destination interface; even if one or both are set to **any**. Both interfaces must match the policy's interface criteria in order to be a successful match.

For example, if you configure policies between port3 (LAN) ingress and port1 (WAN) egress and a packet arrives on port2, the packet would *not* match your policies and, therefore, would be dropped because of the implicit deny policy at the end of the list. Even if the policy is from port3 (LAN) ingress to any egress, the packet would still be dropped because it did not match the incoming interface.

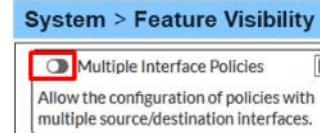
To simplify policy configuration, you can group interfaces into logical zones. For example, you could group port4 to port7 as a DMZ zone. Zones can be created from the **Interfaces** page. However, you should note that an interface in a zone cannot be referenced individually, and, if you need to add the interface to the zone, you must remove all references to that interface (for example, firewall policies, firewall addresses, and so on). If you think that you might need to reference interfaces individually, you should set multiple source and destination interfaces in the firewall policy, instead of using zones.

DO NOT REPRINT

© FORTINET

Selecting Multiple Interfaces or Any Interface

- Disabled by default
 - Cannot select multiple interfaces or any interface in firewall policy from the GUI
- Can be made visible in the GUI



The screenshot shows the 'Policy & Objects > Firewall Policy' page. A new policy is being created with the name 'Single Int'. The 'Incoming Interface' dropdown is set to 'port3' and the 'Outgoing Interface' dropdown is set to 'port1'. Both dropdowns are highlighted with red boxes.

Policy & Objects > Firewall Policy

The screenshot shows the 'Policy & Objects > Firewall Policy' page. A new policy is being created with the name 'Multiple Int'. The 'Incoming Interface' dropdown contains 'port3' and 'port4', both highlighted with red boxes. The 'Outgoing Interface' dropdown is set to 'any'.

Multiple interface policies enabled

© Fortinet Inc. All Rights Reserved.

8

By default, you can select only a single interface as the incoming interface and a single interface as the outgoing interface. This is because the option to select multiple interfaces, or **any** interface in a firewall policy, is disabled on the GUI. However, you can enable the **Multiple Interface Policies** option on the **Feature Visibility** page to disable the single interface restriction.

You can also specify multiple interfaces, or use the **any** option, if you configure a firewall policy on the CLI, regardless of the default GUI setting.

It is also worth mentioning that when you choose the **any** interface option, you cannot select multiple interfaces for that interface. In this example, because **any** is selected as the outgoing interface, you cannot add any additional interfaces, because **any** interface implies that all interfaces have already been selected.

DO NOT REPRINT**© FORTINET**

Matching by Source

- Must specify at least one source (address or Internet service database (ISDB) object)

- IP address or range
- Subnet (IP/Netmask)
- FQDN
- Geography
- Fabric Connector Address
- MAC Address Range

- May specify:

- Source User—Individual user or user group
- This may refer to:
 - Local firewall accounts
 - Accounts on a remote server (for example, Active Directory, LDAP, RADIUS)
 - FSSO
 - Personal certificate (PKI-authenticated) users



Addresses	FQDN	testfor123.com
Internet Service Database	Abtest adobe	⚠️ Unresolved FQDN: testfor123.com

Warning for
unresolved FQDN

FORTINET

© Fortinet Inc. All Rights Reserved.

9

The next match criteria that FortiGate considers is the packet's source.

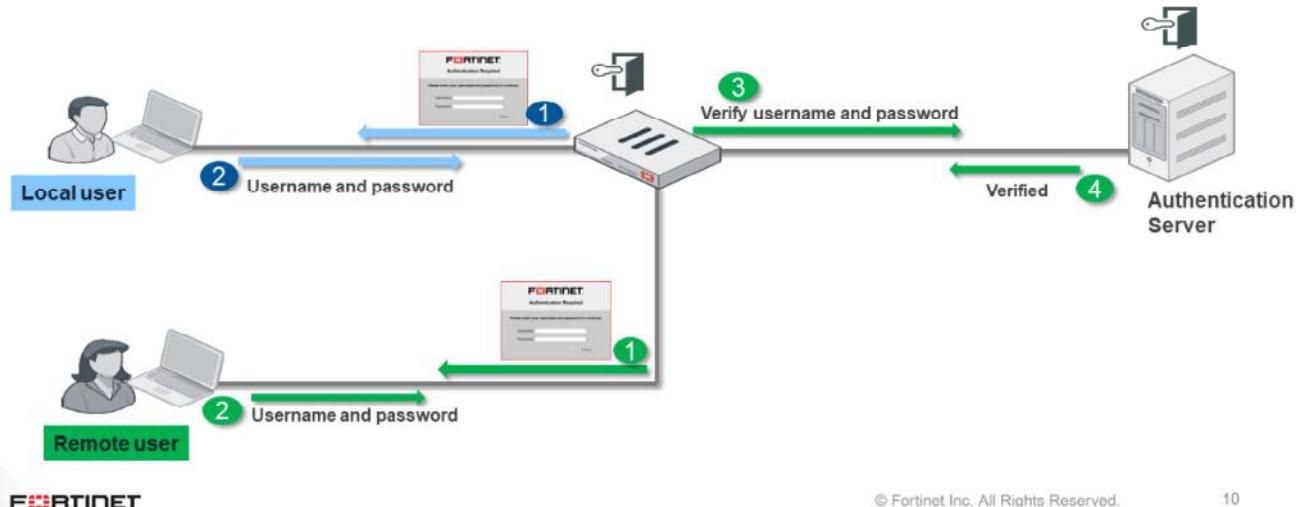
In each firewall policy, you *must* select a source address object. Optionally, you can refine your definition of the source address by *also* selecting a user, or a user group, which provides a much more granular match, for increased security. You can also select ISDB objects as source in the firewall policy which we will discuss later in the lesson.

When selecting a fully qualified domain name (FQDN) as the source address, it must be resolved by DNS and cached in FortiGate. Make sure FortiGate is configured properly for DNS settings. If FortiGate is not able to resolve an FQDN address, it will present a warning message, and a firewall policy configured with that FQDN may not function properly.

DO NOT REPRINT**© FORTINET**

Source–User Identification

- Confirms identity of user
- Access to network is provided after confirming user credentials



© Fortinet Inc. All Rights Reserved.

10

If a user is added as part of the source, FortiGate must verify the user before allowing or denying access based on the firewall policy. There are different ways that a user can authenticate.

For local users, the username and password is configured *locally* on FortiGate. When a local user authenticates, the credentials that they enter must match the username and password configured locally on FortiGate.

For a remote user (for example, LDAP or RADIUS), FortiGate receives the username and password from the remote user and passes this information to the authentication server. The authentication server verifies the user login credentials and updates FortiGate. After FortiGate receives that information, it grants access to the network based on the firewall policy.

A Fortinet single sign-on (FSSO) user's information is retrieved from the domain controller. Access is granted based on the group information on FortiGate.

DO NOT REPRINT

© FORTINET

Example—Matching Policy by Source

- Matches by source address, user
- Source as Internet service database (ISDB) objects

The screenshot shows two instances of the 'Policy & Objects > Firewall Policy' interface.

Left Window (Training Policy):

- Name: Training
- Incoming Interface: port3
- Outgoing Interface: port1
- Source: LOCAL_SUBNET (selected), student (selected)

Right Window (Training Policy):

- Name: Training
- Incoming Interface: port3
- Outgoing Interface: port1
- Source: Amazon-AWS (selected)
- Destination: always
- Schedule: always
- Service: (empty)

Annotations with blue arrows point from labels to specific fields:

- An arrow labeled 'Address' points to the 'LOCAL_SUBNET' entry in the Source field of the left window.
- An arrow labeled 'User' points to the 'student' entry in the Source field of the left window.
- An arrow labeled 'Internet Service' points to the 'Amazon-AWS' entry in the Source field of the right window.

At the bottom left is the FORTINET logo, and at the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 11

In this example, source selectors identify the specific subnet and user group.

Remember, user is an optional object. The user object is used here to make the policy more specific. If you wanted the policy to match more traffic, you would leave the user object undefined.

You can also use Internet service (ISDB) objects as a source in the firewall policy. There is an either/or relationship between Internet service objects and source address objects in firewall policies. This means that you can select either a source address or an Internet service, but not both.

DO NOT REPRINT**© FORTINET**

Matching by Destination

Like source, destination criteria can use:

- Address objects:
 - Subnet (IP or netmask)
 - IP address or address range
 - FQDN
 - DNS query used to resolve FQDN
 - Geography
 - Country defines addresses by ISP's geographical location
 - Database updated periodically through FortiGuard
 - Fabric Connector Address
- Internet service database (ISDB) objects



© Fortinet Inc. All Rights Reserved.

12

Like the packet's source, FortiGate also checks the destination address for a match.

You can use address objects or ISDB objects as destinations in the firewall policy. The address object may be a host name, IP subnet, or range. If you enter an FQDN as the address object, make sure that you've configured your FortiGate with DNS servers. FortiGate uses DNS to resolve those FQDN host names to IP addresses, which are what actually appear in the IP header.

Geographic addresses, which are groups or ranges of addresses allocated to a country, can be selected instead. These objects are updated through FortiGuard.

Why is there is no option to select a user? The user identification is determined at the ingress interface, and packets are forwarded only to the egress interface after user authentication is successful.

DO NOT REPRINT

© FORTINET

Internet Service

- Database that contains IP addresses, IP protocols, and port numbers used by the most common Internet services
 - Regularly updated through FortiGuard
- Can be used as Source or Destination in the firewall policy
- If Internet Service is selected as Source:
 - You cannot use Address in the Source
- If Internet Service is selected as Destination:
 - You cannot use Address in the Destination
 - You cannot select Service in the firewall policy

Policy & Objects > Internet Service Database

Name	Rep...	Direction
Internet Service Database	3/1408	
Microsoft.Outlook	5	Both 1,021
Google.Google.Bot	4	Source 31
Facebook.Whatsapp	5	Destination 1,823

Policy & Objects > Firewall Policy

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Destination' section, there is a list of entries: 'all' and 'Facebook-Web'. A red box highlights the 'Facebook-Web' entry. A red arrow points from this highlighted entry to a 'Select Entries' sidebar on the right. The sidebar lists various objects, and 'Facebook-Web' is highlighted with a yellow background. A tooltip at the bottom of the main interface states: 'Addresses/groups cannot be mixed with Internet services'.

FORTINET

© Fortinet Inc. All Rights Reserved.

13

Internet Service is a database that contains a list of IP addresses, IP protocols, and port numbers used by the most common Internet services. FortiGate periodically downloads the newest version of this database from FortiGuard. These can be selected as **Source** or **Destination** in the firewall policy.

What happens if you need to allow traffic to only a few well-known public Internet destinations, such as Dropbox or Facebook?

When configuring your firewall policy, you can use **Internet Service** as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information which is hardcoded.

Compared with address objects, which you need to check frequently to make sure that none of the IP addresses have changed or appropriate ports are allowed, Internet services helps make this type of deployment easier and simpler.

DO NOT REPRINT

© FORTINET

Geographic Based Internet Service Database

- Allows users to define ISDB objects based on a country, region, and city
- Objects can be used in firewall policies for more granular control over the location of the parent ISDB object

Policy & Objects > Internet Service Database

+ Create New ▾ Edit Delete

Geographic Based Internet Service



New Internet Service

Name	Training-location-ISDB	Master Internet Service Name	Google-Other
Type	Predefined Geographic Based	Master Internet Service ID	65536
Master Internet Service	Google-Other	Direction	Destination
Country/Region	United Kingdom	Entries	
Region	England	View/Edit Entries	
City	London		

Google-Other

Location: (United Kingdom, England, London)

IP	Port	Protocol	Status
2.127.239.205, 2.127.239.206	1-65535	TCP	Enabled
2.127.239.205, 2.127.239.206	1-65535	UDP	Enabled
2.127.244.140 - 2.127.244.142	1-65535	TCP	Enabled
2.127.244.140 - 2.127.244.142	1-65535	UDP	Enabled

FORTINET

© Fortinet Inc. All Rights Reserved.

14

Geographic-based ISDB objects allow users to define a country, region, and city. These objects can be used in firewall policies for more granular control over the location of the parent ISDB object.

ISDB objects are referenced in policies by name, instead of by ID.

DO NOT REPRINT

© FORTINET

Scheduling

- Policies apply only during specific times and on specific days

- Example: A less restrictive *lunch time* policy
- The default schedule applies all the time



- Recurring**

- Happens at the same time during specified day(s) of the week

- One-time**

- Happens only once

Policy & Objects > Schedules

New Schedule	
Type	<input checked="" type="radio"/> Recurring <input type="radio"/> One Time
Name	Maintenance
Color	<input type="button" value="Change"/>
Days	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday
All Day	<input type="radio"/>
Start Time	12:00 AM
Stop Time	12:00 PM

FORTINET

Policy & Objects > Schedules

New Schedule

- Type Recurring One Time

Name Maintenance

Start Date 04/30/2020

12:02 PM

End Date 04/30/2020

01:02 PM

Pre-expiration event log

Number of days before 1

© Fortinet Inc. All Rights Reserved.

15

Schedules add a time element to the policy. For example, you might use a policy to allow backup software to activate at night, or create a test window for a remote address that is allowed for testing purposes.

Schedules can be configured and use a 24-hour time clock. There are a few configuration settings worth mentioning:

- Recurring:** If **All Day** is enabled, traffic will be allowed for 24 hours for the days selected. When configuring recurring schedules, if the stop time is set earlier than the start time, the stop time will occur the next day. For example, if you select Sunday as the day, 10:00 as the start time, and 09:00 as the stop time, the schedule will stop on Monday at 09:00. If the start and stop time are identical, the schedule will run for 24 hours.
- One-time:** The start date and time must be earlier than the stop date and time. You can also enable **Pre-expiration event log**, which will generate an event log N number of days before the schedule expires, where N can be from 1 to 100 days.

DO NOT REPRINT

© FORTINET

Matching by Service

- Service determines matching transmission protocol (UDP, TCP, and so on) and port number
- Can be predefined or custom
- ALL matches all ports and protocols



Policy & Objects > Services

Policy & Objects > Services				
Create New Edit Clone Delete Category Settings <input type="text"/> Search Ref.				
Service Name	Details	IP/FQDN	Show in Service List	Ref.
ALL	ANY		<input checked="" type="checkbox"/> Visible	1
ALL_TCP	TCP/1-65535	0.0.0	<input checked="" type="checkbox"/> Visible	0
ALL_UDP	UDP/1-65535	0.0.0	<input checked="" type="checkbox"/> Visible	0
ALL_ICMP	ANY		<input checked="" type="checkbox"/> Visible	1
ALL_ICMP6	ANY		<input checked="" type="checkbox"/> Visible	0
Web Access				
HTTP	TCP/80	0.0.0.0	<input checked="" type="checkbox"/> Visible	1
HTTPS	TCP/443	0.0.0.0	<input checked="" type="checkbox"/> Visible	2

FORTINET

© Fortinet Inc. All Rights Reserved.

16

Another criterion that FortiGate uses to match policies is the packet's service.

At the IP layer, protocol numbers (for example, TCP, UDP, SCTP, and so on) together with source and destination ports, define each network service. Generally, only a destination port (that is, the server's listening port) is defined. Some legacy applications may use a specific source port, but in most modern applications, the source port is randomly identified at transmission time, and therefore is not a reliable way to define the service.

For example, the predefined service object named HTTP is TCP destination port 80, and the predefined service object named HTTPS is TCP destination port 443. However, the source ports are ephemeral and, therefore, not defined.

By default, services are grouped together to simplify administration by categories. If the predefined services don't meet your organizational needs, you can create one or more new services, service groups, and categories.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What criteria does FortiGate use to match traffic to a firewall policy?
 A. Source and destination interfaces
B. Security profiles

2. What must be selected in the **Source** field of a firewall policy?
 A. At least one address object or ISDB
B. At least one source user and one source address object



© Fortinet Inc. All Rights Reserved.

17

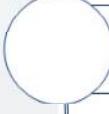
DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Good job! You now understand the components used in firewall policies and matching criteria used by FortiGate.

Now, you'll learn how to configure firewall policies.

DO NOT REPRINT

© FORTINET

Configuring Firewall Policies

Objectives

- Restrict access and make your network more secure using security profiles
- Configure logging

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

By demonstrating competence in configuring firewall policies, you will be able to apply the correct settings, such as security profiles, logging, and traffic shaping to firewall policies on FortiGate, and make your network more secure.

DO NOT REPRINT

© FORTINET

Configuring Firewall Policies

- Mandatory policy name when creating on GUI
 - Can relax the requirement by enabling **Allow Unnamed Policies**

- Flat GUI view allows:
 - Select by clicking
 - Drag-and-drop

```
config firewall policy
edit 1
  set name "Training"
  set uuid 2204966e-47f7-51...
```

Universally Unique Identified (UUID)

The screenshot shows two windows side-by-side. On the left is the 'Firewall Policy' configuration window. It has fields for Name (Training), Incoming Interface (port3), Outgoing Interface (port1), Source (LOCAL_SUBNET), Destination (all), Schedule (always), Service (ALL), and Action (ACCEPT). A callout bubble points to the 'Name' field with the text 'Enabled by default MUST specify unique name'. Another callout bubble points to the 'Source' field with the text 'Highlights selected entry'. On the right is the 'System > Feature Visibility' window, which contains a checkbox for 'Allow Unnamed Policies'. Below it is a list of objects including ADDRESS (13), FABRIC_DEVICE, FORTINET, gmail.com, LINUX.ETH1, LOCAL_SUBNET, LOCAL_WINDOWS, and login.microsoft.com. The 'LOCAL_SUBNET' object is highlighted with a yellow background.

FORTINET

© Fortinet Inc. All Rights Reserved.

20

When you configure a new firewall policy on the GUI, you *must* specify a unique name for the firewall policy because it is enabled by default, but it is optional in the CLI. This helps the administrator to quickly identify the policy that they are looking for. However, you can make this feature optional on the GUI on the **Feature Visibility** page by enabling **Allow Unnamed Policies**.

Note that if a policy is configured without a policy name on the CLI and you modify that existing policy on the GUI, you *must* specify a unique name. The FortiGate flat GUI view allows you to select interfaces and other objects by clicking or dragging and dropping from the list populated on the right side.

You can select Internet service as the source. Internet service is a combination of one or more addresses and one or more services associated with a service found on the Internet, such as an update service for software.

There are many other options that you can configure in the firewall policy, such as firewall and network options, security profiles, logging options, and enabling or disabling a policy.

When creating firewall objects or policies, a universally unique identified (UUID) attribute is added so that logs can record these UUID and improve functionality when integrating with FortiManager or FortiAnalyzer.

When creating firewall policies, remember that FortiGate is a stateful firewall. As a result, you need to create only one firewall policy that matches the direction of the traffic that initiates the session. FortiGate will automatically remember the source-destination pair and allow replies.

DO NOT REPRINT**© FORTINET**

Security Profiles

- Firewall policies limit access to configured networks
- Security profiles configured in firewall policies protect your network by:
 - Blocking threats
 - Controlling access to certain applications and URLs
 - Preventing specific data from leaving your network

Policy & Objects > Firewall Policy

Security Profiles	
AntiVirus	<input checked="" type="radio"/> AV default <input type="button" value="edit"/>
Web Filter	<input checked="" type="radio"/> WEB default <input type="button" value="edit"/>
DNS Filter	<input checked="" type="radio"/> DNS default <input type="button" value="edit"/>
Application Control	<input checked="" type="radio"/> APP default <input type="button" value="edit"/>
IPS	<input checked="" type="radio"/> IPS default <input type="button" value="edit"/>
VoIP	<input checked="" type="radio"/> VOIP default <input type="button" value="edit"/>
SSL Inspection 	<input checked="" type="radio"/> SSL deep-inspection <input type="button" value="edit"/>

FORTINET

© Fortinet Inc. All Rights Reserved.

21

One of the most important features that a firewall policy can apply is security profiles, such as IPS and antivirus. A security profile inspects each packet in the traffic flow, where the session has already been conditionally accepted by the firewall policy.

When inspecting traffic, FortiGate can use one of two methods: flow-based inspection or proxy-based inspection. Different security features are supported by each inspection type.

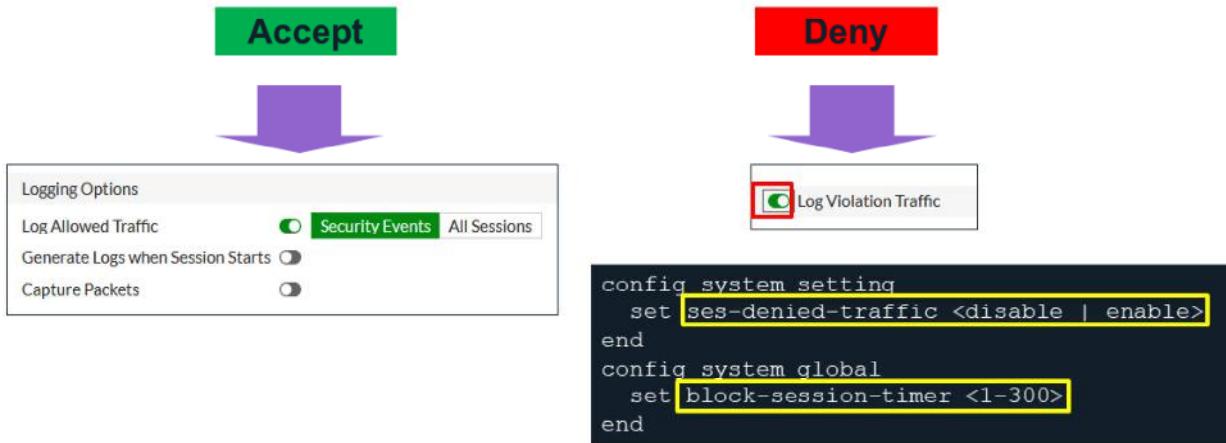
Note that by default, the **VOIP** security profile option is not visible in the policy page on the GUI. You need to enable **VOIP** on the **Feature Visibility** page.

DO NOT REPRINT

© FORTINET

Logging

- By default, set to **Security Events**
 - Generates logs based on applied security profile only
- Can change to **All Sessions**



FORTINET

© Fortinet Inc. All Rights Reserved.

22

If you have enabled logging in the policy, FortiGate will generate traffic logs after a firewall policy closes an IP session.

By default, **Log Allowed Traffic** is enabled and set to **Security Events** and generates logs for only the applied security profiles in the firewall policy. However, you can change the setting to **All Sessions**, which generates logs for all sessions.

If you enable **Generate Logs when Session Starts**, FortiGate creates a traffic log when the session begins. FortiGate also generates a second log for the same session when it is closed. But remember that increasing logging decreases performance, so use it only when necessary.

During the session, if a security profile detects a violation, FortiGate records the attack log immediately. To reduce the amount of log messages generated and improve performance, you can enable a session table entry of dropped traffic. This creates the denied session in the session table and, if the session is denied, all packets of that session are also denied. This ensures that FortiGate does not have to do a policy lookup for each new packet matching the denied session, which reduces CPU usage and log generation.

This option is in the CLI, and is called `ses-denied-traffic`. You can also set the duration for block sessions. This determines how long a session will be kept in the session table by setting `block-session-timer` in the CLI. By default, it is set to 30 seconds.

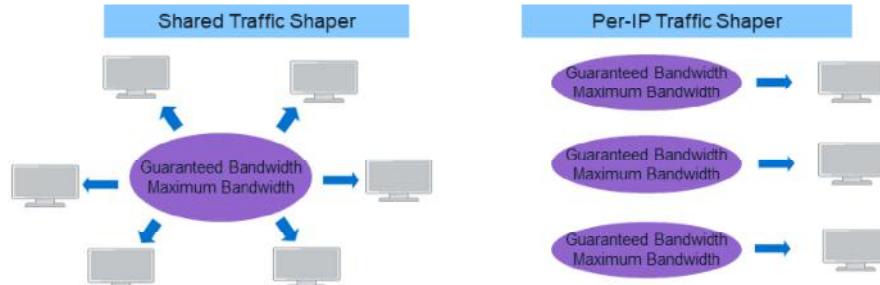
If the GUI option **Generate Logs when Session Starts** is not displayed, this means that your FortiGate device does not have internal storage. This option is in the CLI, regardless of internal storage, and is called `set logtraffic-start enable`.

DO NOT REPRINT**© FORTINET**

Traffic Shapers

- Rate limiting is configurable
 - In bandwidth and out bandwidth
 - Defines maximum and guaranteed bandwidth

Policies & Objects > Traffic Shaping Policy



FORTINET

© Fortinet Inc. All Rights Reserved.

23

Two types of traffic shapers can be configured: shared and per IP.

A shared shaper applies a total bandwidth to all traffic using that shaper. The scope can be per policy or for all policies referencing that shaper. FortiGate can count the packet rates of ingress and egress to police traffic.

FortiGate allows you to create three types of traffic shaping policies:

- Shared policy shaping: Bandwidth management of security policies
- Per-IP shaping: Bandwidth management of user IP addresses
- Application control shaping: Bandwidth management by application

When creating traffic shaping policies, you must ensure that the matching criteria is the same as the firewall policies you want to apply shaping to. Note that these apply equally to TCP and UDP, and UDP protocols may not recover as gracefully from packet loss.

DO NOT REPRINT**© FORTINET**

Consolidated IPv4 and IPv6 Policy Configuration

- IPv4 and IPv6 policies are combined into a single consolidated policy, instead of separate policies
- The IP version of the sources and destinations in a policy must match
- Single policy table for GUI
- Different IP addresses and IP pool for IPv4 and IPv6

ID	Name	From	To	Source	Destination	Schedule	Action	NAT	Security Profiles
34		port4	port1	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled no-Inspection
44		port4	port3	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Disabled certificate-inspection All
99		port3	port1	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled no-Inspection UTM
91		port2	port2	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled no-Inspection UTM
222		port2	port1	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> ipv4-ippool-1 <input checked="" type="checkbox"/> ipv6-ippool-1 certificate-inspection UTM
0	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY	<input checked="" type="checkbox"/> Disabled

FORTINET

© Fortinet Inc. All Rights Reserved.

24

By default, IPv4 and IPv6 policies are combined into a single consolidated policy, rather than creating and maintaining two different policy sets for IPv4 and IPv6.

You can share the **Incoming Interface**, **Outgoing Interface**, **Schedule**, and **Service** fields with both IPv4 and IPv6. For source addresses, destination addresses, and IP pool, you must select addresses for both IPv4 and IPv6.

While configuring a consolidated firewall policy, you can configure a policy with IPv4 source addresses, IPv4 destination addresses, and an IPv4 IP pool, without specifying any IPv6 references. You can also configure the policy with same behavior for IPv6. However, if you want to combine IPv4 and IPv6, you must select both IPv4 addresses and IPv6 addresses in the **Source** and **Destination** address fields in the firewall policy. The IP version of the sources and destinations in a policy must match. For example, a policy cannot have only an IPv4 source and an IPv6 destination. The policy table in the GUI can be filtered to show policies with IPv4, IPv6, or IPv4 and IPv6 sources and destinations.

Note that by default, the **IPv6** option is not visible in the policy table in the GUI. You need to enable **IPv6** on the **Feature Visibility** page.

When upgrading from FortiOS 6.2.3 to 6.4.0, if consolidated policy mode is enabled, consolidated policies will be changed to firewall policies:

- In NGFW profile-based mode, IPv4 and IPv6 policies will all be added to the firewall policy list, with IPv6 policies listed after IPv4 policies.
- In NGFW policy-based mode, policies will be changed from consolidated policies to firewall policies on the CLI.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. To configure a firewall policy, you must include a firewall policy name when configuring using the ____.
A. CLI
 B. GUI

2. What is the purpose of applying security profiles to a firewall policy?
A. To allow access to certain subnets
 B. To protect your network from threats and control access to specific applications and URLs



© Fortinet Inc. All Rights Reserved.

25

DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Good job! You now understand how to configure firewall policies on FortiGate.

Next, you'll learn how to manage and fine-tune settings for firewall policies.

DO NOT REPRINT

© FORTINET

Managing Firewall Policies

Objectives

- Identify policy list views
- Understand the use of policy IDs
- Identify where an object is referenced

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

By demonstrating competence in managing firewall policies, you will be able to understand the use of policy ID of a firewall policy. Also, you will be able to pinpoint object usage, and simplify policies using object groups.

DO NOT REPRINT

© FORTINET

Policy List—Interface Pair View and By Sequence

- Interface Pair View

- Lists policies by ingress and egress interfaces (or zone) pairings

Can view **By Sequence** also

Policy & Objects > Firewall Policy

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
port3 → port1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection UTM 0B
Full_Access	all	all	always	ALL	ACCEPT	Enabled	no-inspection All	912.05 kB
port3 → port2	Backup_Access	all	always	ALL	ACCEPT	Enabled	no-inspection UTM	0B

Interface policy pairs

- By Sequence (only)

- If policies are created using multiple source and destination interfaces or any interface

Policy & Objects > Firewall Policy

Name	From	To	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
Fortinet	port3	port1	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection UTM	0B
Full_Access	port3	port1	all	all	always	ALL	ACCEPT	Enabled	no-inspection All	941.50 kB
Any Interface	port3	any	all	all	always	ALL	ACCEPT	Enabled	no-inspection UTM	0B
Implicit Deny	any	any	all	all	always	ALL	DENY	Disabled		981.97 kB

FORTINET

© Fortinet Inc. All Rights Reserved.

28

Firewall policies appear in an organized list. The list is organized either in **Interface Pair View** or **By Sequence**.

Usually, the list will appear in **Interface Pair View**. Each section contains policies for that ingress-egress pair. Alternatively, you can view your policies as a single, comprehensive list by selecting **By Sequence** at the top of the page.

In some cases, you won't have a choice of which view is used.

If you use multiple source or destination interfaces, or the **any** interface in a firewall policy, policies cannot be separated into sections by interface pairs—some would be triplets or more. So instead, policies are then always displayed in a single list (**By Sequence**).

To help you remember the use of each interface, you can give them aliases by editing the interface on the **Network** page. For example, you could call port1 *ISP1*. This can help to make your list of policies easier to understand.

DO NOT REPRINT**© FORTINET**

Real-Time Policy Status

- Real-time policy status update

Policy & Objects > Firewall Policy

The screenshot shows the 'Edit Policy' interface for a policy named 'Full_Access'. The policy details are as follows:

- Name:** Full_Access
- Incoming Interface:** port3
- Outgoing Interface:** port1
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ✓ ACCEPT (selected), DENY
- Inspection Mode:** Flow-based (selected)
- Firewall / Network Options:** NAT (radio button selected), IP Pool Configuration (radio button selected), Use Outgoing Interface Address, Use Dynamic IP Pool

On the right side, a summary of the policy usage is displayed:

- ID:** 2
- Last used:** 0 second(s) ago
- First used:** 1 hour(s) ago
- Hit count:** 58
- Active sessions:** 27
- Total bytes:** 453.97 kB
- Current bandwidth:** 34.94 kB/s

A red box highlights the summary statistics on the right.

FORTINET

© Fortinet Inc. All Rights Reserved.

29

When you edit the policy, policy information will be visible.

This feature is very useful if admin wanted to check the policy usage such as last used, first used, hit count, active sessions, and so on.

DO NOT REPRINT

© FORTINET

Policy ID

- Firewall policies are primarily ordered on a *top-down* basis
- Policy IDs are identifiers:
 - The policy ID is assigned by the system when the rule is created
 - The ID number never changes as rules move higher or lower in the sequence
 - Policy IDs are not displayed by default on the GUI

```
config firewall policy
edit <policy_id>
end
```

Policy ID

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Action	NAT
	port3 → port1					
2	Block_FTP	all	all	always	FTP DENY	
1	Full_Access	LOCAL_SUBNET	all	always	ALL ACCEPT	Enabled
	port6 → port8					
3	DMZ	DMZ	all	always	ALL ACCEPT	Enabled

```
config firewall policy
edit 2
  set name "Block_FTP"
...
next
edit 1
  set name "Full_Access"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

30

An important concept to understand about how firewall policies work is the precedence of order, or, if you prefer a more recognizable term, first come, first served.

Policy IDs are identifiers. By default, policy IDs are not displayed on the policy list GUI. You can add a **Policy ID** column using the **Configure Table** settings icon.

FortiGate automatically assigns a policy ID when you create a new firewall policy on the GUI. The policy ID never changes, even if you move the rule higher or lower in the sequence.

If you enable **Policy Advanced Options**, then you can manually assign policy ID while creating a new policy. If a duplicate entry is found, the system will produce an error, so you can assign a different available policy ID number.

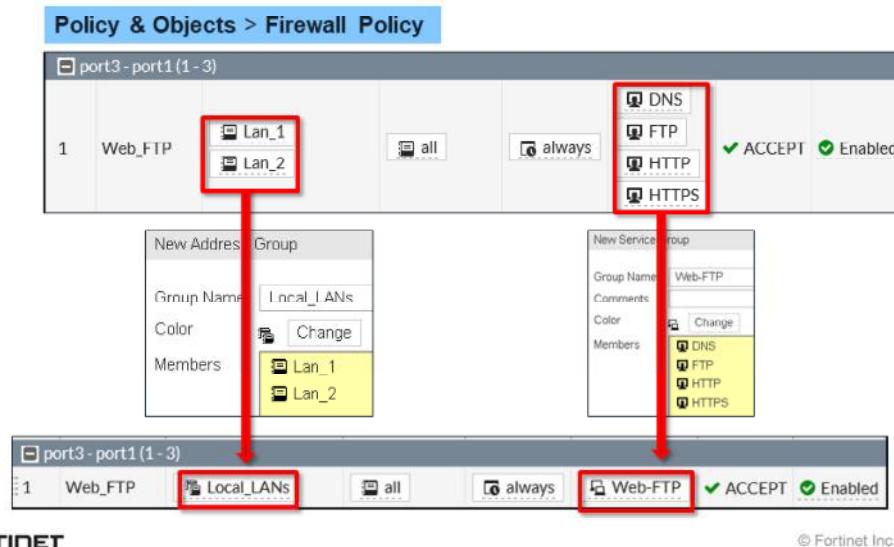
Policy Advanced Options is not available on the GUI by default, you need enable it on the **Feature Visibility** page.

DO NOT REPRINT

© FORTINET

Simplify—Groups of Addresses or Services

- You can reference address and service objects individually, or use groups to simplify policy configuration



To simplify administration, you can group service and address objects. Then, you can reference that group in the firewall policy, instead of selecting multiple objects each time or making multiple policies.

On this slide, four services are used to configure the policy: HTTP, HTTPS, FTP, and DNS. DNS is used by browsers to resolve URLs to IP addresses because people remember domain names for web sites instead of IP addresses. If you need to make many policies for web and FTP traffic, then it makes sense to create a service object named **Web-FTP**. That way, you don't have to manually select all four services each time you make a policy. Policies can reference the **Web-FTP** service group instead.

Also, you can consolidate source addresses in source groups.

DO NOT REPRINT

© FORTINET

Object Usage

- Allows for faster changes to settings
- Reference column shows *if the object is being used*
 - Links directly to the referencing object

The screenshot illustrates the FortiGate GUI interface for managing objects. On the left, a sidebar titled 'Edit Policy' shows a configuration for a policy named 'DMZ' with source and destination interfaces set to 'all'. In the center, a modal window titled 'Usage of Address: all' displays the usage details for the 'all' address object. It lists 'Address Group (1)' and 'Policy (3)' as references, with counts of '2 References' for each. A callout 'Number of times object used' points to these counts. On the right, a 'Properties of Policy: policy' panel shows the policy's configuration, including its ID, name, and interface assignments. A red box highlights the 'Ref.' column in the top table, which shows a value of 'B' for the 'all' object, indicating it is being used by three policies. Red arrows point from the 'Edit', 'View List', and 'View Properties' buttons in the central modal to their respective counterparts in the policy properties panel.

Name	Type	Details	Visibility	Ref.
LOCAL_SUBNET	Subnet	10.0.1.0/24	Visible	1
all	Subnet	0.0.0.0/0	Visible	B

Attribute	Policy
policyid	4
name	DMZ
uuid	52382dd8-4041-4000-8000-000000000000
srcintf.0.name	port6
dstintf.0.name	port4
srcaddr.0.name	all
dstaddr.0.name	all

We've just shown several component objects that can be reused as you make policies. What if you want to delete an object?

If an object is being used, you can't delete it. First, you *must* reconfigure the objects that are currently using it. The GUI provides a simple way to find out where in the FortiGate's configuration an object is being referenced. See the numbers in the **Ref.** column? They are the number of places where that object is being used. The number is actually a link, so if you click it, you can see which objects are using it.

In this example, the **all** address object is being used by the **Training** address group and three firewall policies. If you select a firewall policy, you can use the **Edit**, **View List**, and **View Properties** tabs.

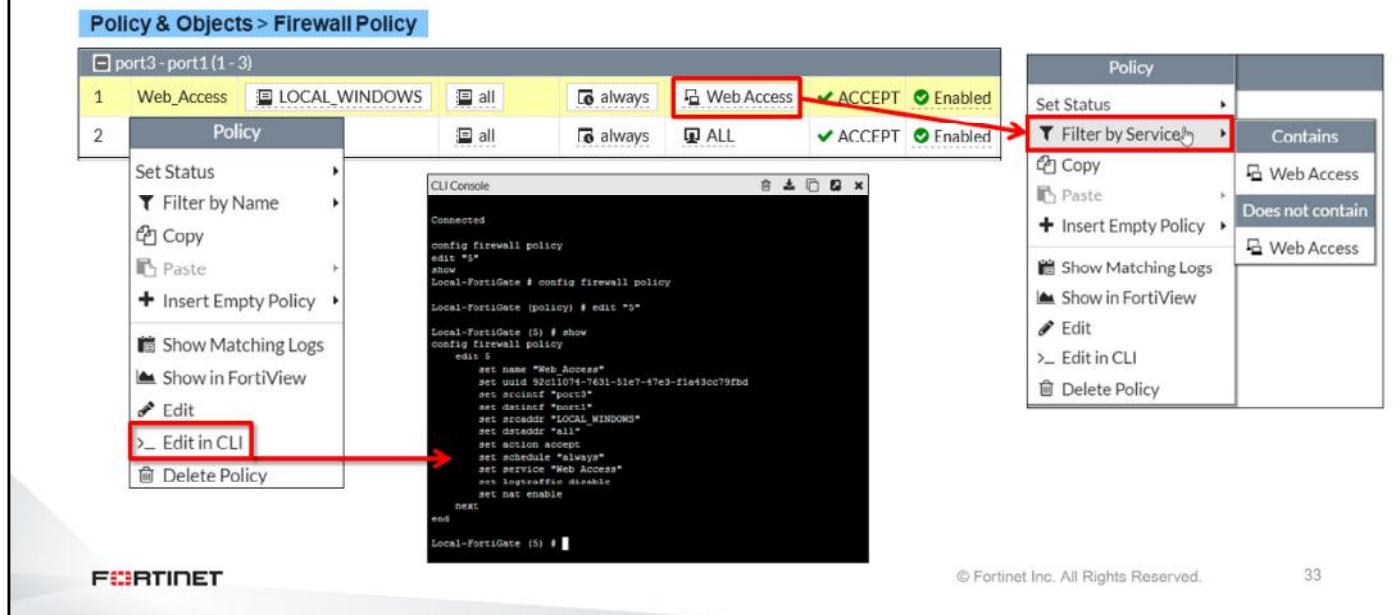
- Edit:** Allows you to edit the selected object. In this example, it shows the edit page for the firewall policy ID 4.
- View List:** Allows you to view selected objects in its category. In this example, it will show you the list of all the firewall policies.
- View Properties:** Shows where the object is used in that configuration. In this example, address object **all** is being used in the destination address and source address of that firewall policy.

DO NOT REPRINT

© FORTINET

Firewall Policy—Fine Tuning

- Right-click menu contains various options to add and modify policies



You can right-click any firewall policy to see different menu options to edit or modify the policy. The options include enabling or disabling a firewall policy, inserting firewall policies (above or below), copying and pasting policies, and cloning reverse (only if NAT is disabled on that policy).

Clicking **Edit in CLI** opens the CLI console for the selected firewall policy or object. It shows the configured settings in the CLI and can modify the selected firewall policy or object directly in the **CLI Console**.

DO NOT REPRINT

© FORTINET

Filter Column

- You can use filters in each column to filter firewall policies

ID	Name	Source	Destination
1	Fortinet	port3 → port1	1/2
1	Fortinet	LOCAL_CLIENT	FORTINET

You can filter firewall policies on the GUI using filters in each column. You can add the **ID** column and then click the **ID** column filter icon to filter and search policies based on policy Id numbers. You can click the **Name** filter icon to search policies based on policy name, and so on.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. If you configure a firewall policy with the **any** interface, you can view the firewall policy list only in which view? _____.
 A. The By Sequence View
 B. The Interface Pair View

DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Good job! You now understand how to manage firewall policies on FortiGate.

Now, you'll learn about best practices and troubleshooting related to firewall policies.

DO NOT REPRINT

© FORTINET

Best Practices and Troubleshooting

Objectives

- Identify naming restrictions for firewall policies and objects
- Reorder firewall policies for correct matching
- Demonstrate how to find matching policies for traffic type

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

By demonstrating competence in knowing firewall policy restrictions and using policy matching techniques, you will be able to apply best practices and basic troubleshooting techniques when working with firewall policies.

DO NOT REPRINT**© FORTINET**

Naming Rules and Restrictions

- Most firewall object name fields accept up to 35 characters
- Supported characters in a firewall object name:
 - Numbers: 0 to 9
 - Letters: A to Z (uppercase and lower case)
 - Special characters: hyphen - and underscore _
 - Spaces
 - Avoid using spaces in general

The screenshot shows the 'Policy & Objects > Addresses' interface. A new address is being created with the name 'Training(LAN)'. An error message 'Invalid characters: < > () # " "' is displayed next to the name field, with the problematic characters highlighted in red. The address is set to a subnet of 10.0.1.0/24 and is associated with port3.

- Some special characters are supported in passwords, comments, replacement messages, and so on
 - < > () # " " '

FORTINET

© Fortinet Inc. All Rights Reserved.

38

When configuring names for firewall objects, only certain characters are supported. For example, Training (LAN) is not a valid name for an address object because it includes special characters that are not supported. Although spaces are supported in the names, as a best practice, avoid using spaces in names. Instead, use a hyphen or underscore. Using spaces can cause issues when trying to modify on the CLI or troubleshooting.

However, many special characters are supported in passwords, comments, replacement messages, and so on.

DO NOT REPRINT

© FORTINET

Best Practices

- Test policies in a maintenance window before deploying in production
 - Test policy for few IP addresses, users, and so on
- Be careful when editing, disabling, or deleting firewall policies and objects
 - Changes are saved and activated immediately
 - Resets active sessions
- Create firewall policies to match as specifically as possible
 - Example: Restrict firewall policies based on source, destination, service
 - Use proper subnetting for address objects
- Analyze and enable appropriate settings on a per-policy basis
 - Security profiles
 - Logging settings



© Fortinet Inc. All Rights Reserved.

39

Always plan a maintenance window and create a test case for a few IP addresses, users, before implementing configuration changes in the production network. Any configuration changes made using the GUI or CLI take effect immediately, and can interrupt service.

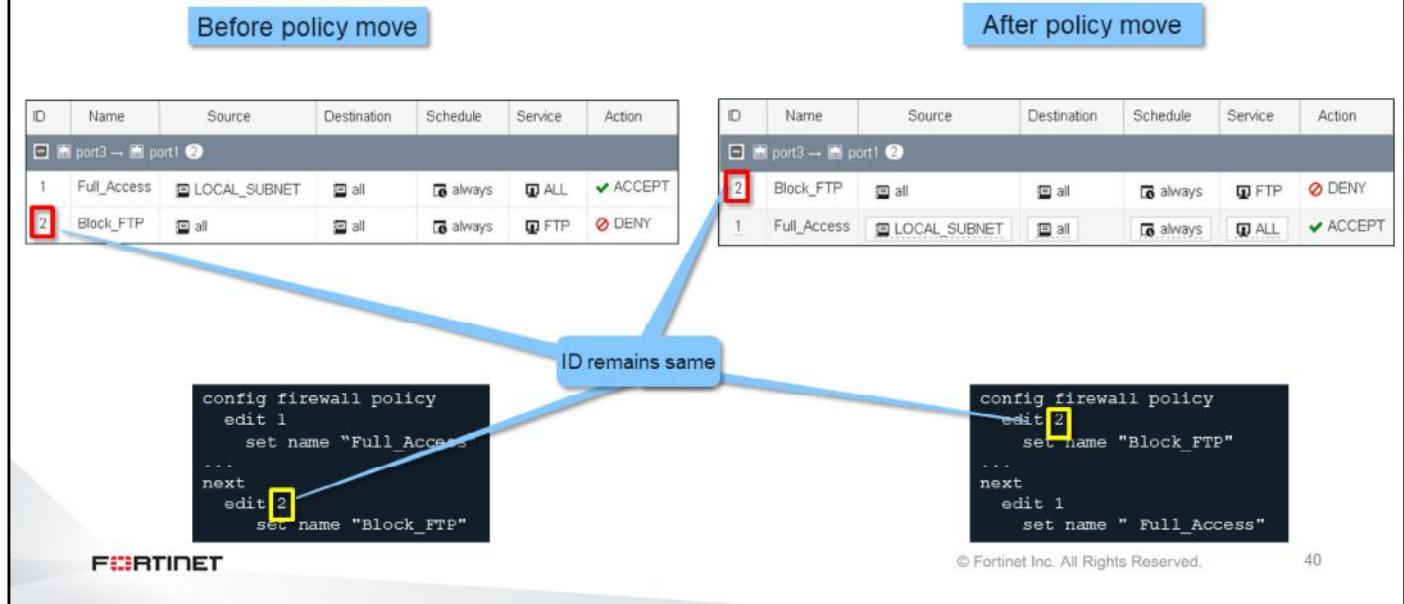
As a best practice, try to configure firewall policies as specifically as possible. This helps to restrict access only to those resources. For example, use proper subnets when configuring address objects.

Another setting worth mentioning is security profiles. Security profiles help to provide appropriate security for your network. Proper logging configuration can also help you to analyze, diagnose, and resolve common network issues.

DO NOT REPRINT**© FORTINET**

Adjusting Policy Order

- On the GUI, drag-and-drop



Remember you learned that only the first matching policy applies? Arranging your policies in the *correct position* is important. It affects which traffic is blocked or allowed. In the applicable interface pair's section, FortiGate looks for a matching policy, beginning at the top. So, you should put more specific policies at the top; otherwise, more general policies will match the traffic first, and more granular policies will never be applied.

In the example shown on this slide, you're moving the **Block_FTP** policy (ID 2) that matches only FTP traffic, to a position above a more general **Full_Access** (accept everything from everywhere) policy. Otherwise, FortiGate would always apply the first matching policy in the applicable interface pairs—**Full_Access**—and never reach the **Block_FTP** policy.

When moving the policies across the policy list, policy IDs remain unchanged.

Note that FortiGate assigns the next highest available ID number as policies are created.

Note that, policy IDs are identifiers and are not displayed by default on the policy list GUI. You can add a policy **ID** column using **Configure Table** settings icon.

DO NOT REPRINT**© FORTINET**

Combining Firewall Policies

- Check the settings before combining firewall policies
 - Source and destination interfaces
 - Source and destination addresses
 - Services
 - Schedules
 - Security profiles
 - Logging
 - NAT rules

Can combine Policy ID 1 and 2 by combining services

Make decisions for logging settings when combining Policy ID 1 and 2

Policy & Objects > Firewall Policy

ID	Name	Source	Destin...	Schedule	Service	Action	NAT	Security Profiles	Log
Port3 → Port1 (2)									
2	Training2	LOCAL	all	always	FTP Web Access	✓ ACCEPT ✓ Enabled	AV default WEB default SSL deep-inspection	UTM	
1	Training1	LOCAL	all	always	ALL_ICMP	✓ ACCEPT ✓ Enabled		All	

FORTINET

© Fortinet Inc. All Rights Reserved.

41

In order to optimize and consolidate firewall policies, always check all configured settings. In this example, the two firewall policies have differences in terms of services, security profiles, and logging settings. You can consolidate these two firewall policies by combining services and choosing appropriate logging settings.

If you select **Security Events** (UTM) for the logging settings, traffic logs will not be generated for **ALL_ICMP** traffic.

Note that the **ALL_ICMP** service is not subject to web filter and antivirus scans, which means that applying these security profiles to the ICMP traffic will result in the traffic passing through without being inspected.

DO NOT REPRINT**© FORTINET**

Policy Lookup (GUI)

- Identify matching policy without real traffic
 - Does not generate any packets
- Searches matching policy based on input criteria
 - Source interface
 - Protocol
 - Requires more granular input criteria
 - Source IP address
 - Destination IP/FQDN
- Policy lookup checks
 - Reverse path forward (RPF)
 - Destination NAT, if matching virtual IP
 - Route lookup, to resolve destination interface



© Fortinet Inc. All Rights Reserved.

42

You can find a matching firewall policy based on the policy lookup input criteria. Policy lookup creates a packet flow over FortiGate without real traffic. From this, policy lookup can extract a policy ID from the flow trace and highlight it on the GUI policy configuration page.

Depending on the protocol you select (for example, TCP, UDP, IP, ICMP, and so on), you need to define other input criteria. For example, when you select TCP as the protocol, you need to define the source address, source port (optional), destination port, and destination address. When you select ICMP as the protocol, you need to define the ICMP type/code, source address, and destination address.

When FortiGate is performing policy lookup, it performs a series of checks on ingress, stateful inspection, and egress, for the matching firewall policy, from top to bottom, before providing results for the matching policy.

Note that if the firewall policy status is set to **disabled**, the policy lookup skips the disabled policy and checks for the next matching policy in the list.

DO NOT REPRINT

© FORTINET

Policy Lookup Example (GUI)

- Highlights matching policy after search

The screenshot shows the FortiGate GUI for 'Policy & Objects > Firewall Policy'. A search dialog box titled 'Policy Lookup' is overlaid on the main table. The search criteria are: Incoming Interface: port3, IP Version: IPv4, Protocol: TCP, Source: 10.0.1.10, Source Port: Optional (1-65535), Destination: fortinet.com, Destination Port: 443. The 'Search' button is highlighted with a red box and arrow. In the main table, three policies are listed. The third policy, 'Training2', is highlighted with an orange background, indicating it is the matching result. The first two policies, 'Training1' and 'FTP', are not highlighted.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Training1	LOCAL_CLIENT	FORTINET	always	ALL_ICMP	ACCEPT	Enabled
2	FTP	all	all	always	FTP	ACCEPT	Enabled
3	Training2	LOCAL_SUBNET	Fortinet_FQDN	always	Web Access ALL_ICMP	ACCEPT	Enabled

© Fortinet Inc. All Rights Reserved. 43

Based on the input criteria, after clicking **Search**, the trace result will be selected and highlighted on the **Firewall Policy** page.

Why didn't policy **ID #1** or **ID #2** match the input criteria?

Because policy **ID #1** status is set to **disable**, policy lookup skips the disabled policy. For firewall policy **ID #2**, it doesn't match the destination port specified in the policy lookup matching criteria.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which of the following naming formats is correct when configuring a name for a firewall address object?
 A. Good_Training
 B. Good(Training)

2. What is the purpose of the policy lookup feature on FortiGate?
 A. To find a matching policy based on input criteria
 B. To block traffic based on input criteria



© Fortinet Inc. All Rights Reserved.

44

DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify components of firewall policies
- ✓ Identify how FortiGate matches traffic to firewall policies
- ✓ Restrict access and make your network more secure using security profiles
- ✓ Configure logging
- ✓ Identify policy list views
- ✓ Understand the use of policy IDs
- ✓ Identify where an object is referenced
- ✓ Identify naming restrictions for firewall policies and objects
- ✓ Reorder firewall policies for correct matching
- ✓ Demonstrate how to find matching policies for traffic type

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

By mastering the objectives covered in this lesson, you learned how to configure, use, and manage firewall policies.

DO NOT REPRINT**© FORTINET****FORTINET**

FortiGate Security

Network Address Translation (NAT)

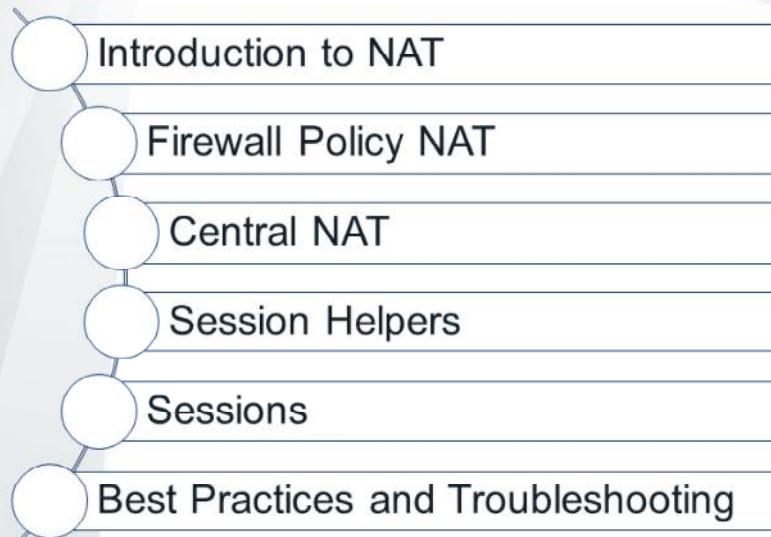
FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.Last Modified: 29 May 2020

In this lesson, you will learn how to configure network address translation (NAT) and use it to implement source NAT and destination NAT for the traffic passing through FortiGate.

DO NOT REPRINT**© FORTINET**

Lesson Overview



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

DO NOT REPRINT

© FORTINET

Introduction to NAT

Objectives

- Understand NAT and port address translation (PAT)
- Understand the different configuration modes available for NAT

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

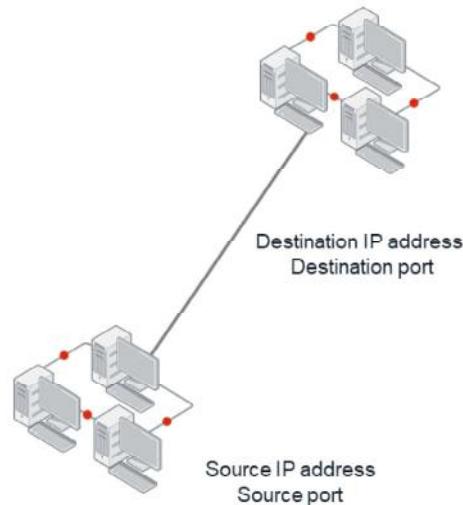
By demonstrating competence in understanding how NAT and PAT work, and the available NAT configuration modes, you will have a good start for planning the implementation of NAT in your network.

DO NOT REPRINT

© FORTINET

NAT and PAT

- NAT
 - Changes the IP layer address of a packet
 - Some protocols, like SIP, have addresses at the application layer, requiring session helpers or proxies
 - Source NAT (SNAT)
 - Destination NAT (DNAT)
- PAT (NAT overload)
 - Map multiple private IPv4 addresses to a single public IP address by using different source ports
- NAT64 and NAT46
 - A mechanism that allows IPv6 addressed hosts to communicate with IPv4 addressed hosts and the reverse
- NAT66
 - NAT between two IPv6 networks



FORTINET

© Fortinet Inc. All Rights Reserved.

4

NAT is the process that enables a single device, such as a firewall or router, to act as an agent between the Internet, or public network, and a local, or private, network.

NAT is usually implemented for one, or a combination, of the following reasons:

- Improved security: The addresses behind the NAT device are virtually hidden.
- Amplification of addresses: Hundreds of computers can use as few as one public IP address.
- Internal address stability: The addresses can stay the same, even if Internet service providers (ISPs) change.

NAT and PAT, also known as NAPT, translate internal, typically private, IP addresses to external, typically public or Internet, IP addresses. In FortiOS, NAT and traffic forwarding apply to the same firewall policy. However, diagnostics clearly show NAT and forwarding as separate actions.

- For outgoing connections: The NAT option in a central SNAT, IP pool, and central SNAT table can be used and is known as *source NAT*.
- For incoming connections: Virtual IPs (VIPs) and DNAT can be used and are known as *destination NAT*.

NAT64 and NAT46 are the terms used to refer to the mechanism that allows IPv6 addressed hosts to communicate with IPv4 addressed hosts and the reverse. Without this mechanism, an IPv6 node on a network, such as a corporate LAN, would not be able to communicate with a website that was in an IPv4-only environment, and IPv4 environments would not be able to connect to IPv6 networks.

NAT66 is NAT between two IPv6 networks.

DO NOT REPRINT**© FORTINET**

Configuration Modes for NAT

- There are two ways to configure SNAT and DNAT:
 - Firewall policy NAT
 - SNAT and DNAT must be configured for each firewall policy
 - SNAT uses the outgoing interface address or configured IP pool
 - DNAT uses the configured VIP as the destination address
 - Central NAT
 - SNAT and DNAT configurations are done per virtual domain
 - It applies to multiple firewall policies, based on SNAT and DNAT rules
 - SNAT rule is configured from central SNAT policy
 - DNAT is configured from DNAT and VIPs



When you use firewall policy NAT mode, you must configure SNAT and DNAT for each firewall policy.

Central NAT configurations are done per virtual domain, which means SNAT and DNAT configurations automatically apply to multiple firewall policies. This is according to the SNAT and DNAT rules that you specify, as opposed to each firewall policy in firewall policy NAT.

As a best practice, when you use central NAT, you should configure specific SNAT and DNAT rules, so that they match only the desired firewall policies in your configuration.

Both firewall policy NAT and central NAT produce the same results; however, some deployment scenarios are best suited to firewall policy NAT and some are best suited to central NAT.

Firewall policy NAT is suggested for deployments that include relatively few NAT IP addresses and where each NAT IP address would have separate policies and security profiles. Central NAT is suggested for more complex scenarios where multiple NAT IP addresses have identical policies and security profiles, or in next generation firewall (NGFW) policy mode, where the appropriate policy may not be determined at the first packet.

DO NOT REPRINT**© FORTINET**

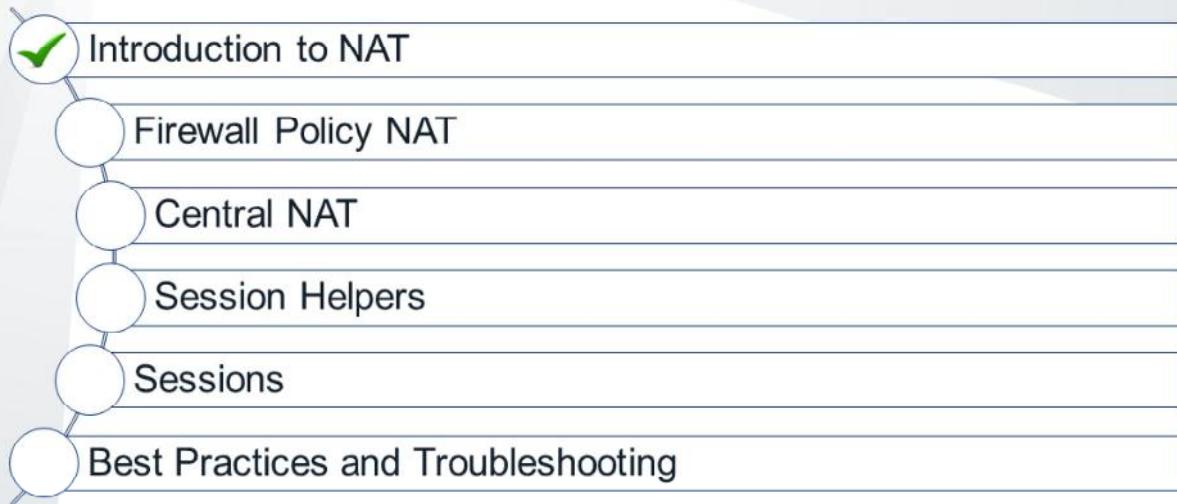
Knowledge Check

1. What is NAT used for?
 A. Preserving IP addresses
B. Traffic shaping

2. Which statement about NAT66 is true?
 A. It is NAT between two IPv6 networks.
B. It is NAT between two IPv4 networks.

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now know about NAT.

Now, you'll learn about firewall policy NAT.

DO NOT REPRINT**© FORTINET**

Firewall Policy NAT

Objectives

- Configure a firewall policy to perform SNAT and DNAT (VIP)
- Apply SNAT with IP pools
- Configure DNAT with VIPs or a virtual server

After completing this section, you should be able to achieve the objectives shown on this slide. By demonstrating competence in these areas, you will be able to configure firewalls policies and apply appropriate SNAT and DNAT, and understand how it is applied to the traffic traversing through FortiGate.

DO NOT REPRINT**© FORTINET**

Firewall Policy SNAT

- There are two ways to SNAT traffic:
 - Using the outgoing interface address
 - Using the dynamic IP pool

Policy & Objects > Firewall Policy

Edit Policy	
Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input type="radio"/> Use Outgoing Interface Address <input checked="" type="radio"/> Use Dynamic IP Pool

© Fortinet Inc. All Rights Reserved. 9

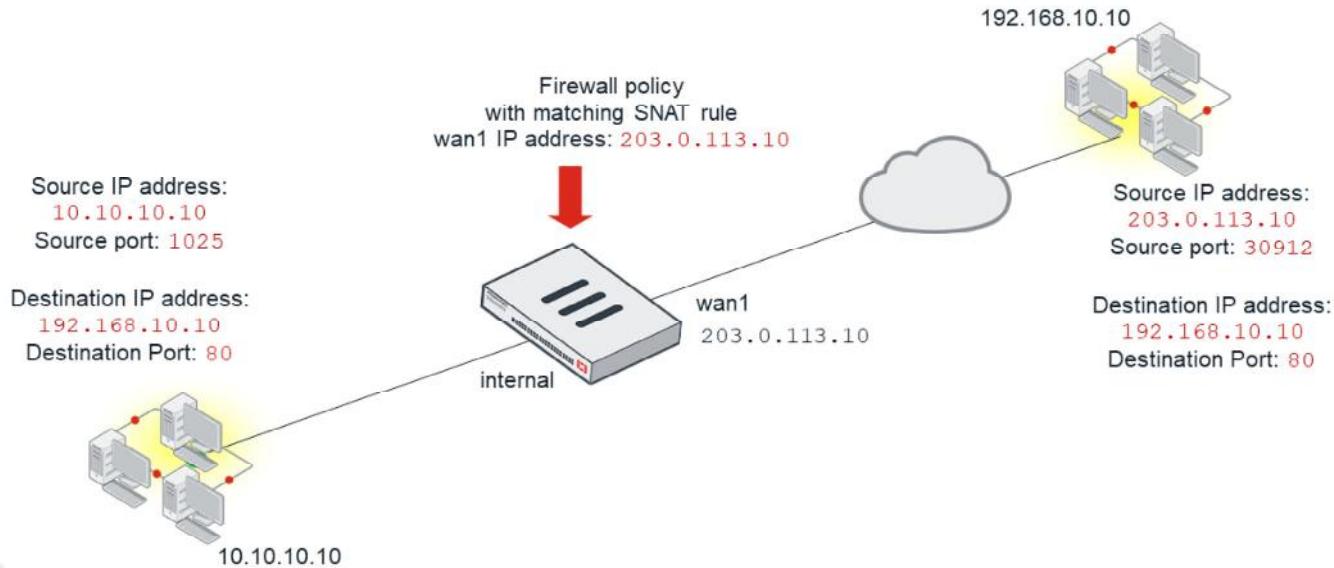
FORTINET

There two ways to configure firewall policy SNAT:

- Use the outgoing interface address
- Use the dynamic IP pool

DO NOT REPRINT**© FORTINET**

Firewall Policy SNAT Using the Outgoing Interface

**FORTINET**

© Fortinet Inc. All Rights Reserved.

10

The source NAT option uses the egress interface address when NAT is enabled on the firewall policy. This is many-to-one NAT. In other words, PAT is used, and connections are tracked using the original source address and source port combinations, as well as the allocated source port. This is the same behavior as the overload IP pool type, which you will also learn about.

Optionally, you may select a fixed port, in which case the source port translation is disabled. With a fixed port, if two or more connections require the same source port for a single IP address, only one connection can establish.

In the example shown on this slide, a firewall policy from internal to wan1 (IP address 203.0.113.10) is created, and the user initiates traffic from source 10.10.10.10:1025 destined for 192.168.10.10:80. Because NAT is enabled on the firewall policy, the source IP address is translated to the egress interface IP, with port translation.

DO NOT REPRINT

© FORTINET

IP Pools

- IP pools define a single IP address or a range of IP addresses to be used as the source address for the duration of the session
- IP pools are usually configured in the same range as the interface IP address
- There are four types of IP pools:
 - Overload (default)
 - One-to-one
 - Fixed port range
 - Port block allocation

Policy & Objects > IP Pools

New Dynamic IP Pool

Name	<input type="text"/>
Comments	<input type="text"/> Write a comment... 0/255
Type	<input checked="" type="radio"/> Overload <input type="radio"/> One-to-One <input type="radio"/> Fixed Port Range <input type="radio"/> Port Block Allocation
External IP address/range	<input type="text"/> 0.0.0.0-0.0.0.0
ARP Reply	<input checked="" type="checkbox"/>

FORTINET

Policy & Objects > Firewall Policy

Edit Policy

Name	Full_Access
Incoming Interface	<input checked="" type="checkbox"/> port3
Outgoing Interface	<input checked="" type="checkbox"/> port1
Source	<input checked="" type="checkbox"/> LOCAL_SUBNET
Destination	<input checked="" type="checkbox"/> all
Schedule	<input checked="" type="checkbox"/> always
Service	<input checked="" type="checkbox"/> ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	Use Outgoing Interface Address <input checked="" type="checkbox"/> Use Dynamic IP Pool <input checked="" type="radio"/> INTERNAL-HOST-EXT-IP

© Fortinet Inc. All Rights Reserved. 11

IP pools are a mechanism that allow sessions leaving the FortiGate firewall to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses will be used instead of the IP address assigned to that FortiGate interface.

IP pools are usually configured in the same range as the interface IP address.

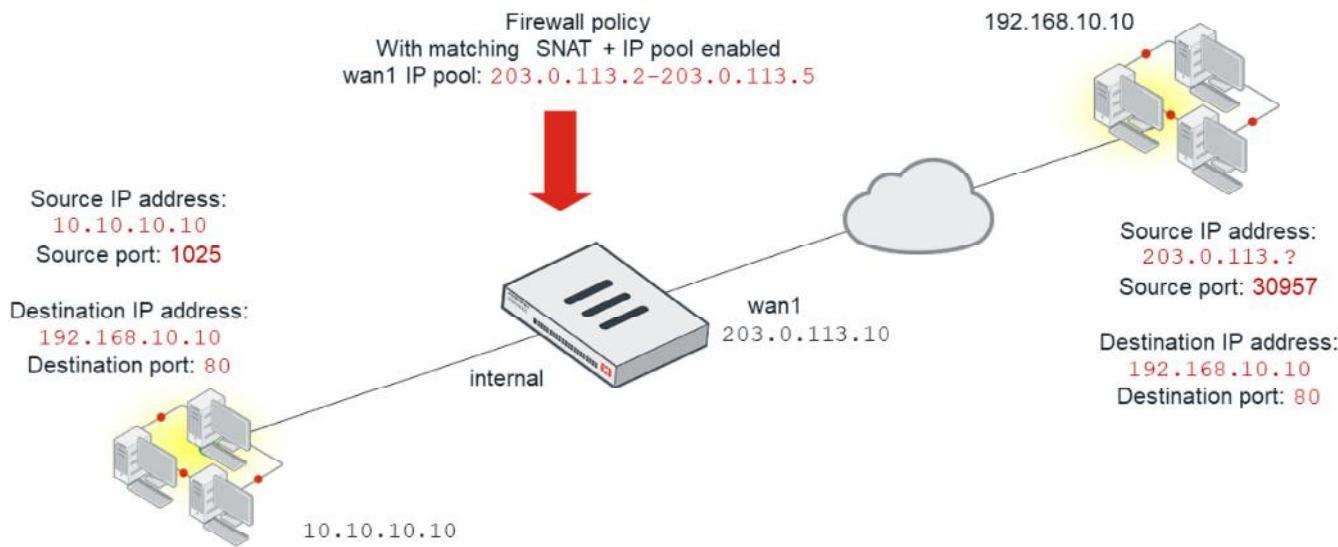
When you configure the IP pools that will be used for NAT, there is a limitation that you must take into account. If the IP addresses in the IP pool are different from the IP addresses that are assigned to the interface(s), communications based on those IP addresses *may fail if the routing is not properly configured*. For example, if the IP address assigned to an interface is 172.16.100.1/24, you cannot choose 10.10.10.1 to 10.10.10.50 for the IP pool unless appropriate routing is configured.

There are four types of IP pools that can be configured on the FortiGate firewall:

- Overload
- One-to-one
- Fixed port range
- Port block allocation

DO NOT REPRINT**© FORTINET**

IP Pool Type—Overload

**FORTINET**

© Fortinet Inc. All Rights Reserved.

12

If you use an IP pool, the source address is translated to an address from that pool, rather than the egress interface address. The larger the number of addresses in the pool, the greater the number of connections that can be supported. For example, in an enterprise network where you require a greater number of connections, or in a network where you want one subnet to use one specific public IP over another to restrict access based on source IP address.

The default IP pool type is overload. In the overload IP pool type, a many-to-one or many-to-few relationship and port translation is used.

In this example, source IP 10.10.10.10 will be translated to an IP address from the IP pool (203.0.113.2 – 203.0.113.5).

DO NOT REPRINT**© FORTINET**

IP Pool Type—One-to-One

- The IP pool type one-to-one associates an internal IP with a pool IP on a first-come, first-served basis
 - PAT is disabled

```
STUDENT # get system session list
PROTO EXPIRE SOURCE SOURCE-NAT DESTINATION DESTINATION-NAT
tcp 3598 10.0.1.10:2706 10.200.1.6:2706 10.200.1.254:80 -
tcp 3598 10.0.1.10:2704 10.200.1.6:2704 10.200.1.254:80 -
tcp 3596 10.0.1.10:2702 10.200.1.6:2702 10.200.1.254:80 -
tcp 3599 10.0.1.10:2700 10.200.1.6:2700 10.200.1.254:443 -
tcp 3599 10.0.1.10:2698 10.200.1.6:2698 10.200.1.254:80 -
tcp 3598 10.0.1.10:2696 10.200.1.6:2696 10.200.1.254:443 -
udp 174 10.0.1.10:2694 - 10.0.1.254:53 -
udp 173 10.0.1.10:2690 - 10.0.1.254:53 -
```

- Refuses the connection if there is no unallocated address

FORTINET

© Fortinet Inc. All Rights Reserved.

13

In the one-to-one pool type, an internal IP address is mapped with an external address on a first-come, first-served basis.

There is a single mapping of an internal address to an external address. Mappings are not fixed and, if there are no more addresses available, a connection will be refused.

Also, in one-to-one, PAT is not required. In the example on this slide, you can see the same source port is shown for both the ingress and egress address.

DO NOT REPRINT**© FORTINET**

IP Pool Type—Fixed Port Range

- The fixed port range IP pool type associates an internal IP range with an external IP range
 - A type of PAT

STUDENT	#	get system session list	PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT
			tcp	3574	10.0.1.11:60843	10.200.1.8:60843	216.23.154.83:80	-
			tcp	3570	10.0.1.11:60809	10.200.1.8:60809	216.23.154.81:80	-
			tcp	3590	10.0.1.11:60819	10.200.1.8:60819	216.23.154.74:80	-
			tcp	3599	10.0.1.11:60817	10.200.1.8:60817	216.23.154.74:80	-
			tcp	3586	10.0.1.11:60815	10.200.1.8:60815	216.23.154.81:80	-
			tcp	3564	10.0.1.11:60807	10.200.1.8:60807	216.23.154.74:80	-
			tcp	9	10.0.1.10:7112	10.200.1.7:7112	10.200.1.254:80	-
			tcp	7	10.0.1.10:7110	10.200.1.7:7110	10.200.1.254:80	-
			tcp	5	10.0.1.10:7108	10.200.1.7:7108	10.200.1.254:80	-
			tcp	3	10.0.1.10:7106	10.200.1.7:7106	10.200.1.254:80	-
			tcp	1	10.0.1.10:7104	10.200.1.7:7104	10.200.1.254:80	-



For the overload and one-to-one IP pool types, we do not need to define the internal IP range. For the fixed port range type of IP pool, we can define both internal IP range and external IP range.

Since each external IP address and the number of available port numbers is a specific number, if the number of internal IP addresses is also determined, we can calculate the port range for each address translation combination. So we call this type fixed port range. This type of IP pool is a type of port address translation (PAT).

The fixed port range allows fixed mapping of the internal start IP or internal end IP range to the external start IP or external end IP range.

The example on this slide shows a fixed port range IP pool. The internal address range 10.0.1.10 to 10.0.1.11 maps to the external address range 10.200.1.7 to 10.200.1.8.

DO NOT REPRINT**© FORTINET**

IP Pool Type—Port Block Allocation

- The port block allocation IP pool type assigns a block size and number per host for a range of external IP addresses

- Using a small 64-block size and 1 block
 - hping --faster -p 80 -S 10.200.1.254

```
STUDENT # diagnose sys session stat
misc info:          session_count=79 setup_rate=0 exp_count=0 clash=0
                     memory_tension_drop=0 ephemeral=0/65536 removable=0
                     delete=0, flush=0, dev_down=0/0 ses_flush_filters=0
TCP sessions:
              2 in ESTABLISHED state
              74 in SYN_SENT state
              1 in CLOSE_WAIT state
```

- Using an overload type
 - hping --faster -p 80 -S 10.200.1.254

```
STUDENT # diagnose sys session stat
misc info:          session_count=10227 setup_rate=982 exp_count=0 clash=0
                     memory_tension_drop=0 ephemeral=0/65536 removable=0
                     delete=0, flush=0, dev_down=0/0 ses_flush_filters=0
TCP sessions:
              34 in ESTABLISHED state
              10117 in SYN_SENT state
              1 in SYN_RECV state
```

FORTINET

© Fortinet Inc. All Rights Reserved.

15

IP Pool type port block allocation is also a type of PAT. It gives users a more flexible way to control the way external IPs and ports are allocated.

Users need to define **Block Size** and **Block Per User** and external IP range. **Block Size** means how many ports each block contains. **Block per User** means how many blocks each host or (internal IP) can use.

The two CLI outputs shown on this slide illustrate the behavior difference between the port block allocation IP pool type and the default overload IP pool type.

Using hping, a rogue client generates many SYN packets per second. In the first example, the port block allocation type limits the client to 64 connections for that IP pool. Other users will not be impacted by the rogue client.

In the second example, the overload type imposes no limits, and the rogue client uses many more connections in the session table. Other users will be impacted.

Port block allocation timeout period is configurable on the FortiGate CLI.

DO NOT REPRINT

© FORTINET

Virtual IPs (VIPs)

- DNAT objects
- Default type is static NAT
 - Can be restricted to forward only certain ports
- On the CLI, you can specify load-balance or server-load-balance
- VIPs should be routable to the external facing (ingress) interface for return traffic

The screenshot displays two configuration pages from the FortiGate management interface:

- Policy & Objects > Virtual IPs**: Shows the configuration for a new Virtual IP named "VIP-INTERNAL-HOST". It is set to IPv4, has an incoming interface of "port1", and an outgoing interface of "port3". The type is "Static NAT" with an external IP of "100.64.100.22" and a mapped internal IP of "10.0.1.10".
- Policy & Objects > Firewall Policy**: Shows a policy named "Web-Server-Access" with the following settings:
 - Source**: All (selected)
 - Destination**: VIP-INTERNAL-HOST (selected)
 - Schedule**: Always
 - Service**: HTTP and HTTPS (selected)
 - Action**: ACCEPT (selected)
 - Inspection Mode**: Flow-based (selected)

A blue callout box points from the "Destination" field in the Firewall Policy to the "VIP-INTERNAL-HOST" entry in the policy list, with the text: "VIP used as destination in firewall policy".

Fortinet Inc. All Rights Reserved. 16

VIPs are DNAT objects. For sessions matching a VIP, the destination address is translated: usually a public Internet address is translated to a server's private network address. VIPs are selected in the firewall policy's **Destination** field.

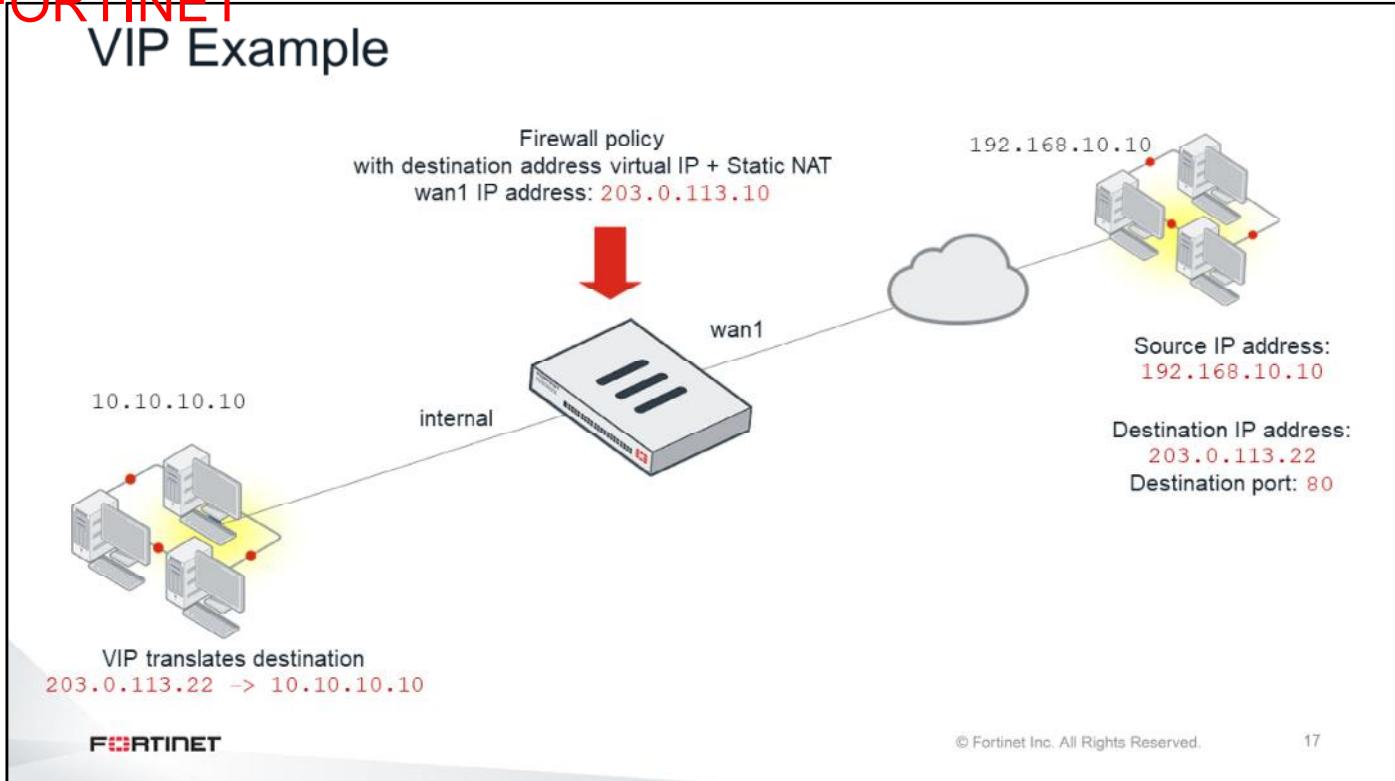
The default VIP type is static NAT. This is a one-to-one mapping, which applies for incoming and outgoing connections; that is, an outgoing policy with NAT enabled would use the VIP address instead of the egress interface address. However, this behavior can be overridden using an IP pool.

The static NAT VIP can be restricted to forward only certain ports. For example, connections to the external IP on port 8080 map to the internal IP on port 80.

On the CLI, you can select the NAT type as load-balance and server-load-balance. Plain load balancing distributes connections from an external IP address to multiple internal addresses. Server load balancing builds on that mechanism, using a virtual server and real servers, and provides session persistence and server availability check mechanisms.

VIPs should be routable to the external facing (ingress) interface. FortiOS responds to ARP requests for VIP and IP pool objects. ARP responses are configurable.

DO NOT REPRINT
© FORTINET
VIP Example



In this example, source IP address 192.168.10.10 is trying to access destination IP address 203.0.113.22 over port TCP 80.

Connections to the VIP 203.0.113.22 are NATed to the internal host 10.10.10.10.

Because this is a static NAT, all NATed outgoing connections from 10.10.10.10 will use VIP address 203.0.113.22 in the packet's IP source field and not the egress interface IP address 203.0.113.10.

DO NOT REPRINT

© FORTINET

Matching Policies—VIP

- Default behavior: firewall address objects do not match VIPs
 - Doesn't block an egress-to-ingress connection, even when the deny policy is at the top of the list.
- VIP policy (WAN to LAN)

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3)						
2	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Web_server	always	ALL	ACCEPT

Action = Deny

- Two ways to resolve it by modifying the deny policy:

- Enable match-vip in deny policy

```
config firewall policy
edit <policy ID for deny>
set match-vip enable
end
```

- Set the destination address as VIP object

```
config firewall policy
edit <policy ID for deny>
set dstaddr "VIP object"
end
```

Can still access the VIP from the policy below, even though the deny policy is at the top of the list.

FORTINET

© Fortinet Inc. All Rights Reserved.

18

In FortiOS, VIPs and firewall address objects are completely different, they are stored separately with no overlap. By default, firewall address objects do not match VIPs. In the example shown on this slide, the **all** address object as a destination in the first policy does not include any VIPs, so traffic destined to the Webserver VIP will skip the first policy and match the second **Allow_access**. In order for the first policy to match the VIP, you either need to edit the policy on the CLI and set **match-vip enable**, which allows address objects to match the VIP address, or change the destination address of the first policy to be the VIP in question.

Traffic is permitted to fall through to the next policy; however, when you use VIP firewall policies, there can be some exceptions.

When VIP(s) are configured, for incoming (WAN to LAN) connections, it will be first matched against the VIP table.

In the example shown on this slide, a firewall policy from WAN to LAN is configured with a specific source and the action is **Deny**. There is second firewall policy that is allowing access to the VIP (the destination address). Even though the deny firewall policy is at the top of the list, the denied source is still allowed by the second firewall policy to access the VIP.

In order to block traffic from the denied source, you must enable **set match-vip enable** in the deny firewall policy, which skips the VIP id checking. Alternatively, you can configure the destination address as the virtual IP in the deny policy instead of **all**.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is the default IP pool type?
 - A. One-to-one
 - B. Overload

2. Which of the following is the default VIP type?
 - A. static-nat
 - B. load-balance

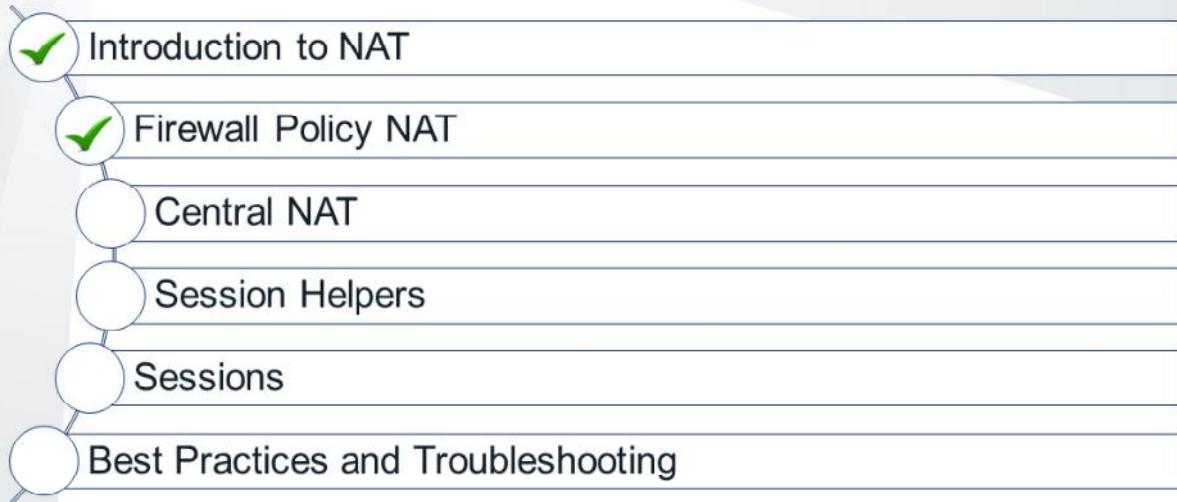


© Fortinet Inc. All Rights Reserved.

19

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand firewall policy NAT.

Now, you'll learn about central NAT.

DO NOT REPRINT

© FORTINET

Central NAT

Objectives

- Configure central NAT

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

By demonstrating competence in configuring central NAT to perform SNAT and DNAT, you will be able to use NAT on a more granular level to control IP address, protocol, and port translation.

DO NOT REPRINT**© FORTINET**

Central NAT

- Enabled or disabled on the CLI *only*

```
config system settings
  set central-nat {enable|disable}
end
```

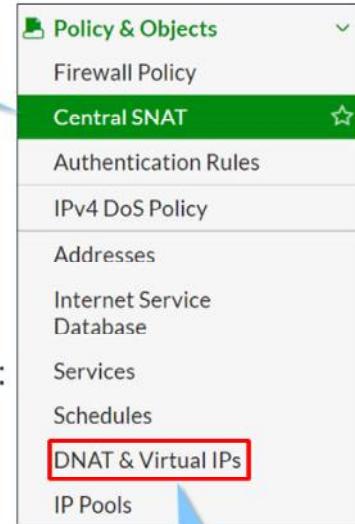
- Must remove VIP and IP pool references from existing policies*

```
config system settings
  set central-nat enable
Cannot enable central-nat with firewall policy using vip (id=2).
```

- Once enabled, these two options are available on the GUI:
 - Central SNAT
 - DNAT & Virtual IPs

- Central SNAT is mandatory for NGFW policy-based mode

Source NAT



Destination NAT

FORTINET

© Fortinet Inc. All Rights Reserved.

22

By default, central NAT is disabled and can only be enabled on the CLI. After central NAT is enabled, these two options are available to be configured on the GUI:

- Central SNAT
- DNAT & Virtual IPs

What happens if you try to enable central NAT, but there are still IP pool or VIPs configured in firewall policies?

The CLI will not allow this and will present a message referencing the firewall policy ID with the VIP or IP pool. You *must* remove VIP or IP pool references from existing firewall policies in order to enable central NAT.

Central SNAT is mandatory for the new NGFW mode in policy-based. This means SNAT behaves only according to the NAT settings found by clicking **Policy & Objects > Central SNAT**.

DO NOT REPRINT

© FORTINET

Central SNAT

- SNAT configuration changes when central NAT is enabled

Central NAT Enabled	Steps to Configure
SNAT	<ol style="list-style-type: none"> Define IP pool or use outgoing interface address Configure central SNAT policy

- Central SNAT rules process from top to bottom
 - SNAT policy is selected according to the configuration of the firewall policy that matches the traffic.
 - If no matching central SNAT rule exists, NAT will not be applied
- Matching criteria is based on:
 - Source interface
 - Destination interface
 - Source address
 - Destination address
 - Protocol
 - Source port
 - Most protocols don't need this

Policy & Objects > Central SNAT

ID	From	To	Source Address	Destination Address	Translated Address	Protocol Number
1	LAN (port3)	WAN (port1)	all	all	SNAT-Pool	6
2	port2	WAN (port1)	all	REMOTE_FORTIGATE	INTERNAL-HOST-EXT-IP	1



© Fortinet Inc. All Rights Reserved.

23

You can have more granular control, based on source and destination interfaces in the central SNAT policy, over traffic passing through firewall policies.

You can now define matching criteria in the central SNAT policy, based on:

- Source interface
- Destination interface
- Source address
- Destination address
- Protocol
- Source port

Starting in FortiOS version 6.0, a matching central SNAT policy is mandatory for all firewall policies. If there is no matching SNAT policy, no NAT will be applied and session will be created using original source IP address.

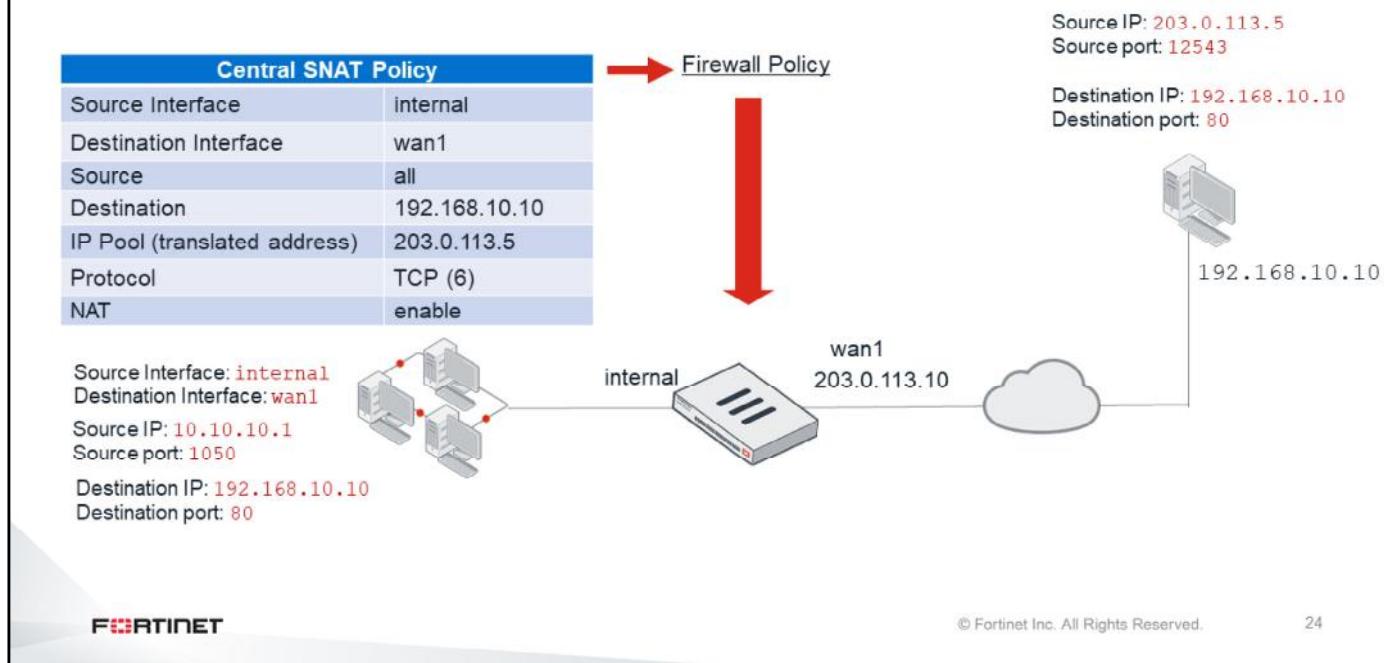
If the central SNAT policy criteria matches the traffic based on multiple firewall policies, the central SNAT policy will be applied to those firewall policies.

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

DO NOT REPRINT

© FORTINET

Central SNAT Example



In the example shown on this slide, the central SNAT policy translates the source IP address to the defined IP pool address (203.0.113.5). However, the translation takes place only if the traffic matches all the variables defined in the central SNAT policy, that is, traffic from the source IP address through the source interface internal to FortiGate must be destined for destination IP address (192.168.10.10) through destination interface wan1 and the protocol must be TCP. For illustration purposes, only a single IP address is used for the destination, and the IP pool type is set to overload with a single IP address.

The firewall policy is created from internal to wan1 . There is no NAT option available in FortiOS version 6.0 onwards firewall policy, and matching SNAT policy is mandatory to pass the traffic. If there is no matching central SNAT policy, no NAT will be applied and session will be created using original source IP address.

If the user tries any TCP-based sessions (for example HTTP, HTTPS) to the destination IP address 192.168.10.10, the source IP address will be translated to an IP pool address or addresses defined in the central NAT policy.

What if the user tries to send any ICMP or UDP-based traffic to 192.168.10.10? Will the source address be translated to the IP pool defined in the central NAT policy?

As the central SNAT policy does not match, FortiGate will apply no NAT. What if the user tries TCP-based traffic to another destination IP address, 192.168.10.20? Will the source address be translated to the IP pool defined in the central SNAT policy?

Again, the destination IP address of 192.168.10.20 does not match the central NAT policy, so FortiGate will not apply NAT and firewall session will be created using original source IP.

DO NOT REPRINT**© FORTINET**

Central DNAT and VIPs

- Enabling central NAT changes the DNAT configuration

Central NAT Enabled	Steps to Configure
Destination NAT (VIP)	Define DNAT & Virtual IPs (No additional configurations required)

- As soon as a VIP is created, a rule is created in the kernel to allow DNAT to occur
 - Firewall policy destination address—all or mapped IP of VIP
 - VIP cannot be selected in the firewall policy as the destination address



© Fortinet Inc. All Rights Reserved.

25

Traditionally on FortiGate, VIPs are selected in the firewall policy as the destination address.

On FortiGate, you can configure DNAT and VIPs for DNAT. As soon as a VIP is configured, FortiGate automatically creates a rule in the kernel to allow DNAT to occur. No additional configuration is required.

Do you lose the granularity of being able to define a firewall policy for a specific VIP and services?

No, you don't. If you have several WAN-to-internal policies and multiple VIPs, and you want to allow specific services for specific VIPs, you can define each firewall policy with the destination address of the mapped IP of the VIP, and select the appropriate services to allow or deny.

Note that if both central SNAT and central DNAT (VIP) are configured, the outgoing (internal-to-WAN) traffic will source NAT, based on the matching central SNAT policy configurations and if there is not matching central SNAT policy no NAT will applied outgoing traffic.

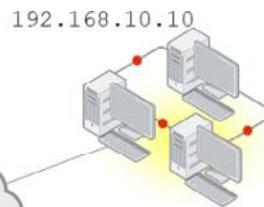
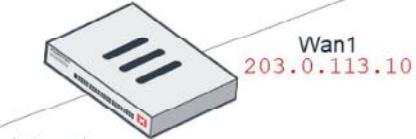
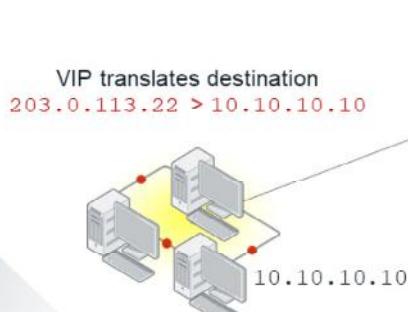
DO NOT REPRINT

© FORTINET

DNAT and VIPs Example

DNAT & Virtual IPs	
External IP/Address Range	203.0.113.22
Mapped IP Address/Range	10.10.10.10

Firewall policy destination address – all or mapped IP of VIP



Source IP address:
192.168.10.10

Destination IP address:
203.0.113.22
Destination port: 80

© Fortinet Inc. All Rights Reserved.

26

In the example shown on this slide, a DNAT and VIP rule is created to map external IP address 203.0.113.22 to internal IP address 10.10.10.10. Remember, as soon as a VIP is created, a rule is created in the kernel to allow DNAT to occur.

The firewall policy from wan1 to internal is created with the destination address **all** or **Mapped IP Address/Range** (10.10.10.10) of the VIP.

The source IP address 192.168.10.10 is trying to access the destination IP address 203.0.113.22 over port TCP 80. Connections to the VIP 203.0.113.22 are NATed to the internal host 10.10.10.10, without any additional configuration.

DO NOT REPRINT**© FORTINET**

Disabling Central NAT

- If central NAT is enabled and configured for SNAT and DNAT, and then disabled, the following will occur:
 - Outgoing traffic SNAT will no longer be performed
 - Incoming traffic that was previously configured with DNAT and VIPs will stop working because there will be no rule present in the kernel for DNAT



© Fortinet Inc. All Rights Reserved.

27

You can disable central NAT on the CLI by running `set central-nat disable` under the `config system` setting. What happens to firewall policies that are using central SNAT and DNAT rules, if central NAT is disabled?

For new firewall sessions, the incoming to outgoing firewall policies will no longer perform SNAT. You must manually edit firewall policies to enable NAT and select appropriate IP pool addresses, which were previously tied to the central SNAT policy.

Egress-to-ingress firewall policies that use DNAT and VIP will no longer perform DNAT. In central NAT, the destination address in the firewall policy is simply an address object, not an actual VIP. Without the central NAT hook into the DNAT table, the address object will cause a forward policy check failure—the traffic will be denied by policy ID 0.

You must edit the egress-to-ingress firewall policies and select VIP as the destination address.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which statement is true?
 A. Central NAT is not enabled by default.
 B. Both central NAT and firewall policy NAT can be enabled together.

2. What happens if there is no matching central SNAT policy or no central SNAT policy configured?
 A. The egress interface IP will be used.
 B. NAT will not be applied to firewall session.

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand central NAT.

Now, you'll learn about session helpers.

DO NOT REPRINT**© FORTINET**

Session Helpers

Objectives

- Understand how session helpers work
- Use a SIP session helper for VoIP

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

By demonstrating competence in understanding how session helpers work, you will be able to use session helpers to analyze data in the packets of some protocols and allow those protocols to pass traffic through FortiGate.

DO NOT REPRINT**© FORTINET**

Session Helpers

- Some traffic types require more packet modification for the application to work (configurable on the CLI), examples include:
 - The handling of FTP active mode connections—the control connection is separate from the data connection
 - Header rewrites in SIP SDP payloads required because of NAT actions
- To show configured session helpers, use this command:
 - `show system session-helper`
- Application layer gateway (ALG)
 - When more advanced application tracking and control is required, an ALG can be used—the VOIP profile is an example of an ALG.



© Fortinet Inc. All Rights Reserved.

31

Some application layer protocols are not fully independent of the lower layers, such as the network or transport layers. The addresses may be repeated in the application layer, for example. If the session helper detects a pattern like this, it may change the application headers, or create the required secondary connections.

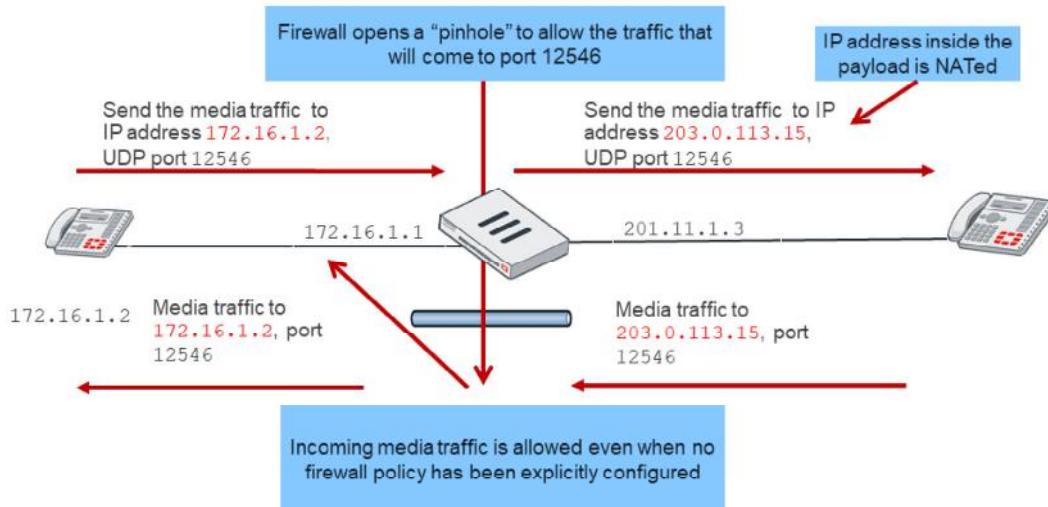
A good example of this is an application that has both a control channel and a data or media channel, such as FTP. Firewalls will typically allow the control channel and rely on the session helpers to handle the dynamic data or media transmission connections.

When more advanced application tracking and control is required, ALG can be used. The VOIP profile is an example of an ALG.

DO NOT REPRINT**© FORTINET**

Session Helpers—SIP Example

- Stateful firewall with NAT of 172.16.1.2 to 203.0.113.15

**FORTINET**

© Fortinet Inc. All Rights Reserved.

32

In the examples shown on this slide, the media recipient address in the SIP SDP payload is modified to reflect the translated IP address.

Notice how, because firewall policies are stateful, a pinhole is opened to allow reply traffic, even though you have not explicitly created a firewall policy to allow incoming traffic. This concept is used with some other protocols, such as NAT-T for IPsec.

DO NOT REPRINT**© FORTINET**

Knowledge Check

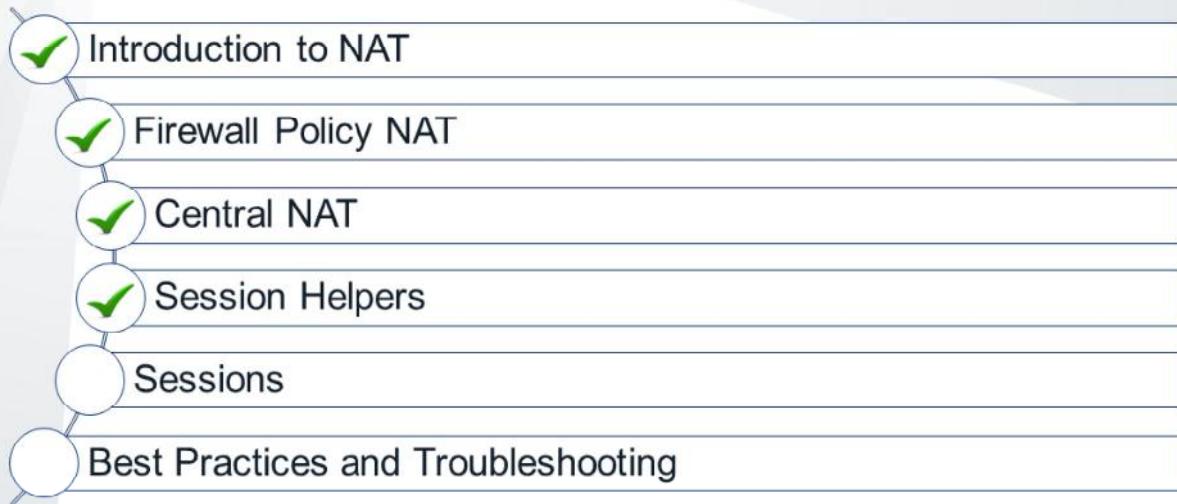
1. Which method would you use for advanced application tracking and control?
 - A. Session helper
 - B. Application layer gateway

2. Which profile is an example of application layer gateway?
 - A. WAF profile
 - B. VOIP profile



DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand session helpers.

Now, you'll learn about sessions.

DO NOT REPRINT**© FORTINET**

Sessions

Objectives

- Understand the session table on FortiGate
- Understand the session time to live (TTL)
- Analyze session diagnose command output
- Understand the TCP, UDP, and ICMP states on FortiGate

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

By demonstrating competence in understanding how a session table keeps track of the session information, you will be better able to use that information to understand the actions applied to traffic, such as SNAT, DNAT, and routing.

DO NOT REPRINT**© FORTINET**

Session Table

- Accepted IP sessions are tracked in the kernel's session table, but this can be affected by hardware acceleration
- The session table stores the following information about the session:
 - The source and destination addresses, port number pairs, state, and timeout
 - The source and destination interfaces
 - The source and destination NAT actions
- The session table stores the following performance metrics:
 - Maximum concurrent sessions
 - New sessions per second

Dashboard > Top Sources > <select a source> >Sessions

Applications	Destinations	Threats	Web Sites	Web Categories	Policies	Sessions	Search Phrases	
Date/Time	Source	Source Interface	Source NAT IP	Source NAT Port		Destination	Destination Interface	Sent / Received
2020/04/29 23:33:12	10.0.1.10	port3	10.200.1.200	0		10.200.3.254	port1	10.08 kB / 10.08 kB
2020/04/29 23:31:27	10.0.1.10	port3	10.200.1.200	40,962		8.8.8.8 (dns.google)	port1	68 B / 148 B
2020/04/29 23:31:27	10.0.1.10	port3	10.200.1.200	48,553		8.8.8.8 (dns.google)	port1	68 B / 84 B
2020/04/29 23:31:27	10.0.1.10	port3	10.200.1.200	36,686		8.8.8.8 (dns.google)	port1	81 B / 263 B

FORTINET

© Fortinet Inc. All Rights Reserved.

36

You can view the **Sessions** page on the GUI, but the CLI provides more information regarding sessions in the session table.

Firewall performance of connections for each session, and the maximum number of connections, are indicated by the session table. However, if your FortiGate contains security processors designed to accelerate processing without loading the CPU, the session table information may not be completely accurate, because the session table reflects what is known to, and processed by, the CPU.

DO NOT REPRINT**© FORTINET**

Session TTL

- When the session table is full, reducing timers may improve performance by closing sessions earlier; however, be careful not to close sessions *too* soon, because this can cause connection errors

TCP default TTL

```
config system session-ttl  
set default 3600  
end
```

Specific state timers

```
config system global  
set tcp-halfclose-timer 120  
set tcp-halfopen-timer 10  
set tcp-timewait-timer 1  
set udp-idle-timer 180  
end
```

- Timers can be applied in policies and objects, and have precedence:
 - Firewall Services > Firewall Policies > Global Sessions**



Each session on FortiGate can idle for a finite time, which is defined by TTL. When the FortiGate detects the session is idle after some time of inactivity, and TTL is reached, the session is deleted from the session table.

Because the session table has a finite amount of RAM that it can use on FortiGate, adjusting the session TTL can improve performance. There are global default timers, session state timers, and timers configurable in firewall objects.

DO NOT REPRINT**© FORTINET**

Firewall Session Diagnostics

- `diagnose sys session`
 - The session table also indicates policy actions.
 - Clear any previous filter:
 - `diagnose sys session filter clear`
 - Set the filter:
 - `diagnose sys session filter ?`
 - `dport` Destination port
 - `dst` Destination IP address
 - `policy` Policy ID
 - `sport` Source port
 - `src` Source IP address
 - List all entries matching the configured filter:
 - `diagnose sys session list`
 - Purge all entries matching the configured filter:
 - `diagnose sys session clear`



© Fortinet Inc. All Rights Reserved.

38

The `diagnose sys session` command tree provides options to filter, clear, or show the list of sessions. You can also list brief information about sessions by running the `get system session list` command.

Before looking at the session table, first build a filter. To look at our test connection, you can filter on `dst 10.200.1.254` and `dport 80`.

DO NOT REPRINT**© FORTINET**

Session Table—TCP Example

```
# diagnose sys session filter dst 10.200.1.254
# diag sys session filter dport 80
# diag sys session list

session info: proto=6 proto_state=05 duration=2 expire=78 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=538/6/1 reply=5407/6/0 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 2/0

origin->sink: org pre->post, reply pre->post dev=5->3/3->5
gwy=10.200.1.254/10.0.1.10

hook=post dir=org act=snat 10.0.1.10:64624->10.200.1.254:80(10.200.1.1:64624)
hook=pre dir=reply act=dnat 10.200.1.254:80->10.200.1.1:64624(10.0.1.10:64624)
pos/(before,after) 0/(0,0), 0/(0,0)

misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
```

FORTINET

© Fortinet Inc. All Rights Reserved.

39

In the example shown on this slide, you can see the session TTL, which reflects how long FortiGate can go without receiving any packets for this session, until it will remove the session from its table.

Here you can see the routing and NAT actions that apply to the traffic. The firewall policy ID is also tracked.

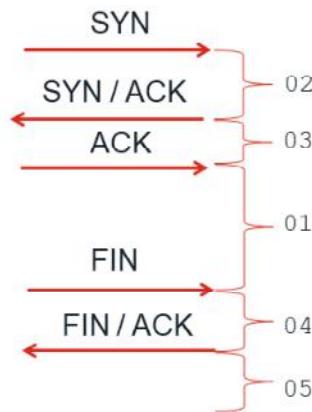
The `proto_state` for TCP is taken from its state machine, which you'll learn about in this lesson.

DO NOT REPRINT**© FORTINET**

TCP States

- proto_state=05
 - First digit (from left to right): server-side state
 - 0 if no inspection, 1 if proxy or flow
 - Second digit (from left to right): client-side state

TCP State	Value	Expire Timer in sec (default)
NONE	0	10
ESTABLISHED	1	3600
SYN_SENT	2	120
SYN & SYN/ACK	3	60
FIN_WAIT	4	120
TIME_WAIT	5	1
CLOSE	6	10
CLOSE_WAIT	7	120
LAST_ACK	8	30
LISTEN	9	120

**FORTINET**

© Fortinet Inc. All Rights Reserved.

40

Earlier in this lesson, you learned that the session table contains a number that indicates the connection's current TCP state. These are the states of the TCP state machine. They are single-digit values, but `proto_state` is always shown as two digits. This is because FortiGate is a stateful firewall and keeps track of the original direction (client-side state) and the reply direction (server-side state). If there are too many connections in the SYN state for long periods of time, this indicates a SYN flood, which you can mitigate with DoS policies.

This table and flow graph correlate the second digit value with the different TCP session states. For example, when the FortiGate receives the SYN packet, the second digit is 2. It goes to 3 once the SYN/ACK is received. After the three-way handshake, the state value changes to 1.

When a session is closed by both sides, FortiGate keeps it in the session table for a few seconds more, to allow any out-of-order packets that could arrive after the FIN/ACK packet. This is the state value 5.

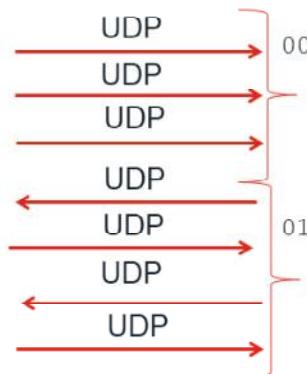
DO NOT REPRINT**© FORTINET**

ICMP and UDP Protocol States

- Even though UDP is stateless, FortiGate still uses two session state values:

UDP State	Value
UDP traffic one way only	0
UDP traffic both ways	1

- ICMP has no state
 - `proto_state` is always 00



© Fortinet Inc. All Rights Reserved.

41

Although (UDP) is a message-oriented, stateless protocol, it doesn't inherently require confirmed bidirectional connections like TCP, so there is no connection state. However, FortiGate's session table does use the `proto_state=` field to track the unidirectional UDP as state 0, and the bidirectional UDP as state 1.

When FortiGate receives the first packet, it creates the entry and sets the state to 0. If the destination replies, FortiGate updates the state flag to 1 for the remainder of the conversation.

Notably, (ICMP), such as ping and traceroute, have no protocol state and it will always show `proto_state=00`.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. If session diagnostic output indicates that a TCP protocol state is proto_state=01, which of the following statements is true?
 A. The session is established.
 B. The session is not established.



© Fortinet Inc. All Rights Reserved.

42

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand sessions.

Now, you'll learn about best practices and troubleshooting NAT.

DO NOT REPRINT**© FORTINET**

Best Practices and Troubleshooting

Objectives

- Identify common NAT issues by reviewing traffic logs
- Monitor NAT sessions using diagnose commands
- Use VIP filters for central NAT
- Use NAT implementation best practices

After completing this section, you should be able to achieve the objectives shown on this slide. By demonstrating competence in using traffic logs, diagnose commands, VIP filters, and best practices for NAT implementation, you should be able to monitor for and troubleshoot common NAT issues and successfully implement NAT in your network.

DO NOT REPRINT**© FORTINET**

NAT Port Exhaustion

- If traffic log is enabled, the following log is displayed when the NAT ports are exhausted:

```
Message meets Alert condition date=2011-02-01 time=19:52:01
devname=master device_id="" log_id=0100020007 type=event
subtype=system pri=critical vd=root service=kernel status=failure
msg="NAT port is exhausted."
```



© Fortinet Inc. All Rights Reserved.

45

NAT port exhaustion occurs when FortiGate is unable to allocate ports for performing NAT on new sessions because there are no available ports. When NAT port exhaustion occurs, FortiGate informs the administrator by displaying the log shown on this slide, with a severity of critical.

To address NAT port exhaustion, you must take one of the following actions:

- Create an IP pool that has more than one external IP tied to it (so it load balances across them)
- Reduce the number of sessions that require NAT

To receive important logs like this one, you must make sure that the necessary logging is enabled. On the FortiGate GUI, click **Log&Report > Log Settings**, to check that the default setting, logging to disk or memory, is activated.

DO NOT REPRINT**© FORTINET**

NAT Port Exhaustion

```
# diagnose sys session stat
misc info: session_count=16 setup_rate=0 exp_count=0 clash=889
memory_tension_drop=0 ephemeral=1/16384 removable=3
delete=0, flush=0, dev_down=16/69 ses_walkers=0
...
firewall error stat:
...
ids_recv=000fdc94
url_recv=00000000
av_recv=001fee47
fqdn_count=00000000
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

A number above 0 indicates that some sessions have been rejected because of NAT port exhaustion



© Fortinet Inc. All Rights Reserved.

46

NAT port exhaustion is also highlighted by a rise in the clash counter from the `diagnose system session stat` command.

DO NOT REPRINT**© FORTINET**

Monitoring NAT Sessions with Diagnose Commands

- diagnose firewall ippool-all list
 - Lists all the configured NAT IP pools with NAT IP range and type

```
Local-FortiGate # diagnose firewall ippool-all list  
vdom:root owns 1 ippool(s)  
name:INTERNAL-HOST-EXT-IP  
type:overload  
nat-ip-range:10.200.1.100-10.200.1.100  
.....  
.....
```

Command will list all configured IP Pools.



© Fortinet Inc. All Rights Reserved.

47

You can use the `diagnose firewall ippool-all list` command which will lists all of the configured NAT IP pools with their NAT IP range and type.

DO NOT REPRINT

© FORTINET

Monitoring NAT Sessions with Diagnose Commands (Cont'd)

- diagnose firewall ippool-all stats <Optional IP Pool name>

- Lists stats for all of the IP pools:

- NAT sessions per IP pool
- Total tcp sessions per IP pool
- Total udp sessions per IP pool
- Total others (non-tcp and non-udp) sessions per IP pool

```
# diagnose firewall ippool-all stats EXT
name: EXT
type: overload
startip: 10.200.1.100
endip: 10.200.1.100
total ses: 100
tcp ses: 75
udp ses: 20
other ses: 5
```

Command will only show stats of IP pool named as EXT

```
# diagnose firewall ippool-all stats
vdom:root owns 2 ippool(s)
name: EXT
type: overload
startip: 10.200.1.100
endip: 10.200.1.100
total ses: 100
tcp ses: 75
udp ses: 20
other ses: 5
```

Command will show stats of all IP pools.

```
name: Training
type: one-to-one
startip: 10.200.1.50
endip: 10.200.1.60
total ses: 10
tcp ses: 8
udp ses: 2
other ses: 0
```

FORTINET

© Fortinet Inc. All Rights Reserved.

48

The `diagnose firewall ippool-all stats` shows the stats for all of the IP pools.

The `stats` command provide the following data and information:

- NAT sessions per IP pool
- Total tcp sessions per IP pool
- Total udp sessions per IP pool
- Total others (non-TCP and non-UDP) sessions per IP pool

Optionally, you can filter the output for specific IP pool by using the name of IP pool.

DO NOT REPRINT**© FORTINET**

VIP Filters for Central NAT

- Enabling the **Services** option:
 - Allows complex scenarios where multiple external sources of traffic are using multiple services to connect to a single internal server
 - Avoids the requirement for numerous VIPs to be bundled into VIP groups

Policy & Objects > DNAT & Virtual IPs

Optional Filters	
Source address	145.20.3.5 149.32.10.10-149.32.10.20
Services	FTP HTTP HTTPS TFTP

```
config firewall vip
edit "VIP_1"
set uuid 31da2e74-8ab2-51ea-4f81-7bfeecd2fb28
set src-filter "145.20.3.5" "149.32.10.10-149.32.10.20"
set service "FTP" "HTTP" "HTTPS" "TFTP"
set extip 20.23.2.1
set extintf "external"
set mappedip "10.1.0.59"
next
```

FORTINET

© Fortinet Inc. All Rights Reserved.

49

The **Services** option has been added to VIP objects. When services and portforward are configured, only a single mapped port can be configured. However, multiple external ports can be mapped to that single internal port.

This configuration was made possible to allow for complex scenarios where multiple sources of traffic are using multiple services to connect to a single computer, while requiring a combination of source and destination NAT, and not requiring numerous VIPs to be bundled into VIP groups.

VIPs with different services are considered non-overlapping.

DO NOT REPRINT**© FORTINET**

NAT Implementation Best Practices

- Avoid the misconfiguration of an IP pool range:
 - Double-check the start and end IPs of each IP pool
 - Ensure that the IP pool does not overlap with addresses assigned to the FortiGate and hosts
 - If internal and external users are accessing the same servers, use split DNS, instead of external VIP
- Don't configure NAT rule for inbound traffic unless it is required by an application
- Schedule maintenance window to switch from one NAT mode to another



© Fortinet Inc. All Rights Reserved.

50

Use the following best practices when implementing NAT:

- Avoid the misconfiguration of an IP pool range:
 - Double-check the start and end IPs of each IP pool.
 - Ensure that the IP pool does not overlap with addresses assigned to FortiGate interfaces or to any hosts on directly connected networks.
 - If you have internal and external users accessing the same servers, use split DNS to offer an internal IP to internal users so that they don't have to use the external-facing VIP.
- Don't configure NAT rule for inbound traffic unless it is required by an application. If, for example, if there is a matching NAT rule for inbound SMTP traffic, the SMTP server might act as an open relay.
- You must schedule a maintenance window to switch from central NAT mode, to firewall policy NAT mode, or from firewall policy NAT mode to central NAT mode. Switching between NAT modes can create a network outage.

DO NOT REPRINT**© FORTINET**

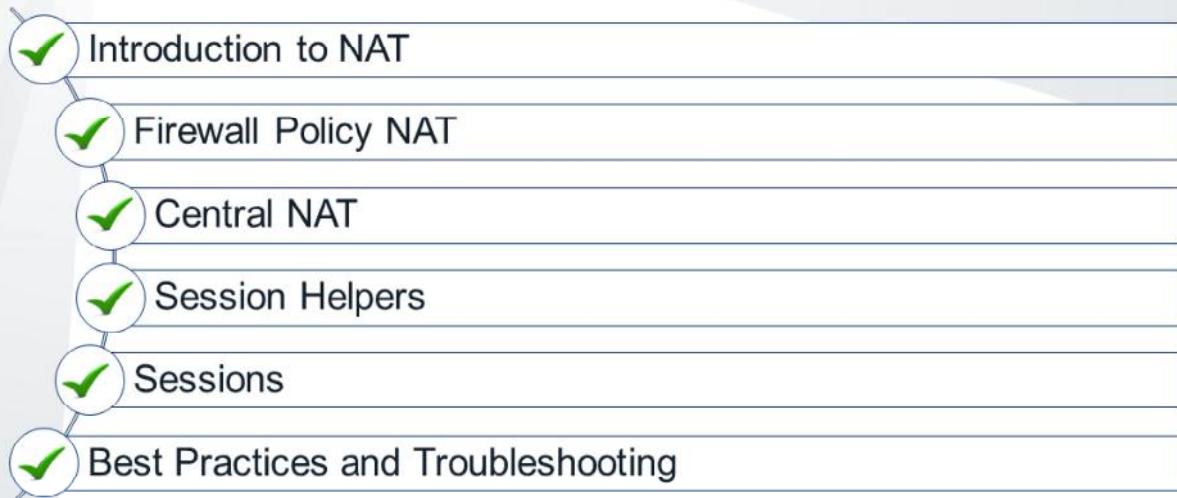
Knowledge Check

1. An administrator wants to check the total number of TCP sessions for an IP pool named INTERNAL. Which CLI command should the administrator use?
 A. diagnose firewall ippool-all stats INTERNAL
 B. diagnose firewall ippool-all list INTERNAL

2. Which statement about NAT port exhaustion is true?
 A. Reducing the NATed connections traversing the firewall will cause NAT port exhaustion.
 B. Increasing the number of NATed connections traversing the firewall can cause NAT port exhaustion.

DO NOT REPRINT**© FORTINET**

Lesson Progress



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Understand NAT and PAT
- ✓ Understand the different configuration modes for NAT
- ✓ Configure a firewall policy to perform SNAT and DNAT (VIPs)
- ✓ Configure central NAT
- ✓ Understand session helpers and use a SIP session helper for VoIP
- ✓ Understand and interpret the session table
- ✓ Analyse the session diagnose command output
- ✓ Understand TCP, UDP, and ICMP states
- ✓ Use traffic logs to identify common NAT issues and monitor NAT sessions using session diagnose commands
- ✓ Use NAT implementation best practices

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

By mastering the objectives covered in this slide, you learned how to understand and configure NAT so that you can use it in your network.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Firewall Authentication

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified: 1 June 2020

In this lesson, you will learn about using authentication on the firewall policies of a FortiGate.

DO NOT REPRINT**© FORTINET**

Lesson Overview

Methods of Firewall Authentication

Remote Authentication Servers

User Groups

Authentication Using Firewall Policies

Authenticating Through Captive Portal

Monitoring and Troubleshooting

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

DO NOT REPRINT

© FORTINET

Methods of Firewall Authentication

Objectives

- Describe firewall authentication
- Identify the different methods of firewall authentication available on FortiGate devices
- Identify supported remote authentication servers
- Describe active and passive authentication and order of operations

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

By demonstrating competence in methods of firewall authentication, you will be able to describe and identify the supported methods of firewall authentication available on FortiGate.

DO NOT REPRINT**© FORTINET**

Firewall Authentication

- Includes the authentication of users and user groups
 - It is more reliable than just IP address and device-type authentication
 - Users must authenticate by entering valid credentials
- After FortiGate identifies the user or device, FortiGate applies firewall policies and profiles to allow or deny access to each specific network resource

**FORTINET**

© Fortinet Inc. All Rights Reserved.

4

Traditional firewalls grant network access by verifying the source IP address and device. This is inadequate and can pose a security risk, because the firewall cannot determine who is using the device to which it is granting access.

FortiGate includes authentication of users and user groups. As a result, you can follow individuals across multiple devices.

Where access is controlled by a user or user group, users must authenticate by entering valid credentials (such as username and password). After FortiGate validates the user, FortiGate applies firewall policies and profiles to allow or deny access to specific network resources.

DO NOT REPRINT**© FORTINET**

FortiGate Methods of Firewall Authentication

- Local password authentication
 - Username and password stored on FortiGate
- Server-based password authentication (also called remote password authentication)
 - Password stored on a POP3, RADIUS, LDAP, or TACACS+ server
- Two-factor authentication
 - Enabled on top of an existing method
 - Requires something you know and something you have (token or certificate)



© Fortinet Inc. All Rights Reserved.

5

FortiGate supports multiple methods of firewall authentication:

- Local password authentication
- Server-based password authentication (also called remote password authentication)
- Two-factor authentication
This is a system of authentication that is enabled on top of an existing method—it cannot be enabled without first configuring one of the other methods. It requires something you know, such as a password, and something you have, such as a token or certificate.

During this lesson, you will learn about each method of firewall authentication in detail.

DO NOT REPRINT

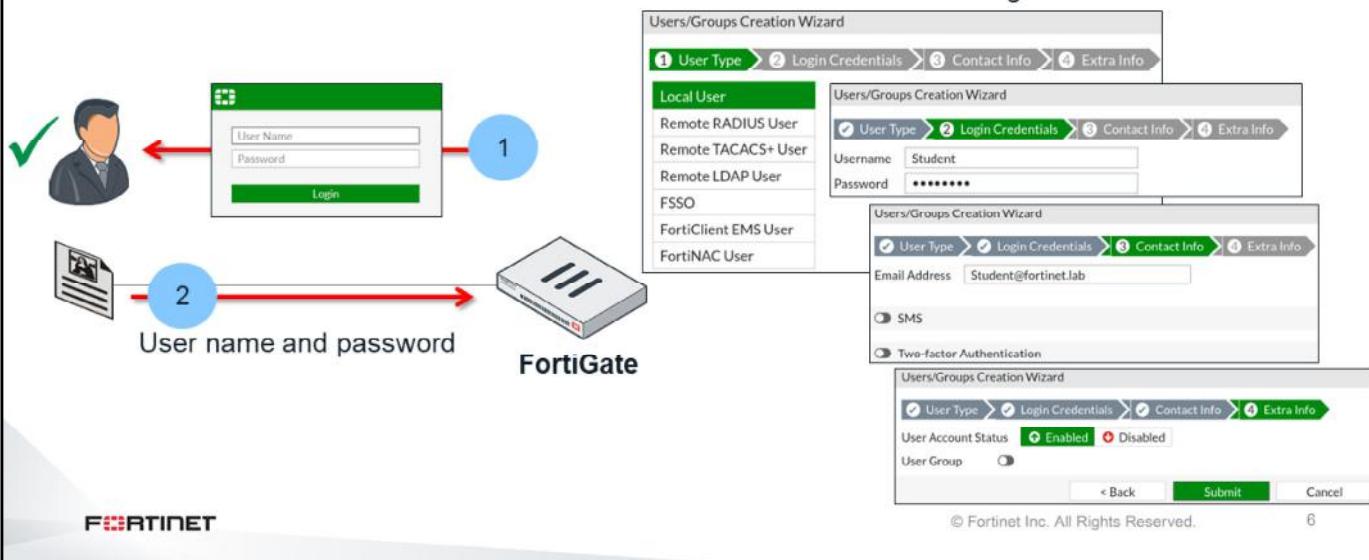
© FORTINET

Local Password Authentication

- User accounts created through

User & Authentication > User Definition

- User accounts stored locally on FortiGate
 - Works well for single FortiGate installations



The simplest method of authentication is local password authentication. User account information (username and password) is stored locally on the FortiGate device. This method works well for a single FortiGate installation.

Local accounts are created on the **User Definition** page where a wizard takes you through the process. For local password authentication, select **Local User** as the user type and create a username and password. If desired, you can also add email and SMS information to the account, enable two-factor authentication, and add the user to a preconfigured user group.

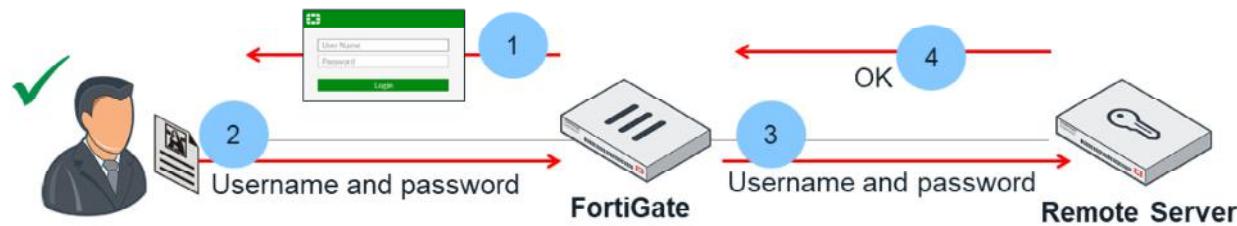
After you create the user, you can add the user—or any preconfigured user group in which the user is a member—to a firewall policy, in order to authenticate. You will learn about user groups and firewall policies in this lesson.

DO NOT REPRINT

© FORTINET

Server-Based Password Authentication

- Accounts are stored on a remote authentication server
- Administrators can do one of the following:
 - Create an account for the user locally, and specify the server to verify the password
 - Add the authentication server to a user group
 - All users in that server become members of the group



FORTINET

© Fortinet Inc. All Rights Reserved.

7

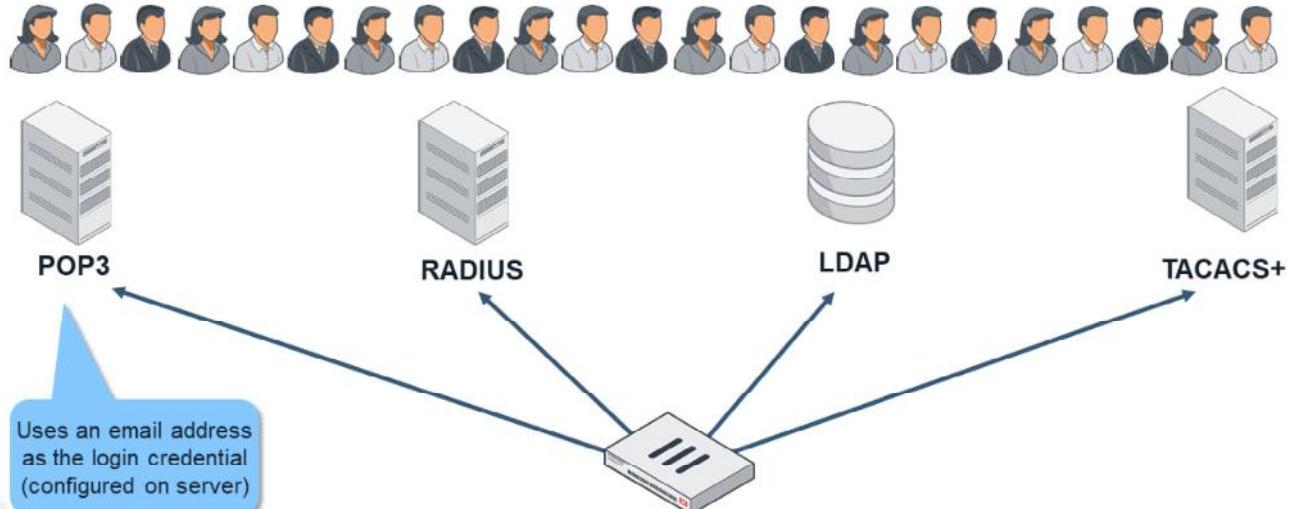
When server-based password authentication is used, a remote authentication server authenticates users. This method is desirable when multiple FortiGate devices need to authenticate the same users or user groups, or when adding a FortiGate to a network that already contains an authentication server.

When you use a remote authentication server to authenticate users, FortiGate sends the user's entered credentials to the remote authentication server. The remote authentication server responds by indicating whether the credentials are valid or not. If valid, FortiGate consults its configuration to deal with the traffic. Note that it is the remote authentication server—not FortiGate—that evaluates the user credentials.

When the server-based password authentication method is used, FortiGate does not store all (or, in the case of some configurations, any) of the user information locally.

DO NOT REPRINT**© FORTINET**

Remote Authentication Servers



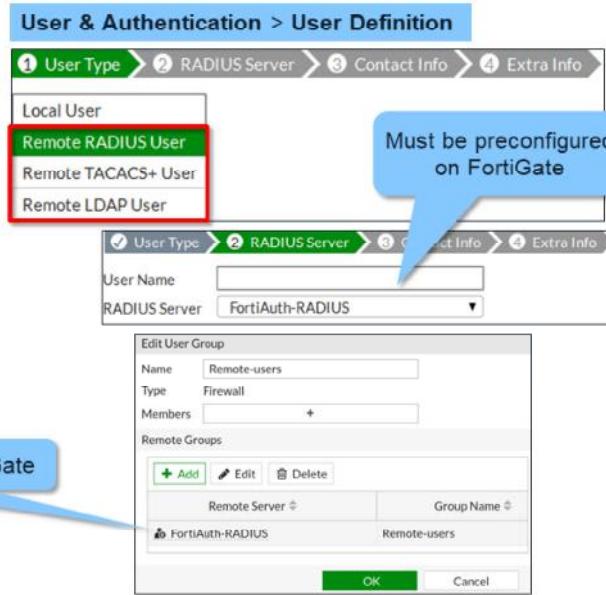
FortiGate provides support for many remote authentication servers, including POP3, RADIUS, LDAP, and TACACS+.

POP3 is the only server that requires an email address as the login credential. All other remote authentication servers use the user name. Some POP3 servers require the full email with domain (user@example.com), others require the suffix only, while still others accept both formats. This requirement is determined by the configuration of the server and is not a setting on FortiGate. You can configure POP3 authentication only through the CLI. Note that LDAP can be configured to validate with email, rather than the user name.

DO NOT REPRINT**© FORTINET**

Server-Based Password Authentication—Users

- Create user accounts on FortiGate
 - Select remote server type and point to preconfigured remote server
 - Add user to a group
- Add the remote authentication server to user groups



FORTINET

© Fortinet Inc. All Rights Reserved.

9

You can configure FortiGate to use external authentication servers in the following two ways:

- Create user accounts on FortiGate. With this method, you must select the remote authentication server type (RADIUS, TACACS+, or LDAP), point FortiGate to your preconfigured remote authentication server, and add the user to an appropriate group. This is usually done when you want to add two-factor authentication to your remote users. Remember, POP3 is only configurable through the CLI.
- Add the remote authentication server to user groups. With this method, you must create a user group and add the preconfigured remote server to the group. Accordingly, any user who has an account on the remote authentication server can authenticate. If you are using other types of remote server, such as an LDAP server, as the remote authentication server, you can control access to specific LDAP groups, as defined on the LDAP server.

Similar to local password authentication, you must then add the preconfigured user group (in which the user is a member) to a firewall policy in order to authenticate. We will discuss user groups and firewall policies later in this lesson.

DO NOT REPRINT**© FORTINET**

Two-Factor Authentication and One-Time Passwords

- Strong authentication that improves security by preventing attacks associated with the use of static passwords alone
- Requires two independent methods of identifying a user:
 - Something you know, such as password or PIN
 - Something you have, such as a token or certificate
- One-time passwords (OTPs) can be used one time only
 - OTPs are more secure than static passwords
- Available on both user and administrator accounts
 - The user or user group is added to a firewall policy in order to authenticate
- Methods of OTP delivery include:
 - FortiToken 200 or FortiToken Mobile
 - Generates a six-digit code every 60 seconds based on a unique seed and GMT time
 - Email or SMS
 - An OTP is sent to the user's email or SMS
 - Email or SMS must be configured on the user's account
 - FortiToken mobile push
 - Supports two-factor authentication without requiring user to enter code
- NTP server recommended!



© Fortinet Inc. All Rights Reserved.

10

Traditional user authentication requires your user name plus something you know, such as a password. The weakness with this traditional method of authentication is that if someone obtains your user name, they only need your password to compromise your account. Furthermore, since people tend to use the same password across multiple accounts (some sites with more security vulnerabilities than others), accounts are vulnerable to attack, regardless of password strength.

Two-factor authentication, on the other hand, requires something you know, such as a password, and something you have, such as a token or certificate. Because this method places less importance on, often vulnerable passwords, it makes compromising the account more complex for an attacker. You can use two-factor authentication on FortiGate with both user and administrator accounts. The user (or user group to which the user belongs) is added to a firewall policy in order to authenticate. Note that you cannot use two-factor authentication with explicit proxies.

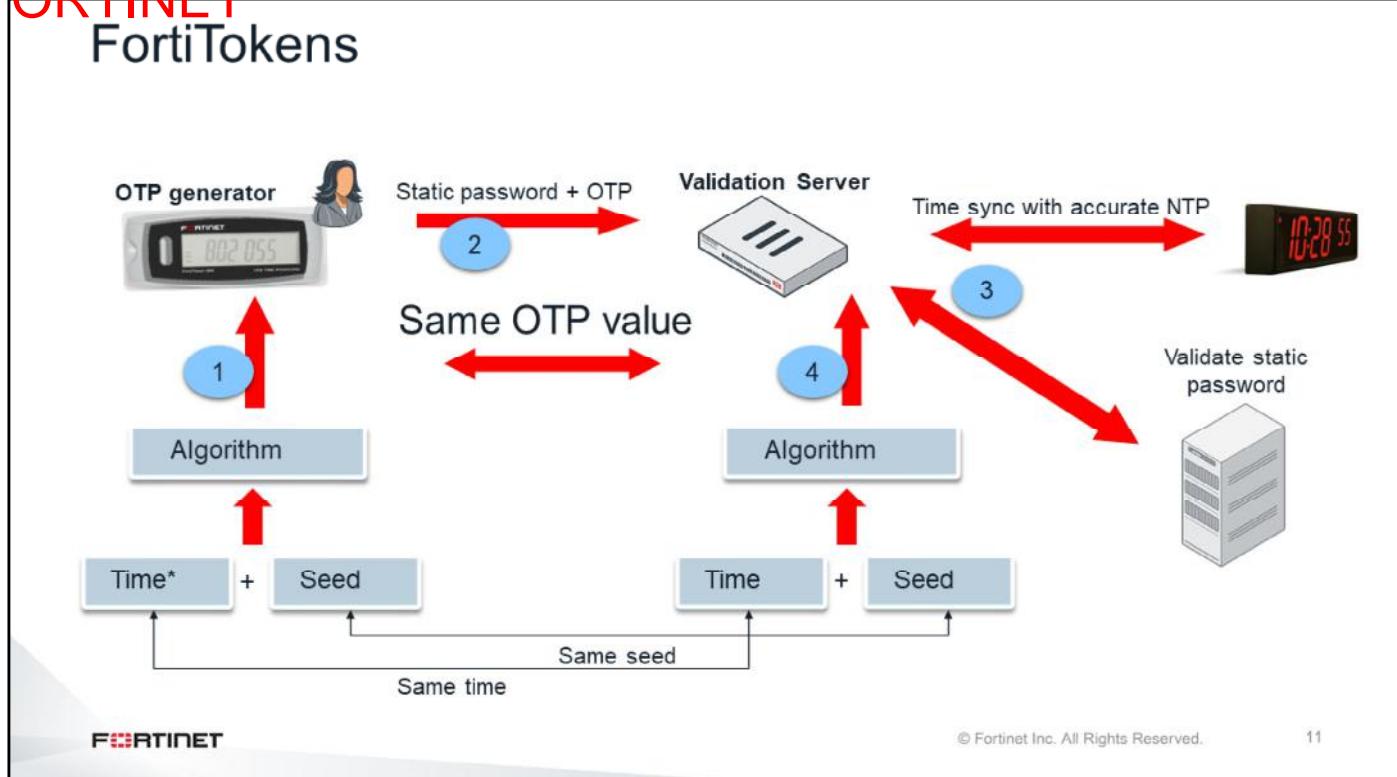
You can use one-time passwords (OTPs) as your second factor. OTPs are more secure than static passwords because the passcode changes at regular intervals and is only valid for a short amount of time. Once you use the OTP, it cannot be used again. So, even if it is intercepted, it is useless. FortiGate can deliver OTPs through tokens, such as FortiToken 200 (hardware token) and FortiToken Mobile (software token), as well as through email or SMS. To deliver an OTP over email or SMS, the user account must contain user contact information.

FortiTokens and OTPs delivered through email and SMS are time based. FortiTokens, for example, generate a new six-digit password every 60 seconds (by default). An NTP server is highly recommended to ensure the OTPs remain in sync. FortiToken Mobile Push allows users to simply accept the authorization request from their FortiToken mobile app, without the need to enter an additional code.

DO NOT REPRINT

© FORTINET

FortiTokens



Tokens use a specific algorithm to generate an OTP. The algorithm consists of:

- A seed: a unique, randomly-generated number that does not change over time
- The time: obtained from an accurate internal clock

Both seed and time go through an algorithm that generates an OTP (or passcode) on the token. The passcode has a short life span, usually measured in seconds (60 seconds for a FortiToken 200, possibly more or less for other RSA key generators). Once the life span ends, a new passcode generates.

When using two-factor authentication using a token, the user must first log in with a static password followed by the passcode generated by the token. A validation server (FortiGate) receives the user's credentials and validates the static password first. The validation server then proceeds to validate the passcode. It does so by regenerating the same passcode using the seed and system time (which is synchronized with the one on the token) and comparing it with the one received from the user. If the static password is valid, and the OTP matches, the user is successfully authenticated. Again, both the token and the validation server must use the same seed and have synchronized system clocks. As such, it is crucial that you configure the date and time correctly on your FortiGate, or link it to an NTP server (recommended).

DO NOT REPRINT

© FORTINET

Assigning a FortiToken to a User

The screenshot shows the FortiGate User & Authentication interface. On the left, a table lists existing FortiTokens: one Mobile Token (FTKMOB781E57E34F) and another Mobile Token (FTKMOB783867923E), both marked as Available. A blue callout points to this table with the text "Two free FortiToken Mobile activations".

In the center, two "New FortiToken" creation forms are shown side-by-side. The left form has "Type" set to "Hard Token" and the right form has "Type" set to "Mobile Token". Both forms include fields for "Comments" (with placeholder "Write a comment..."), "Serial Number" (with placeholder "0000-0000-0000-0000-0000"), and "Activation Code" (with placeholder "0000-0000-0000-0000-0000"). A blue callout points to these forms with the text "Enable Two-factor Authentication and select the registered FortiToken".

On the right, a detailed view of a user account for "student" is shown. The account is "Enabled". It includes fields for "User Type" (Local User), "Password" (redacted), "Email Address" (redacted), "User Group" (selected "External-Server-users"), and "SMS" (radio button). A blue callout points to this account with the text "Can add a user to a group and create a firewall policy based on the user group".

At the bottom right of the interface, there is a note: "© Fortinet Inc. All Rights Reserved. 12".

You can add a FortiToken 200 or FortiToken Mobile to FortiGate on the **FortiTokens** page.

For the hard token, a serial number is used to provide FortiGate with details on the initial seed value. If you have several hard tokens to add, you can import a text file, where one serial number is listed per line.

For the soft token, an activation code is required. Note that each FortiGate (and FortiGate VM) provides two free FortiToken Mobile activations. Any additional tokens must be purchased from Fortinet.

You cannot register the same FortiToken on more than one FortiGate. If you want to use the same FortiToken for authentication on multiple FortiGate devices, you must use a central validation server, such as FortiAuthenticator. In that case, FortiTokens are registered and assigned to users on FortiAuthenticator, and FortiGate uses FortiAuthenticator as its validation server.

Once you have registered the FortiTokens with FortiGate, you can assign them to users to use as their second-factor authentication method. To assign a token, edit (or create) the user account and select **Enable Two-factor Authentication**. From the **Token** drop-down list, select the registered token you want to assign.

DO NOT REPRINT**© FORTINET**

Authentication Methods and Active Authentication

- Active
 - User receives a login prompt
 - Must manually enter credentials to authenticate
 - POP3, LDAP, RADIUS, Local, and TACACS+
- Passive
 - User does not receive a login prompt from FortiGate
 - Credentials are determined automatically
 - Method varies depending on type of authentication used
 - FSSO, RSSO, and NTLM



© Fortinet Inc. All Rights Reserved.

13

All the authentication methods you've learned about—local password authentication, server-based authentication, and two-factor authentication—use active authentication. Active authentication means that users are prompted to manually enter their login credentials before being granted access.

But not all users authenticate the same way. Some users can be granted access transparently, because user information is determined without asking the user to enter their login credentials. This is known as passive authentication. Passive authentication occurs with the single sign-on method for server-based password authentication: FSSO, RSSO, and NTLM.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which firewall authentication method does FortiGate support?
 A. Local password authentication
 B. Biometric authentication

2. Which type of token can generate OTPs to provide two-factor authentication to users in your network?
 A. FortiToken Mobile
 B. USB FortiToken



© Fortinet Inc. All Rights Reserved.

14

DO NOT REPRINT**© FORTINET**

Lesson Progress



Methods of Firewall Authentication



Remote Authentication Servers



User Groups



Authentication Using Firewall Policies



Authenticating Through Captive Portal



Monitoring and Troubleshooting

Good job! You now understand the basics of firewall authentication.

Now, you will learn about remote authentication servers.

DO NOT REPRINT

© FORTINET

Remote Authentication Servers

Objectives

- Configure remote authentication servers
- Configure user authentication
- Understand the roles of LDAP and RADIUS

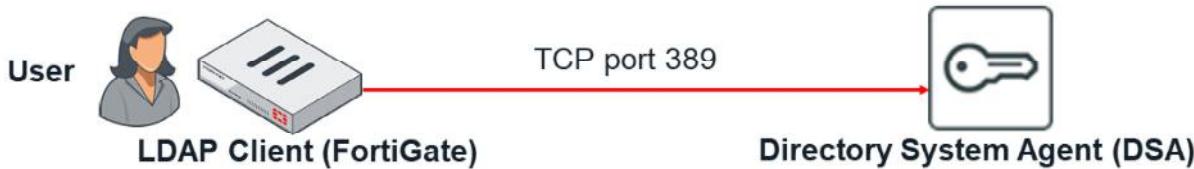
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in remote authentication servers, you will be able to configure firewall authentication using remote user accounts defined on a remote authentication server.

DO NOT REPRINT**© FORTINET**

LDAP Overview

- LDAP is an application protocol for accessing and maintaining distributed directory information services



- LDAP maintains authentication data, including:
 - Departments, people (and groups of people), passwords, email addresses, and printers
- LDAP consists of a data-representation scheme, a set of defined operations, and a request and response network
- Binding is the operation in which the LDAP server authenticates the user

FORTINET

© Fortinet Inc. All Rights Reserved.

17

Lightweight Directory Access Protocol (LDAP) is an application protocol used for accessing and maintaining distributed directory information services.

The LDAP protocol is used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request and response network.

The LDAP protocol includes a number of operations that a client can request, such as search, compare, and add or delete an entry. Binding is the operation in which the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server, based on that user's permissions.

DO NOT REPRINT**© FORTINET**

LDAP Directory Tree

- The LDAP structure is similar to a tree that contains entries (objects) in each branch
- Each entry has a unique ID: the distinguished name (DN)
- Each DN has attributes
- Each attribute has a name and one or more values
- The attributes are defined in the directory schema



© Fortinet Inc. All Rights Reserved.

18

The root of the LDAP directory tree represents the organization itself, and is defined as a domain component (DC). The DC is usually a DNS domain, such as example.com. (Because the name contains a dot, it is written as two parts separated by a comma: dc=example,dc=com.) Additional entries, known as objects, can be added to the hierarchy as needed. Generally, two types of objects make up most entries: containers and leafs.

Containers are objects that can include other objects, similar to a folder in a file system. Example containers include:

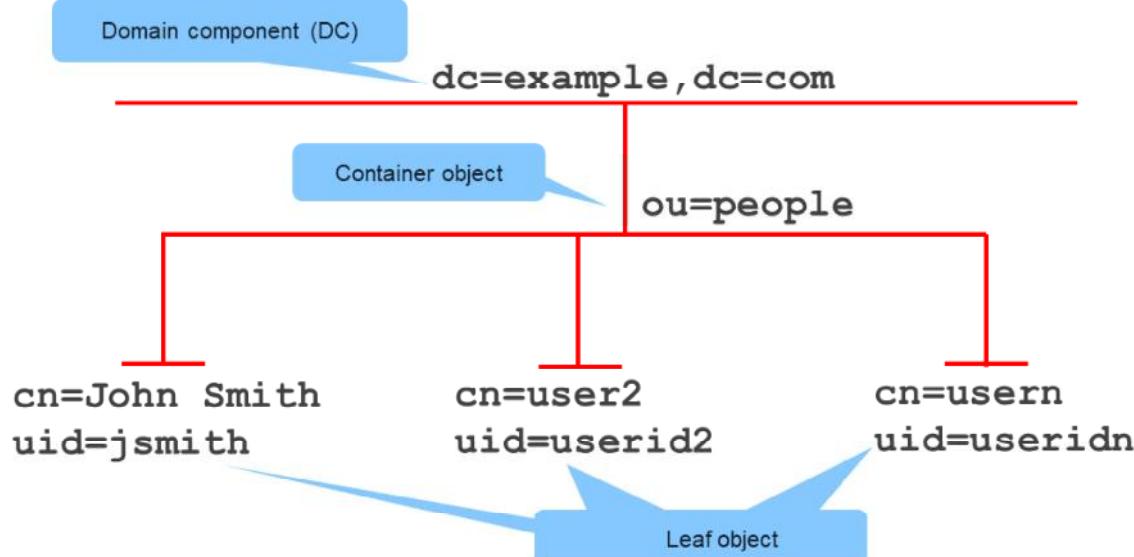
- Country (represented as c)
- Organizational unit (represented as ou)
- Organization (represented as o)

Leafs are objects at the end of a branch and have no subordinate objects. Example leafs include:

- User ID (represented as uid)
- Common name (represented as cn)

DO NOT REPRINT**© FORTINET**

Example Directory Tree

**FORTINET**

© Fortinet Inc. All Rights Reserved.

19

This slide shows an example of a simple LDAP hierarchy.

The FortiGate device (acting as an LDAP client) requesting authentication must be configured to address its request to the part of the hierarchy where user records exist: either the domain component or a specific container where the record exists. Similar to users, containers have DNs, and in this example, the DN is ou=people,dc=example,dc=com.

The authentication request must also specify the user account entry. This can be one of many options including the common name (cn) or, on a computer network, the user ID (uid), which is the information users use to log in. Note that if the object name includes a space, such as John Smith, you must enclose the text with double quotes when testing in the CLI. For example: cn="John Smith".

DO NOT REPRINT

© FORTINET

Configuring an LDAP Server on FortiGate

Directory tree attribute that identifies users

Part of the hierarchy where user records exist

Credentials for an LDAP administrator

User & Authentication > LDAP Servers

Edit LDAP Server

Name	External_Server
Server IP/Name	10.0.1.150
Server Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training
Bind Type	Regular
Username	uid=admin,dc=Users,dc=trainingAD,dc=training
Password	*****
Secure Connection	<input type="checkbox"/>
Connection status	Successful
Test Connectivity	
Test User Credentials	

© Fortinet Inc. All Rights Reserved. 20

On the LDAP Servers page, you can configure FortiGate to point to an LDAP server for server-based password authentication. The configuration depends heavily on the server's schema and security settings. Windows Active Directory (AD) is very common.

The **Common Name Identifier** setting is the attribute name used to find the user name. Some schemas allow you to use the attribute uid. AD most commonly uses sAMAccountName or cn, but can use others as well.

The **Distinguished Name** setting identifies the top of the tree where the users are located, which is generally the dc value; however, it can be a specific container or ou. You must use the correct X.500 or LDAP format.

The **Bind Type** setting depends on the security settings of the LDAP server. The setting **Regular** (to specify a regular bind) is required if you are searching across multiple domains and require the credentials of a user that is authorized to perform LDAP queries (for example, an LDAP administrator).

If you want to have a secure connection between FortiGate and the remote LDAP server, enable **Secure Connection** and include the LDAP server protocol (LDAPS or STARTTLS) as well as the CA certificate that verifies the server certificate.

Note that the **Test Connectivity** button only tests whether the connection to the LDAP server is successful or not. To test whether a user's credentials can successfully authenticate, you must use the CLI.

DO NOT REPRINT**© FORTINET**

Testing the LDAP Query

- diagnose test authserver ldap <server_name> <username> <password>
- Example:

```
# diagnose test authserver ldap External_Server aduser1 Training!
authenticate 'aduser1' against 'ADserver' succeeded!
Group membership(s) - CN=AD-users,OU=Training,DC=trainingAD,DC=training,DC=lab
```



© Fortinet Inc. All Rights Reserved.

21

Use the `diagnose test authserver` command in the CLI to test whether a user's credentials can successfully authenticate. You want to ensure that authentication is successful, prior to implementing it on any of your firewall policies.

The response from the server reports success, failure, and group membership details.

DO NOT REPRINT**© FORTINET**

RADIUS Overview

- RADIUS is a standard protocol that provides AAA services

**FORTINET**

© Fortinet Inc. All Rights Reserved.

22

RADIUS is much different than LDAP, because there is no directory tree structure to consider. RADIUS is a standard protocol that provides authentication, authorization, and accounting (AAA) services.

When a user is authenticating, the client (FortiGate) sends an ACCESS-REQUEST packet to the RADIUS server. The reply from the server will be one of the following:

- ACCESS-ACCEPT, which means that the user credentials are ok
- ACCESS-REJECT, which means that the credentials are wrong
- ACCESS-CHALLENGE, which means that the server is requesting a secondary password ID, token, or certificate. This is typically the reply from the server when using two-factor authentication.

Not all RADIUS clients support the RADIUS challenge method.

DO NOT REPRINT

© FORTINET

Configuring a RADIUS Server on FortiGate

User & Authentication > RADIUS Servers

New RADIUS Server

Name	FortiAuth-RADIUS
Authentication method	Default Specify
NAS IP	
Include in every user group	<input type="checkbox"/>
Primary Server	
IP/Name	10.0.1.150
Secret	*****
Test Connectivity Test User Credentials	

© Fortinet Inc. All Rights Reserved. 23

You can configure FortiGate to point to a RADIUS server for server-based password authentication through the **RADIUS Servers** page.

The **Primary Server IP/Name** setting is the IP address or FQDN of the RADIUS server.

The **Primary Server Secret** setting is the secret that was set up on the RADIUS server in order to allow remote queries from this client. Backup servers (with separate secrets) can be defined in case the primary server fails. Note that FortiGate must be listed on the RADIUS server as a client of that RADIUS server or else the server will not reply to queries done by FortiGate.

The **Authentication Method** setting refers to the authentication protocol that the RADIUS server supports. Options include chap, pap, mschap, and mschap2. If you select **Default** the FortiGate will use pap, mschap2, and chap (in that order).

Unlike LDAP configurations, the **Test Connectivity** button used here can test actual user credentials, but, like LDAP, you can also test this using the CLI.

The **Include in every User Group** option adds the RADIUS server and all users that can authenticate against it, to every user group created on the FortiGate. So, this option should only be enabled in very specific scenarios (for example, when only administrators can authenticate against the RADIUS server and policies are ordered from least restrictive to most restrictive).

DO NOT REPRINT**© FORTINET**

Testing RADIUS Queries

- diagnose test authserver radius <server_name> <scheme> <user> <password>
- Example:

```
# diagnose test authserver radius FortiAuth-RADIUS pap student fortinet
authenticate 'aduser1' against 'pap' succeeded, server=primary
assigned_rad_session_id=610153440 session_timeout=0 secs!
Group membership(s) - remote-AD-admins
```

Group memberships are provided by vendor specific attributes configured on the RADIUS server



© Fortinet Inc. All Rights Reserved.

24

Testing RADIUS is much the same as testing LDAP. Use the `diagnose test authserver` command on the CLI to test whether a user's credentials can successfully authenticate. Again, you should do this to ensure authentication is successful before implementing it on any of your firewall policies.

Like LDAP, it reports success, failure, and group membership details, depending on the server's response. Deeper troubleshooting usually requires RADIUS server access.

Note that Fortinet has a vendor-specific attributes (VSA) dictionary to identify the Fortinet-proprietary RADIUS attributes. This capability allows you to extend the basic functionality of RADIUS. You can obtain the Fortinet VSA dictionary from the Fortinet Knowledge Base (kb.fortinet.com).

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. When FortiGate uses a RADIUS server for remote authentication, which statement about RADIUS is true?
 - A. FortiGate must query the remote RADIUS server using the distinguished name (dn).
 - B. RADIUS group memberships are provided by vendor specific attributes (VSAs) configured on the RADIUS server.

2. Which one of the following is a valid reply from a RADIUS server to an ACCESS-REQUEST packet from FortiGate?
 - A. ACCESS-PENDING
 - B. ACCESS-REJECT

3. A remote LDAP user is trying to authenticate with a username and password. How does FortiGate verify the login credentials?
 - A. FortiGate queries its own database for user credentials.
 - B. FortiGate sends the user-entered credentials to the remote server for verification.



© Fortinet Inc. All Rights Reserved.

25

DO NOT REPRINT**© FORTINET**

Lesson Progress



Methods of Firewall Authentication



Remote Authentication Servers

User Groups

Authentication Using Firewall Policies



Authenticating Through Captive Portal



Monitoring and Troubleshooting

Good job! You now understand the basics of remote authentication servers.

Now, you will learn about user groups.

DO NOT REPRINT

© FORTINET

User Groups

Objectives

- Configure user groups

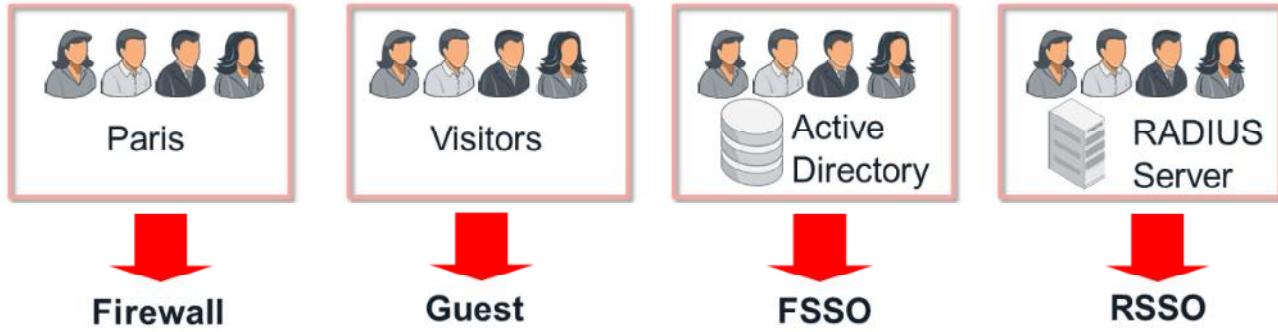
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in user groups, you will be able to configure user groups to efficiently manage firewall policies.

DO NOT REPRINT

© FORTINET

Types of User Groups



- User groups types: Firewall, Fortinet single sign-on (FSSO), Guest, and RADIUS single sign-on (RSSO).
- Firewall user groups provide access to firewall policies that require authentication.
- FSSO and RSSO are used for single sign-on authentication.



© Fortinet Inc. All Rights Reserved.

28

FortiGate allows administrators to assign users to groups. Generally, groups are used to more effectively manage individuals that have some kind of shared relationship. You might want to group employees by business area, such as finance or HR, or by employee type, such as contractors or guests.

After you create user groups, you can add them to firewall policies. This allows you to control access to network resources, because policy decisions are made on the group as a whole. You can define both local and remote user groups on a FortiGate device. There are four user group types:

- Firewall
- Guest
- Fortinet single sign-on (FSSO)
- RADIUS single sign-on (RSSO)

The firewall user groups on FortiGate do not need to match any type of group that may already exist on an external server such as an LDAP server. The firewall user groups exist solely to make configuration of firewall policies easier.

Most authentication types have the option to make decisions based on the individual user, rather than just user groups.

DO NOT REPRINT**© FORTINET**

Guest User Groups

- Most commonly used for guest access in wireless networks
- Guest groups contain temporary accounts

User & Authentication > User Groups

Name	Guests
Type	<input type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> RADIUS Single Sign-On (RSSO) <input checked="" type="radio"/> Guest
Batch Guest Account Creation	
User ID	<input checked="" type="radio"/> Email <input type="radio"/> Auto Generated <input type="radio"/> Specify
Maximum Accounts	<input type="checkbox"/>
Guest Details	
Enable Name	<input type="checkbox"/>
Enable Email	<input checked="" type="checkbox"/>
Enable SMS	<input type="checkbox"/>
Password	<input checked="" type="radio"/> Auto Generated <input type="radio"/> Specify
Sponsor	<input type="radio"/> Optional <input checked="" type="radio"/> Required
Company	<input type="radio"/> Optional <input checked="" type="radio"/> Required
Expiration	
Start Countdown	<input checked="" type="radio"/> On Account Creation <input type="radio"/> After First Login
Time	Days: 0 Hours: 4 Minutes: 0 Seconds: 0

Account expiry

FORTINET

© Fortinet Inc. All Rights Reserved.

29

Guest user groups are different from firewall user groups because they contain exclusively temporary guest user accounts (the whole account, not just the password). Guest user groups are most commonly used in wireless networks. Guest accounts expire after a predetermined amount of time.

Administrators can manually create guest accounts or create many guest accounts at once using randomly-generated user IDs and passwords. This reduces administrator workload for large events. Once created, you can add accounts to the guest user group and associate the group with a firewall policy.

You can create guest management administrators that have access only to create and manage guest user accounts.

DO NOT REPRINT

© FORTINET

Configuring User Groups

The screenshot shows the 'User & Authentication > User Groups' page. A group named 'Training-users' is selected, with its type set to 'Firewall'. The 'Members' section is highlighted in yellow. A callout bubble points to this area with the text 'Can add preconfigured remote servers to the group'. Another callout bubble points to the 'Select Entries' dialog box, which lists 'USER (2)' entries: 'Local (2)', 'guest', and 'student'. This dialog is associated with the text 'Add members to group (local or PKI peer)'. Below this, the 'Remote Groups' section is shown, featuring a table with columns for 'Remote Server' and 'Group Name'. An entry for 'External_Server' with the value 'cn=AD_users,ou=Training,dc=trainingAD,dc=training,dc=lab' is listed. A callout bubble points to this table with the text 'Can select specific LDAP groups as defined on the LDAP server'.

User & Authentication > User Groups

Name	Training-users
Type	Firewall
	Fortinet Single Sign-On (FSSO)
	RADIUS Single Sign-On (RSSO)
	Guest
Members	+ [yellow]

Add members to group (local or PKI peer)

Select Entries

Search	+ Create
USER (2)	
Local (2)	
guest	edit
student	edit

Can add preconfigured remote servers to the group

Remote Groups

Remote Server	Group Name
External_Server	cn=AD_users,ou=Training,dc=trainingAD,dc=training,dc=lab

Can select specific LDAP groups as defined on the LDAP server

FORTINET

© Fortinet Inc. All Rights Reserved.

30

You can configure user groups on the **User Groups** page. You must specify the user group type and add users to the group. Depending on the group you create, different configurations are required. For the firewall user group, for example, members can consist of local users, PKI peer users, and users from one or more remote authentication servers. If your remote authentication server is an LDAP server, you can select specific LDAP groups to add to your user group, as defined on the LDAP server. Note that you can also select RADIUS groups, but this requires additional configuration on your RADIUS server and FortiGate (see the Fortinet Knowledge Base at kb.fortinet.com).

User groups simplify your configuration if you want to treat specific users in the same way, for example, if you want to provide the entire training department with access to the same network resources. If you want to treat all users differently, you need to add all users to firewall policies separately.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which statement about guest user groups is true?
 A. Guest user group accounts are temporary.
 B. Guest user group account passwords are temporary.

2. Guest accounts are most commonly used for which of the following purposes?
 A. To provide temporary visitor access to corporate network resources
 B. To provide temporary visitor access to wireless networks

DO NOT REPRINT**© FORTINET**

Lesson Progress



Methods of Firewall Authentication



Remote Authentication Servers



User Groups



Authentication Using Firewall Policies



Authenticating Through Captive Portal



Monitoring and Troubleshooting

Good job! You now understand the basics of user groups.

Now, you will learn about using firewall policies for authentication.

DO NOT REPRINT

© FORTINET

Authentication Using Firewall Policies

Objectives

- Configure firewall policies

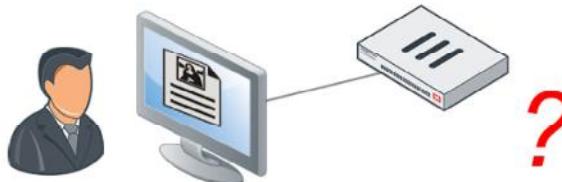
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence with firewall policies, you will be able to configure firewall policies to enforce authentication on specific users and user groups.

DO NOT REPRINT**© FORTINET**

Firewall Policy—Source

- Firewall policies can use user and user group objects to define the source. The objects include:
 - Local firewall accounts
 - External (remote) server accounts
 - PKI (certificate) users
 - FSSO users
- Anyone who belongs to the group and provides correct information, will have a successful authentication



FORTINET

© Fortinet Inc. All Rights Reserved.

34

A firewall policy consists of access and inspection rules (compartmentalized sets of instructions) that tell FortiGate how to handle traffic on the interface whose traffic they filter. After the user makes an initial connection attempt, FortiGate checks the firewall policies to determine whether to accept or deny the communication session. However, a firewall policy also includes a number of other instructions, such as those dealing with authentication. You can use the source of a firewall policy for this purpose. The source of a firewall policy must include the source address (IP address), but you can also include the user, and user group. In this way, any user, or user group that is included in the source definition for the firewall policy can successfully authenticate.

User and user group objects can consist of local firewall accounts, external server accounts, PKI users, and FSSO users.

DO NOT REPRINT**© FORTINET**

Firewall Policy—Service

- DNS traffic can be allowed if user has not authenticated yet
 - Hostname resolution is often required by the application layer protocol (HTTP/HTTPS/FTP/Telnet) that is used to authenticate
 - DNS service must be explicitly listed as a service in the policy

Policies & Objects > Firewall Policy

Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1	Full_Access External-Server-Users LOCAL_SUBNET	all	always	DNS HTTP	ACCEPT	Enabled

FORTINET

© Fortinet Inc. All Rights Reserved.

35

A firewall policy also checks the service in order to transport the named protocols or group of protocols. No service (with the exception of DNS) is allowed through the firewall policy prior to successful user authentication. DNS is usually used by HTTP so that people can use domain names for websites, instead of their IP address. DNS is allowed because it is a base protocol and will most likely be required to initially see proper authentication protocol traffic. Hostname resolution is almost always a requirement for any protocol. However, the DNS service must still be defined in the policy as allowed, in order for it to pass.

In the example shown on this slide, policy sequence 1 (Full_Access) allows users to use external DNS servers in order to resolve host names, prior to successful authentication. DNS is also allowed if authentication is unsuccessful, because users need to be able to try to authenticate again. Any service that includes DNS would function the same way, like the default ALL service.

HTTP service is TCP port 80 and does not include DNS (UDP port 53).

DO NOT REPRINT**© FORTINET**

Protocols

- A firewall policy must allow a protocol in order to show the authentication dialog that is used in active authentication:
 - HTTP
 - HTTPS
 - FTP
 - Telnet
- All other services are not allowed until the user has authenticated successfully through one of the protocols above listed above



© Fortinet Inc. All Rights Reserved.

36

As well as the DNS service, the firewall policy must specify the allowed protocols, such as HTTP, HTTPS, FTP, and Telnet. If the firewall policy that has authentication enabled does not allow at least one of the supported protocols used for obtaining user credentials, the user will not be able to authenticate.

Protocols are required for all authentication methods that use active authentication (local password authentication, server-based password authentication, and two-factor authentication). Active authentication prompts the user for user credentials based on the following:

- The protocol of the traffic
- The firewall policy

Passive authentication, on the other hand, determines the user identity behind the scenes, and does not require any specific services to be allowed within the policy.

DO NOT REPRINT

© FORTINET Mixing Policies

- Enabling authentication on a policy does not always force an active authentication prompt

ID	Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 ②							
1	Full_Access	LOCAL_SUBNET HR-group	all	always	ALL	✓ ACCEPT	✓ Enabled
2		LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled

- Three options:
 - Enable authentication on every policy that could match the traffic.
 - Enforce authentication on demand option (CLI option only)
 - Enable a captive portal on the ingress interface for the traffic
- If login cannot be determined passively, then FortiGate uses active authentication
 - FortiGate will not prompt the user for login credentials when the user can be determined passively
 - By default, active authentication is intended to be used as a backup when passive authentication fails

FORTINET

© Fortinet Inc. All Rights Reserved.

37

In the example shown on this slide, assuming active authentication is used, any initial traffic from LOCAL_SUBNET will not match policy sequence 1 (Full_Access). Policy sequence 1 looks for both IP and user, and user group information (LOCAL_SUBNET and HR-group respectively), and since the user has not yet authenticated, the user group aspect of the traffic does not match. Since the policy match is not complete, FortiGate continues its search down the sequence list, to see if there is a complete match.

Next, FortiGate evaluates policy sequence 2 to see if the traffic matches. It matches all criteria, so traffic is allowed with no need to authenticate.

When only active authentication is used, if all possible policies that could match the source IP have authentication enabled, then the user will receive a login prompt (assuming they use an acceptable login protocol). In other words, if policy sequence 2 also had authentication enabled, the users would receive login prompts.

If passive authentication is used and it can successfully obtain user details, then traffic from LOCAL_SUBNET with users that belong to HR-group will apply to policy sequence 1, even though policy sequence 2 does not have authentication enabled.

If you are using both active and passive authentication, and a user's credentials can be determined through passive authentication, the user will never receive a login prompt, regardless of the order of any firewall policies. This is because there is no need for FortiGate to prompt the user for login credentials when it can determine who the user is passively. When active and passive authentication methods are combined, active authentication is intended to be used as a backup, to be used only when passive authentication fails.

DO NOT REPRINT**© FORTINET**

Active Authentication Behavior

- Enable authentication on every policy that could match the traffic:
 - All firewall policies must have authentication enabled (active or passive)
- If there is a fall-through policy in place, unauthenticated users will not be prompted for authentication

- Enforce authentication on demand option:

- CLI option only

```
# config user setting
(setting) # set auth-on-demand
<always|implicit>
Implicit - default option. It will not
trigger authentication if there is a fall
through policy.
Always - Trigger authentication prompt for
policies that have active authentication
enabled regardless of a fall through policy
```

- Provides more granular control
 - Authentication is enabled at a firewall policy level
- Passive authentication policies must be placed on top of active authentication policy

- Enable a captive portal on the ingress interface for the traffic:

- Authentication happens at an interface level
- Traffic will not be allowed without valid authentication unless it matches an exemption
- All users will be prompted for authentication before they can access any resource

© Fortinet Inc. All Rights Reserved.

38

As mentioned earlier, there are three different ways you can alter active authentication behavior. If you have an active authentication firewall policy followed by a fall-through policy that does not have authentication enabled on it, then all traffic will use the fall-through policy. This means that users will not be asked to authenticate. By default, all traffic will pass through the catch-all policy without being authenticated. You can alter this behavior by enabling authentication on all firewall policies. When you enable authentication, all the systems will have to authenticate before traffic is placed on egress interface.

Alternatively, only on the CLI, you can change the auth-on-demand option to always. This will instruct FortiGate to trigger an authentication request, if there is a firewall policy with active authentication enabled. In this case, the traffic will not be allowed until authentication is successful.

If you wish to have all users connect to a specific interface, then it is better to enable captive portal authentication at the interface level. This way, all devices must authenticate before they are allowed to access any resources.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Firewall policies dictate whether a user or device can or cannot authenticate on a network. Which statement about firewall authentication is true?
 - A. Firewall policies can be configured to authenticate certificate users.
 - B. The order of the firewall policies always determines whether a user's credentials are determined actively or passively.

2. Which statement about active authentication is true?
 - A. Active authentication is always used before passive authentication.
 - B. The firewall policy must allow the HTTP, HTTPS, FTP, and/or Telnet protocols in order for the user to be prompted for credentials.



© Fortinet Inc. All Rights Reserved.

39

DO NOT REPRINT**© FORTINET**

Lesson Progress



Methods of Firewall Authentication



Remote Authentication Servers



User Groups



Authentication Using Firewall Policies



Authenticating Through Captive Portal



Monitoring and Troubleshooting

Good job! You now understand how to use firewall policies for authentication.

Now, you will learn about authenticating through captive portal.

DO NOT REPRINT

© FORTINET

Authenticating Through Captive Portal

Objectives

- Configure captive portal and disclaimers

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

By demonstrating competence in captive portal, you will be able to configure authentication through a captive portal.

DO NOT REPRINT**© FORTINET**

Captive Portal

- Authenticates users on web pages that request a username and password
 - Enabled at interface level
- Only active authentication methods can use captive portal
- Can host captive portal on FortiGate or an external authentication server

Network > Interfaces

The screenshot shows the 'Network > Interfaces' configuration screen. Under the 'Security mode' section, the dropdown menu is set to 'Captive Portal'. Below this, under 'User access', the 'Restricted to Groups' tab is selected. A group named 'CP-group' is listed. At the bottom, there are options for 'Redirect after Captive Portal'.

© Fortinet Inc. All Rights Reserved.

42

If you want all users connecting to the network to be prompted for their login credentials (active authentication), you can enable captive portal. Captive portal is a convenient way to authenticate web users on wired or Wi-Fi networks through an HTML form that requests a username and password.

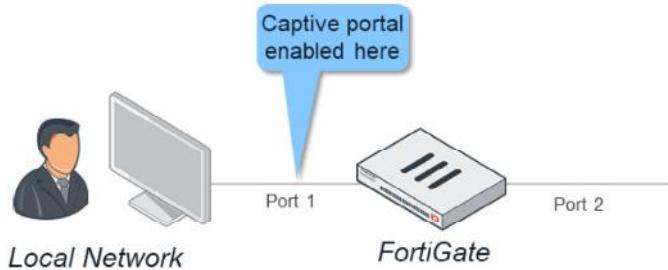
You can host a captive portal on a FortiGate device or an external authentication server, such as a FortiAuthenticator.

DO NOT REPRINT

© FORTINET

Configuring Captive Portal

- Configured on network interfaces



- For Wi-Fi, Wi-Fi SSID must first exist

The screenshot shows two configuration pages from the FortiGate management interface:

- Network > Interfaces**: Shows 'Port 1' configured with 'Security mode' set to 'Captive Portal'. Other settings include 'Authentication portal' (Local), 'User access' (Restricted to Groups), and 'User groups' (CP-group).
- WiFi & Switch Controller > SSIDs**: Shows the 'WIFI' SSID created with 'Security mode' set to 'Captive Portal'. Other settings include 'Authentication' (selected) and 'User groups' (Guest-group).

At the bottom right, there is a copyright notice: © Fortinet Inc. All Rights Reserved.

43

Captive portal, for both wired and Wi-Fi networks, is enabled at the interface level—regardless of the firewall policy that allows it or the port that it ultimately leaves by (authentication being enabled or disabled on the policy is not a factor). This is true for any network interface, including Wi-Fi and VLAN interfaces. On the local network, the captive portal setting must be enabled on the incoming port.

You can configure a captive portal on the **Interfaces** page. Select the required interface. On the **Network** section, enable **Security mode**, and in the drop-down list, select **Captive Portal**. Note that if you are configuring captive portal for a Wi-Fi network, the Wi-Fi SSID must first exist.

Captive portals are not compatible with interfaces in DHCP mode.

DO NOT REPRINT**© FORTINET**

User Access—Restricted to Groups and Allow All

- Restricted to Groups**

- Only groups configured under the **Admission Control** section can successfully authenticate and access resources

Network > Interfaces

Network

Device detection: Security mode: Captive Portal
Authentication portal: Local External
User access: **Restricted to Groups** Allow all
User groups: CP-group, Remote-users

- Allow all:**

- Any groups configured on the firewall policies can successfully authenticate and access resources

Network

Device detection: Security mode: Captive Portal
Authentication portal: Local External
User access: **Allow all**
Exempt sources: CP-group, CP-group2
Exempt destinations/services: +

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Auth	LOCAL_SUBNET CP-group CP-group2	all	always	ALL	ACCEPT	Enabled

FORTINET

© Fortinet Inc. All Rights Reserved.

44

In the **Network** section, you also restrict captive portal user access.

Select **Restricted to Groups** to control the access from the captive portal configuration.

Select **Allow all** to control the access in the firewall policy configuration.

DO NOT REPRINT**© FORTINET**

Captive Portal Exemptions

- Can suppress captive portal for specific devices based on address object:
 - Printers, fax machines, and so on

**Option 1**

```
#config user security-exempt-list
  edit <list_name>
    config rule
      edit <name>
        setsrcaddr|dstaddr|service
      next
    end
```

Option 2

```
#config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

45

You can also configure a firewall policy to suppress captive portal for specific addresses, or services. This is useful for devices that are unable to actively authenticate, such as printers and fax machines, but still need to be allowed by the firewall policy. When suppressed, traffic that matches the source or destination is not presented with the captive portal login page.

There are two ways you can bypass captive portal:

- Through a security exemption list in the GUI or the CLI under `config user security-exempt-list`
- Through the firewall policy. In the CLI, edit the policy and set `captive-portal-exempt enable`. All traffic matching this policy is now exempt from having to authenticate through the captive portal.

DO NOT REPRINT**© FORTINET**

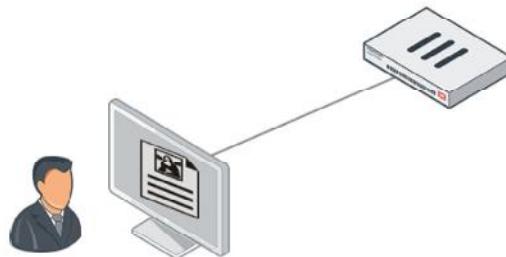
Terms of Service Disclaimer

- Terms and Disclaimer Agreement**

page displays before the user authenticates

- The user must accept the disclaimer to proceed
- After accepting, the user is directed to the intended destination

```
#config firewall policy
edit <policy_id>
    set disclaimer enable
end
```



FORTINET

© Fortinet Inc. All Rights Reserved.

46

If you want to enable a terms of service disclaimer to be used in combination with captive portal authentication, you can do so by using the `config firewall policy` and `set disclaimer enable` command on the CLI. The terms of service disclaimer states the legal responsibilities of the user and the host organization. When you enable the disclaimer, the user must agree to the terms outlined in the statement in order to proceed to the requested URL. When enabled, the terms of service disclaimer opens immediately following a successful authentication.

Neither a security exemption list, nor a captive portal exemption on a firewall, can bypass a disclaimer.

DO NOT REPRINT**© FORTINET**

Customizing Portal Messages

- In the Replacement Messages section, click **Extended View**
- Not all disclaimers are, or need to be, the same
 - Text can be altered.
 - Images can be added (to HTML messages)

System > Replacement Messages

Name	Description	Modified
Admin (2)		
Post-login Disclaimer Message	Replacement message for post-login disclaimer	
Pre-login Disclaimer Message	Replacement message for pre-login disclaimer	
Alert E-mail (5)		

Post-login Disclaimer Message

Message Format: text/plain Message Size: 760 B/32.8 kB

```

POST WARNING:
This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. All users of this system consent to monitoring at all times. Users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information of the user, may be provided to law enforcement officials. If monitoring reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of this system are subject to appropriate disciplinary action.

Last Successful Login: None
Last Failed Login: None
  
```

Restore Defaults Save Cancel

FORTINET

© Fortinet Inc. All Rights Reserved. 47

FortiGate allows you to customize portal messages, which include the login page and disclaimer page. You can customize the messages on the **Replacement Messages** page.

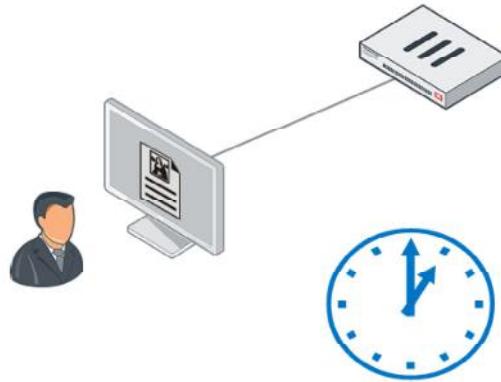
The disclaimer page is in HTML, so you must have knowledge of HTML in order to customize the message. The default layout is **Simple View**, which hides most of the replacement messages. Use **Extended View** to show all editable replacement messages.

DO NOT REPRINT**© FORTINET**

Authentication Timeout

```
#config user setting
    set auth-timeout-type [idle-timeout|hard-timeout|new-session]
end
```

- Timeout specifies how long a user can remain idle before the user must authenticate again
 - Default is 5 minutes
- Three options for behavior:
 - Idle (default): No traffic for that amount of time
 - Hard: Authentication expires after that amount of time, regardless of activity
 - New session: Authentication expires if no new session is created in that amount of time



FORTINET

© Fortinet Inc. All Rights Reserved.

48

An authentication timeout is useful for security purposes. It minimizes the risk of someone using the IP of the legitimate authenticated user. It also ensures users do not authenticate and then stay in memory indefinitely. If users stayed in memory forever, it would eventually lead to memory exhaustion.

There are three options for timeout behavior:

- **Idle:** Looks at the packets from the host's IP. If there are no packets generated by the host device in the configured timeframe, then the user is logged out.
- **Hard:** Time is an absolute value. Regardless of the user's behavior, the timer starts as soon as the user authenticates and expires after the configured value.
- **New session:** Even if traffic is being generated on existing communications channels, the authentication expires if no new sessions are created through the firewall from the host device within the configured timeout value.

Choose the type of timeout that best suits the authentication needs of your environment.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which statements about captive portal is true?
 - A. Captive portal must be hosted on a FortiGate device.
 - B. Captive portal can exempt specific devices from authenticating.

2. Which statement best describes the authentication idle timeout feature on FortiGate?
 - A. The length of time FortiGate waits for the user to enter their authentication credentials
 - B. The length of time an authenticated user is allowed to remain authenticated without any packets being generated by the host device



© Fortinet Inc. All Rights Reserved.

49

DO NOT REPRINT**© FORTINET**

Lesson Progress



Methods of Firewall Authentication



Remote Authentication Servers

User Groups

Authentication Using Firewall Policies



Authenticating Through Captive Portal



Monitoring and Troubleshooting

Good job! You now understand authenticating though captive portals.

Now, you will learn about monitoring and troubleshooting.

DO NOT REPRINT

© FORTINET

Monitoring and Troubleshooting

Objectives

- Monitor firewall users
- Use troubleshooting tools
- Use best practices

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

By demonstrating competence in monitoring and troubleshooting, you will be able to monitor authenticated users and troubleshoot any issues that may occur.

DO NOT REPRINT**© FORTINET**

Monitoring Users

Dashboard > User & Devices > Firewall Users

User Name	IP Address	User Group	Duration	Traffic Volume	Method
student	10.0.1.10	CP-group	1 minute(s) and 25 second(s)	13.53 kB	Firewall

Confirm

⚠ Are you sure you want to deauthenticate the selected user(s)?

OK Cancel

- Also used to terminate authenticated sessions

© Fortinet Inc. All Rights Reserved.

52

You can monitor users who authenticate through your firewall policies using the **Dashboard > User & Devices > Firewall Users** page. It displays the user, user group, duration, IP address, traffic volume, and authentication method.

It does not include administrators, because they are not authenticating through firewall policies that allow traffic, they are logging in directly on FortiGate.

This page also allows you to disconnect a user, or multiple users, simultaneously.

DO NOT REPRINT

© FORTINET Troubleshooting

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled	SSL upg_deep-inspection	UTM	3.47 MB
	Implicit									

- CLI commands:

- diagnose firewall auth list
 - Shows authenticated users, associated groups and their IP address
- diagnose firewall auth clear
 - Clears all authorized users from the current list
- diagnose debug application fnbamd -l
 - Used to troubleshoot active authentication (must use in conjunction with diagnose debug enable)
- diagnose test authserver radius-direct <ip> <port> <secret>
 - Tests preshared key between FortiGate and the RADIUS server
- diagnose test authserver ldap <server_name> <username> <password>
 - Tests LDAP authentication for the specified user account

FORTINET

© Fortinet Inc. All Rights Reserved.

53

In the web-based manager, a good tool for troubleshooting is the **Bytes** column on the security policy page, which is opened by clicking **Policy & Objects > Firewall Policy**. This column displays the number of bytes that have passed through this policy. This is valuable information to have when you are troubleshooting. When you are testing your configuration (end-to-end connectivity, user authentication, policy use) watching the byte count for an increase can help with troubleshooting. An increase indicates if the policy in question is seeing any traffic, which is useful information if you expect a user to require authentication, but they are never prompted.

Use the following CLI commands to gather more information about users and user authentication attempts to help troubleshoot failed authentication attempts:

- diagnose firewall auth list: Shows authenticated users and their IP address.
- diagnose firewall auth clear: Clears all authorized users from the current list. This is useful when you need to force users to reauthenticate after system or group changes. However, this command can easily result in many users having to reauthenticate, so use it carefully.
- diagnose debug application fnbamd -l: Used to troubleshoot active authentication (must use in conjunction with diagnose debug enable).
- diagnose test authserver radius-direct <ip> <port> <secret>: Tests preshared key between FortiGate and the RADIUS server.
- diagnose test authserver ldap <server_name> <username> <password>: Tests LDAP authentication for the specified user account.

DO NOT REPRINT

© FORTINET

Best Practices

- Set the source IP whenever the remote RADIUS server is accessed through a VPN, since most VPNs do not have an IP address associated with the VPN interface
- Servers should not go through an authentication policy. Use a dedicated, non-authentication policy for each server.

CAUTION: Use extreme caution when selecting the **Include in every User Group** option when configuring a RADIUS server. This option places the RADIUS server, and all users who can authenticate against that server, into *every* FortiGate user group, including groups that are used for administrator access.

Name	FortiAuth-RADIUS
Authentication method	Default Specify
NAS IP	[Input field]
Include in every user group	<input checked="" type="checkbox"/>
Primary Server	
IP/Name	10.0.1.150
Secret	[Input field]

FORTINET

© Fortinet Inc. All Rights Reserved.

54

Use the best practices listed on this slide to avoid unnecessary issues when configuring firewall authentication.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which command would you use to identify the IP addresses of all authenticated users?
A. diagnose firewall auth clear
 B. diagnose firewall auth list



© Fortinet Inc. All Rights Reserved.

55

DO NOT REPRINT**© FORTINET**

Lesson Progress



Methods of Firewall Authentication



Remote Authentication Servers



User Groups



Authentication Using Firewall Policies



Authenticating Through Captive Portal



Monitoring and Troubleshooting

Congratulations! You have completed the lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

Review

- ✓ Describe firewall authentication
- ✓ Identify the different methods of firewall authentication available on FortiGate devices
- ✓ Identify supported remote authentication servers
- ✓ Describe active and passive authentication and the order of operations
- ✓ Configure users for local password authentication, server-based password authentication, and two-factor authentication
- ✓ Configure a remote authentication server
- ✓ Configure user authentication, firewall policies, captive portal, and disclaimers
- ✓ Monitor firewall users
- ✓ Use troubleshooting tools and best practices

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

By mastering the objectives covered in this lesson, you learned how to use authentication on the firewall policies of FortiGate.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Logging and Monitoring

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified: 29 May 2020

In this lesson, you will learn how to configure local and remote logging on FortiGate; view, search, and monitor logs; and protect your log data.

DO NOT REPRINT**© FORTINET**

Lesson Overview



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

DO NOT REPRINT

© FORTINET

Log Basics

Objectives

- Describe the log workflow
- Identify log types and subtypes
- Describe log severity levels
- Describe the layout of a log message
- Describe the effect of logging on performance

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

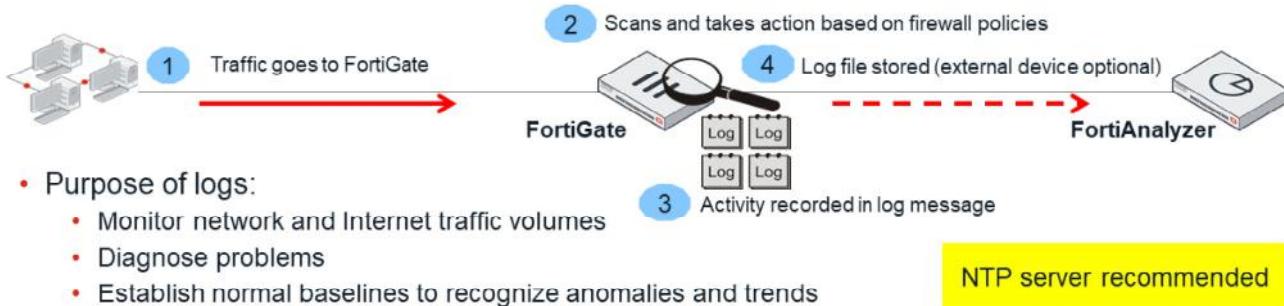
By demonstrating competence in log basics, you will be able to more effectively analyze log data from your database.

DO NOT REPRINT

© FORTINET

Logging Workflow

1. Traffic passes through FortiGate to your network
2. FortiGate scans the traffic and takes action based on configured firewall policies
3. Activity is recorded and the information is contained in a log message
4. Log message is stored in a log file and on a device capable of storing logs (local FortiGate device or an external device, such as FortiAnalyzer)



FORTINET

© Fortinet Inc. All Rights Reserved.

4

When traffic passes through FortiGate to your network, FortiGate scans the traffic, and then takes action based on the firewall policies in place. This activity is recorded, and the information is contained in a log message. The log message is stored in a log file. The log file is then stored on a device capable of storing logs. FortiGate can store logs locally on its own disk space, or can send logs to an external storage device, such as FortiAnalyzer.

The purpose of logs is to help you monitor your network traffic, locate problems, establish baselines, and more. Logs provide you with a greater perspective of your network, allowing you to make adjustments to your network security, if necessary.

Some organizations have legal requirements when it comes to logging, so it is important to be aware of your organization's policies during configuration.

For effective logging, your FortiGate system date and time should be accurate. You can either manually set the system date and time, or configure FortiGate to keep its time correct automatically by synchronizing with a Network Time Protocol (NTP) server. An NTP server is highly recommended.

DO NOT REPRINT**© FORTINET**

Log Types and Subtypes

- *Traffic* logs record traffic flow information, such as an HTTP/HTTPS request and its response (if any)
- *Event* logs record system and administrative events, such as adding or modifying a setting, or daemon activities
- *Security* logs record security events, such as virus attacks and intrusion attempts, based on the security profile type (log type = utm)
 - If no security logs exist, the menu item does not appear in the GUI.

Traffic	Event	Security
Forward	Endpoint Control	Application Control
Local	High Availability	Antivirus
Sniffer	System	Data Leak Prevention (DLP)
	User	Anti-Spam
	Router	Web Filter
	VPN	Intrusion Prevention System (IPS)
	WAD	Anomaly (DoS-policy)
	Wireless	Web Application Firewall (WAF)

WAN optimization logs are found within traffic logs

GPRS Tunneling Protocol (GTP) logs are handled separately from default event logs

© Fortinet Inc. All Rights Reserved.

5

To FortiGate, there are three different types of logs: traffic logs, event logs, and security logs. Each type is further divided into subtypes.

Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response, if any. It contains subtypes named forward, local, and sniffer.

- Forward traffic logs contain information about traffic that FortiGate either accepted or rejected according to a firewall policy.
- Local traffic logs contain information about traffic directly to and from the FortiGate's management IP addresses. They also include connections to the GUI and FortiGuard queries.
- Sniffer logs contain information related to traffic seen by the one-arm sniffer.

Event logs record system and administrative events, such as adding or modifying a setting, or daemon activities. It contains subtypes named endpoint control, high availability, system, user, router, VPN, WAD, and wireless.

- System event logs contain information related to operations, such as automatic FortiGuard updates and GUI logins.
- User logs contain logon and logoff events for firewall policies with user authentication.
- Router, VPN, WAD, and wireless subtypes include logs for those features. For example, VPN contains IPsec and SSL VPN log entries.

Finally, security logs record security events, such as virus attacks and intrusion attempts. They contain log entries based on the security profile type (log type = utm), including application control, antivirus, DLP, anti-spam (email filter), web filter, intrusion protection, anomaly (DoS-policy), and WAF. Security logs and subtypes are only visible in the GUI if logs are created within it—if no security logs exists, the menu item does not appear.

DO NOT REPRINT**© FORTINET**

Log Severity Levels

- Each log entry includes a log level (also known as priority level) that ranges in order of importance
 - 0 = high importance / 6 = low importance

Levels	Description
0 – Emergency	System unstable
1 – Alert	Immediate action required
2 – Critical	Functionality effected
3 – Error	Error exists that can affect functionality
4 – Warning	Functionality could be affected
5 – Notification	Information about normal events
6 – Information	General system information
7 – Debug	Diagnostic information for investigating issues

Rarely used, unless actively investigating an issue with Fortinet Support



© Fortinet Inc. All Rights Reserved.

6

Each log entry includes a log level (or priority level) that ranges in order of importance from emergency to information.

There is also a debug level. It puts diagnostic information into the event log. The debug level is rarely used, unless you are actively investigating an issue with Fortinet Support. Generally, the lowest level you want to use is information, but even this level generates many logs and can cause premature hard disk failure. Depending on the type of log and the needs of your organization, you may want to log only notification levels or higher.

You and your organization's policies dictate what must be logged.

DO NOT REPRINT**© FORTINET**

Log Message Layout

- Log header (similar in all logs)
 - Type and subtype = Name of log file

- Level = Severity level

```
date=2016-06-14 time=12:05:28 logid=0316013056 type=utm subtype=webfilter
eventtype=ftgd_blk level=warning vd=root
```

- Log body (varies by log type)

- policyid = Firewall policy applied to session
- hostname = URL or IP of host

- srcip and dstip = Source and destination IP
- action = Action taken by FortiGate
- msg = Reason for the action

```
policyid=1 sessionid=10879 user="" srcip=10.0.1.10 srcport=60952 srcintf="port3"
dstip=52.81.14.233 dstport=80 dstintf="port1" proto=6 service="HTTP"
hostname="miniclip.com" profile="default" action=blocked reqtype=direct
url="/favicon.ico" sentbyte=297 rcvbyte=0 direction=outgoing
msg="URL belongs to a denied category in policy" method=domain cat=20 catdesc="Games"
crscore=30 crlevel=high
```

FORTINET

© Fortinet Inc. All Rights Reserved.

7

Every log message has a standard layout comprising two sections: a header and a body.

The header contains fields that are common to all log types, such as originating date and time, log identifier, log category, severity level, and virtual domain (VDOM). The value of each field, however, is specific to the log message. In the raw log entry example shown on this slide, the log type is UTM, the subtype is webfilter, and the level is warning. The type and subtype of logs determine what fields appear in the log body.

The body, therefore, describes the reason why the log was created and actions taken by FortiGate. These fields vary by log type. In the example shown on this slide, the fields are as follows:

- the `policyid` field indicates which firewall rule matched the traffic
- the `srcip` field indicates the source IP address
- the `dstip` field indicates the destination IP address
- the `hostname` field indicates the URL or IP of the host
- the `action` field indicates what FortiGate did when it found a policy that matched the traffic
- the `msg` field indicates the reason for the action taken. In this example, the action is `blocked`, which means that FortiGate prevented this IP packet from passing, and the reason is because it belonged to a denied category in the firewall policy.

If you log to a third-party device, such as a syslog server, knowing the log structure is crucial to integration. For information on log structures and associated meanings, visit <http://docs.fortinet.com>.

DO NOT REPRINT**© FORTINET**

Logging in a Security Fabric Design

- Requisite products: Two or more FortiGates and a FortiAnalyzer (a remote logging device)
- With FortiGate, you can enable different security features in different firewalls in the fabric
 - Ensures you do not have to scan and log the same traffic flow more than once when it passes through one firewall
- FortiGate can share network-related information
 - Devices connected to downstream FortiGates will be visible on the upstream device as well (you must enable device detection on the **Interfaces** page of the FortiGate GUI)
- Administrators can view logs and devices connected to the network by logging in to the root FortiGate in the Security Fabric
 - Information is securely shared using the FortiTelemetry protocol



© Fortinet Inc. All Rights Reserved.

8

Collecting logs from the devices in your Security Fabric is important. This is why two or more FortiGate devices and a FortiAnalyzer—a remote logging device—are requisite products at the core of the Security Fabric solution. With FortiGate, you can enable different security features, like antivirus (AV), web filtering, intrusion prevention (IPS), and application control, in different firewalls in the fabric. For example, in the Internal Segmentation firewall (ISFW), you can enable only AV, while in the Next Generation firewall (NGFW) facing the Internet, you can enable web filtering, IPS, and application control. This means you do not have to duplicate scans and logs of the same traffic flow when it passes through multiple firewalls.

The Security Fabric can provide a network topology view (physical and logical), and FortiGate devices can share network-related information. For example, devices connected to downstream FortiGate devices will be visible on the upstream device as well (you must enable device detection on the **Interfaces** page of the FortiGate GUI). In short, administrators can view logs and devices connected to the network by logging on to the root FortiGate in the Security Fabric. This information is securely shared using the FortiTelemetry protocol.

DO NOT REPRINT**© FORTINET**

Effect of Logging on Performance

- More logs = more CPU, memory, and disk space
- Depending on the amount of traffic you have, and the logging settings that are enabled, your traffic logs can swell and impact the performance of your firewall
- Traffic logs record every session
 - Extra information for troubleshooting
 - Some UTM events
 - More system intensive

Enable performance statistic
logging for remote logging
devices on FortiGate

```
# config system global
    set sys-perf-log-interval <number from 0-15>
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

9

It is important to remember that the more logs that get generated, the heavier the toll on your CPU, memory, and disk resources. Storing logs for a period of time also requires disk space, as does accessing them. So, before configuring logging, make sure it is worth the extra resources and that your system can handle the influx.

Also important to note is logging behavior with security profiles. Security profiles can, depending on the logging settings, create log events when traffic matching the profile is detected. Depending on the amount of traffic you have, and logging settings that are enabled, your traffic logs can swell and, ultimately, impact the performance of your firewall.

From the FortiGate CLI, you can enable performance statistic logging for remote logging devices, such as FortiAnalyzer and syslog, to occur every 1-15 minutes (0 to disable). This is not available for local disk logging or FortiCloud.

DO NOT REPRINT**© FORTINET**

Best Practices – Log Management

- You should always have a log management plan that includes and addresses the following:
 - The FortiGate activities that you need logged (for example security features)
 - The logging device that best suits your network architecture
 - The archiving of logs, if required (FortiAnalyzer is recommended)
 - A backup solution to be used in the event of a failure
- Implement a remote logging solution (for example, FortiAnalyzer) and ensure you plan for future growth
- Revisit your plan and backup solution frequently
- Configure alert messages for important activities



© Fortinet Inc. All Rights Reserved.

10

You should always have a log management plan that addresses the following topics:

- The FortiGate activities that you want and need logged (for example, security features)?
- The logging device that is best suited to your network structure
- Log archiving, if required
- A backup solution that will be used in the event of a failure

You should also implement a remote logging solution, such as FortiAnalyzer, and ensure you plan for future growth.

Finally, ensure you revisit your plan and backup solution frequently, and configure alert messages that will notify you of activities that are important.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What type of logs are application control, web filter, antivirus, and DLP?
 - A. Event
 - B. Security

2. The log _____ contains fields that are common to all log types, such as originating date and time, log identifier, log category, and VDOM.
 A. header
 B. body



© Fortinet Inc. All Rights Reserved.

11

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Log Basics****Local Logging****Remote Logging****Log Settings****View, Search, and Monitor Logs****Protect Log Data**

Good job! You now understand log basics.

Now, you will learn about local logging.

DO NOT REPRINT

© FORTINET

Local Logging

Objectives

- Identify local log storage options
- Enable local logging
- Understand disk allocation and reserved space
- Monitor disk usage
- Configure behavior when disk is full

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

By demonstrating competence in local logging, you will be able to successfully store logs to local disk and retain those logs, based on your requirements.

DO NOT REPRINT**© FORTINET**

Log Storage – Local



- FortiGate devices that have a hard drive store logs in an SQL database
- Data is extracted from the SQL database for reports



Local logging

Performance may be impacted under heavy strain

FORTINET

© Fortinet Inc. All Rights Reserved.

14

Storing logs on FortiGate is known as local logging. You can store logs to the device's hard drive.

Typically, mid- to high-end FortiGates have a hard drive. Logging to a hard drive is known as disk logging. Depending on the model series, disk logging may be enabled by default.

FortiGates can store all log types, including log archives and traffic logs locally. Traffic logs and log archives are larger files, and need a lot of room when being logged by FortiGate.

Under heavy log usage, any logging to FortiGate—disk—will result in a performance impact.

If you are using the local hard disk on a device for WAN optimization, you cannot also log to disk (unless your device has two separate disks: you can use one with WAN optimization and the other for logging). If you are using the local hard disk for WAN optimization, you can log to remote FortiAnalyzer devices or syslog servers.

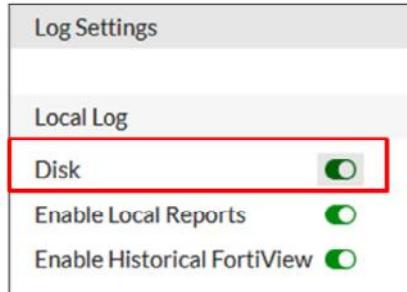
DO NOT REPRINT**© FORTINET**

Enabling Local Logging

- To store logs locally on FortiGate, you must enable disk logging
- With disk logging enabled, the report daemon collects statistics used for historical FortiView from disk
 - If disk logging is disabled, FortiView logs are only available in real-time
- By default, logs older than seven days are deleted from disk (configurable)

```
# config log disk setting
    set maximum-log-age <integer>
```

Log & Report > Log Settings



```
# config log disk setting
    set status enable
```

© Fortinet Inc. All Rights Reserved.

15

If you want to store logs locally on FortiGate, you must enable disk logging from the **Log Settings** page. Only certain FortiGate models support disk logging. If your FortiGate does not support disk logging, you can log to an external device instead. You will learn about remote logging later in this lesson.

Disk logging must be enabled in order for information to appear on the FortiView dashboards. If disabled, logs display in real-time only. You can also enable this setting using the CLI `config log disk setting` command.

By default, logs older than seven (7) days are deleted from the disk (log age is configurable).

DO NOT REPRINT**© FORTINET**

FortiGate Disk Allocation—Reserved Space

- The system reserves approximately 25% of its disk space for system usage and unexpected quota overflow
 - Only ~75% of disk space is available to store logs

```
FGT_A (global) # diagnose sys logdisk usage
Total HD usage: 208MB/118145MB
Total HD logging space: 88608MB
HD logging space usage for vdom "root": 0MB/9965MB
HD logging space usage for vdom "vdom1": 0MB/104857MB
```

Use this command to obtain the amount of reserved space on your FortiGate

- Formulas:
 - disk - logging = reserved (i.e. 118145MB – 88608MB = 29537MB reserved)
 - reserved/disk*100 = reserved % (i.e. 29537/118145*100 = 25%)

FORTINET

© Fortinet Inc. All Rights Reserved.

16

If you decide to log locally on FortiGate, be aware that the entire disk space is not available to store logs. The FortiGate system reserves approximately 25% of its disk space for system usage and unexpected quota overflow.

To determine the amount of reserved space on your FortiGate, use the CLI command `diagnose sys logdisk usage`. Subtract the total logging space from the total disk space to calculate the reserved space.

DO NOT REPRINT**© FORTINET**

Monitoring Disk Usage

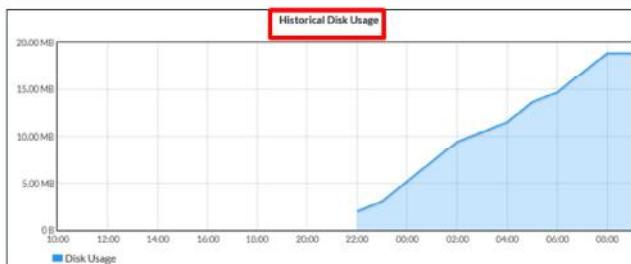
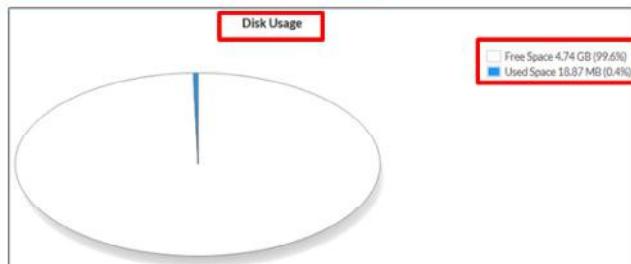
- Local disk usage
 - Free space
 - Used space

- Historical disk usage
 - Volume of disk logging activity over time

Use this command to see how much space is currently being used for logs

```
Local-FortiGate # diagnose sys logdisk usage
Total HD usage: 211MB/31703MB
Total HD logging space: 4755MB
HD logging space usage for vdom "root": 18MB 4755MB
```

Log & Report > Log Settings



© Fortinet Inc. All Rights Reserved.

17

The **Log Settings** page displays two charts to visualize disk space: **Disk Usage**, which is a pie-chart illustrating the free and used space on the internal hard drive, and **Historical Disk Usage**, which displays the volume of disk logging activity over time. These charts may not be visible if disk logging is disabled.

The `diagnose sys logdisk usage` command allows you to view detailed information about how much space is currently being used for logs. FortiGate uses only 75 percent of the available disk capacity to avoid a high storage amount, so the percentage refers to the 75 percent that is available.

DO NOT REPRINT**© FORTINET**

Behavior When Disk Is Full

- By default, when the disk is full, the oldest logs are overwritten
 - Configurable—can set to stop logging when disk is full
- FortiGate issues warnings before disk reaches a full state:
 - First warning: 75%
 - Second warning: 90%
 - Final warning: 95%

Default settings (configurable)

```
# configure log disk setting
    set diskfull [overwrite | nolog]
    set full-first-warning-threshold <1-98>
    set full-second-warning-threshold <2-99>
    set full-final-warning-threshold <3-100>
```



© Fortinet Inc. All Rights Reserved.

18

By default, when your disk is full, the oldest logs are overwritten. However, you can change this behaviour to stop logging when the disk is full using the `config log disk setting` command.

Before your disk reaches a full state, FortiGate sends multiple warnings. By default, the first warning arrives when the disk usage reaches 75%, the second warning at 90%, and the final warning at 95%. These thresholds are configurable using the `config log disk setting` command.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which storage type is preferred for logging?
 A. Remote logging
 B. Hard drive

2. The system reserves approximately ____ % of its disk space for system usage and unexpected quota overflow.
 A. 75
 B. 25

3. By default, what happens when your disk is full?
 A. Logging stops
 B. The oldest logs are overwritten

BONUS: Can you modify this behavior?

Yes

No



DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand local logging.

Now, you will learn about remote logging.

DO NOT REPRINT

© FORTINET

Remote Logging

Objectives

- Identify external log storage options
- Configure remote logging
- Understand how remote logging works with VDOMs
- Understand log transmission
- Enable reliable logging

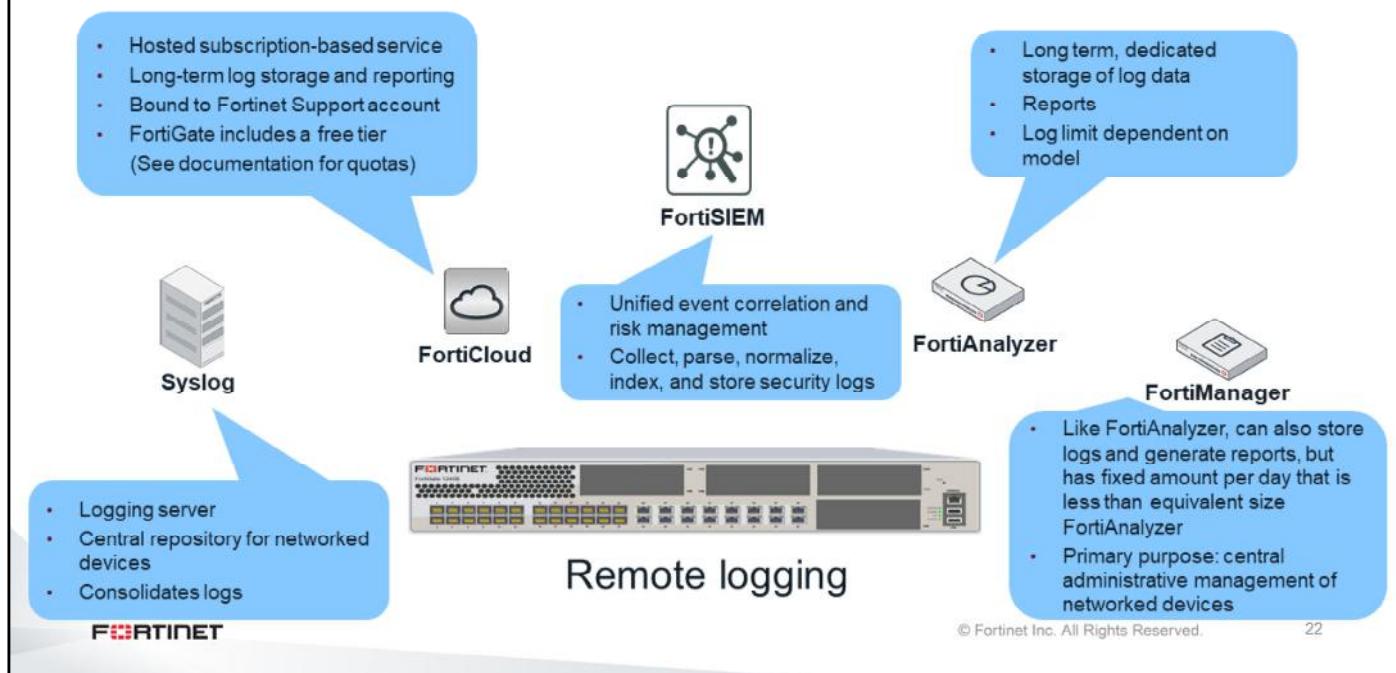
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in remote logging, you will be able to successfully store logs on a remote device and secure log communication.

DO NOT REPRINT

© FORTINET

Log Storage-Remote



If storing logs locally does not fit your requirements, you can store logs externally. You can configure FortiGate to store logs on syslog servers, FortiCloud, FortiSIEM, FortiAnalyzer, or FortiManager. These logging devices can also be used as a backup solution.

Syslog is a logging server that is used as a central repository for networked devices.

FortiCloud is a Fortinet subscription-based, hosted security management and log retention service that offers long-term storage of logs with reporting. If you have a smaller network, FortiCloud is usually more feasible than buying a dedicated logging device. Note that every FortiGate offers a free tier and will keep logs for seven days. You must upgrade to the paid service to retain logs for one year.

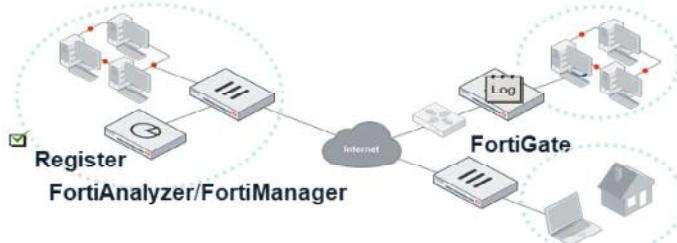
FortiSIEM provides unified event correlation and risk management that can collect, parse, normalize, index, and store security logs.

FortiAnalyzer and FortiManager are external logging devices with which FortiGate can communicate. You can place FortiAnalyzer or FortiManager in the same network as FortiGate, or outside of it. While FortiAnalyzer and FortiManager share a common hardware and software platform and can both take log entries, FortiAnalyzer and FortiManager actually have different capabilities that are worth noting. The primary purpose of FortiManager is to centrally manage multiple FortiGate devices. As such, log volumes are limited to a fixed amount per day, which are less than the equivalent size FortiAnalyzer. On the other hand, the primary purpose of FortiAnalyzer is to store and analyze logs, so the log limit is much higher (though the limit is model dependent). Note that local disk or logging is not required for you to configure logging to FortiAnalyzer or FortiManager.

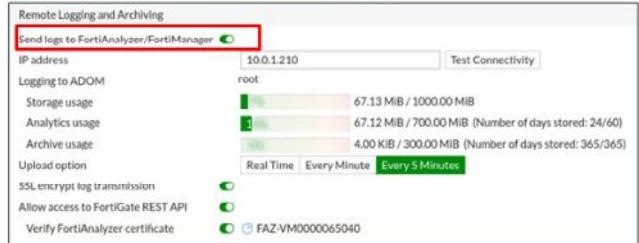
DO NOT REPRINT**© FORTINET**

FortiAnalyzer and FortiManager Log Storage

- FortiGate can send logs to both FortiAnalyzer and FortiManager (FortiGate must be a registered device)



Log & Report > Log Settings



- Can configure up to three separate FortiAnalyzer and FortiManager devices using the CLI
 - Multiple devices may be needed for redundancy
 - Generating and sending logs requires resources—be aware!

```
# config log [fortianalyzer|fortianalyzer2|fortianalyzer3] setting
set status enable
set server <server_IP>
end
```

Commands *not* cumulative

FORTINET

© Fortinet Inc. All Rights Reserved.

23

Configuring FortiGate to send logs to FortiAnalyzer or FortiManager is identical. In order for FortiGate to send logs to either device, you must register FortiGate with FortiAnalyzer or FortiManager. After it is registered, the FortiAnalyzer or FortiManager can begin to accept incoming logs from FortiGate.

You can configure remote logging to FortiAnalyzer or FortiManager using both the GUI and the CLI.

- GUI: On the **Log Settings** page, enable logging to FortiAnalyzer/FortiManager, and type the IP address of the remote logging device.
- CLI: For both FortiAnalyzer and FortiManager, use the `config log fortianalyzer setting` command. Even though FortiManager isn't explicitly mentioned in the command, it is used for FortiManager as well. Using the CLI, up to three separate devices can be added to increase redundancy for the protection of log data. The commands for the three devices are not cumulative. Generating logs uses system resources, so if FortiGate frequently creates and sends logs to multiple places, CPU and RAM usage increase.

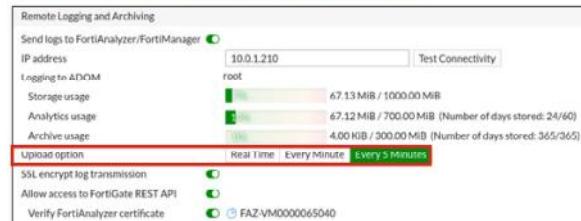
Note that the **Test Connectivity** function on the GUI will report as failing until FortiGate is registered on FortiAnalyzer or FortiManager, because it is not yet authorized to send logs.

DO NOT REPRINT**© FORTINET**

Upload Option

- Near real-time uploading and consistent high-speed compression and analysis
- Configure logging options:
 - store-and-upload (CLI configuration only)
 - Real Time**
 - Every Minute**
 - Every 5 Minutes** (default)

Log & Report > Log Settings



- By default, if the FortiAnalyzer disk is full, the oldest logs are overwritten; however, you can configure FortiAnalyzer to stop logging

© Fortinet Inc. All Rights Reserved.

24

FortiGate allows near real-time uploading and consistent high-speed compression and analysis to FortiAnalyzer and FortiManager.

On the GUI, upload options include **Real Time**, **Every Minute**, and **Every 5 Minutes** (default).

If your FortiGate model includes an internal hard drive, you also have the **store-and-upload** option. This allows you to store logs to disk and then upload to FortiAnalyzer or FortiManager at a scheduled time (usually a low bandwidth time). You can configure the **store-and-upload** option, as well as a schedule, on the CLI only.

DO NOT REPRINT

© FORTINET

FortiAnalyzer Temporarily Unavailable to FortiGate?

- The FortiGate *miglogd* process caches logs on FortiGate when FortiAnalyzer is not reachable
- When maximum cached value is reached, *miglogd* will drop cached logs (oldest first)
- When FortiAnalyzer connection is back, *miglogd* will send the cached logs
 - FortiGate buffer will keep logs long enough to sustain a reboot of FortiAnalyzer, but is not intended for lengthy outages
- FortiGate devices with an SSD have a configurable log buffer

```
Local-FortiGate # diagnose test application miglogd 6
mem=0, disk=4171, alert=0, alarm=0, sys=0, faz=4455, faz-cloud=0, webt=0, fd-
interface-missed=12
Queues in all miglogds: cur:0 total-so-far:42934
global log dev statistics:
faz 0: sent=4455, failed=0 cached=0, dropped=0 , relayed=0
```

Current cache size and total cache size

```
Local-FortiGate # diagnose log kernel-stats
fgtlog: 2
fgtlog 0: total-log=3, failed-log=0 log-in-queue=0
fgtlog 1: total-log=26683, failed-log=0 log-in-queue=0
```

If there are bursts or link is overloaded, failed increases

If queue is full, failed-log value increases

FORTINET

© Fortinet Inc. All Rights Reserved.

25

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the *miglogd* process will begin dropping cached logs (oldest first) once this value is reached. When the connection between the two devices is restored, the *miglogd* process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example), but it is not intended for a lengthy FortiAnalyzer outage.

On FortiGate, the CLI command `diagnose test application miglogd 6` displays statistics for the *miglogd* process, including the total cache size, and current cache size.

The CLI command `diagnose log kernel-stats` will show an increase in `failed-log` if the cache is full and needs to drop logs.

FortiGate devices with an SSD disk have a configurable log buffer. When the connection to FortiAnalyzer is unreachable, the FortiGate is able to buffer logs on disk if the memory log buffer is full. The logs queued on the disk buffer can be sent successfully after the connection to FortiAnalyzer is restored.

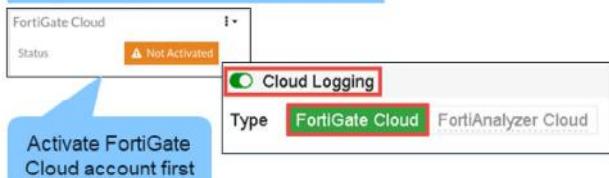
DO NOT REPRINT**© FORTINET**

FortiCloud, Syslog, and FortiSIEM Log Storage

FortiCloud

- Must activate FortiCloud account (dashboard)

Log & Report > Log Settings



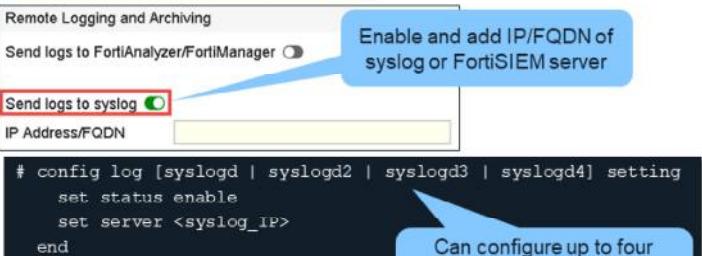
```
# config log fortiguard setting
set status enable
set source-ip <src IP used to connect FortiCloud>
set upload-option <realtime | 1-minute | 5-minute>
set enc-algorithm <high-medium | high | low>
end
```

Encryption algorithm
setting not available to
configure in the GUI

FORTINET

Syslog and FortiSIEM

Log & Report > Log Settings



Can configure up to four
remote syslog service or
FortiSIEMs using the CLI

- FortiGate logs can be sent to syslog servers in default, CSV, or CEF format

```
# config log syslogd3 setting
set format [default | csv | cef]
end
```

© Fortinet Inc. All Rights Reserved.

26

Similar to FortiAnalyzer and FortiManager, you can configure remote logging to FortiCloud on the **Log Settings** page or the CLI. However, you must first activate your FortiCloud account, so FortiGate can communicate with your FortiCloud account. Once complete, you can enable FortiCloud logging and set the upload option. If you want to store your logs to disk first and then upload to FortiCloud, you must specify a schedule. When disk usage is set to WAN optimization (`wanopt`), the store and upload option for logging to FortiCloud is removed.

You can also configure remote logging to syslog and FortiSIEM on the **Log Settings** page or the CLI. You can configure FortiGate to send logs to up to four syslog servers or FortiSIEM devices using the `config log syslogd` CLI command.

FortiGate supports sending logs to syslog in CSV and CEF format, an open log management standard that provides interoperability of security-related information between different network devices and applications. CEF data can be collected and aggregated for analysis by enterprise management or Security Information and Event Management (SIEM) systems, such as FortiSIEM. You can configure each syslog server separately to send log messages in CEF or CSV format.

You can configure an individual syslog to use CSV and CEF format using the CLI. An example shown on this slide is for `syslogd3`. All other syslog settings can be configured as required independently of the log message format, including the server address and transport (UDP or TCP) protocol.

DO NOT REPRINT**© FORTINET**

VDOMs and Remote Logging

- If you have a FortiGate with Virtual Domains (VDOMs) configured, you can globally add multiple FortiAnalyzers and syslog servers.
 - Up to three FortiAnalyzer devices
 - Up to four syslog servers

```
# config global
config log fortianalyzer setting
    set status enable
    set server 10.0.1.1
end
config log fortianalyzer2 setting
    set status enable
    set server 10.0.2.1
end
```

If override FAZ/Syslog
needed, must enable it
from vdom level

```
# config vdom
edit Training
    config log setting
        set faz-override enable
        set syslog-override enable
    end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

27

If you have a FortiGate with virtual domains (VDOMs) configured, you can globally add multiple FortiAnalyzers and syslog servers. You can configure up to three FortiAnalyzer devices and up to four syslog servers under global settings.

DO NOT REPRINT**© FORTINET**

VDOMs and Remote Logging (Contd)

- On each VDOM, you can override the global settings, that allow you to configure up to 3 override FortiAnalyzer devices and up to 4 override syslog servers for that VDOM
- After you enable override, the user can use the CLI to configure multiple FortiAnalyzer devices or syslog servers for their VDOM
- The management VDOM is responsible for sending logs to FortiAnalyzer
- If you use the `override-setting` in a VDOM, then that VDOM is responsible for sending logs to the new FortiAnalyzer or syslog server

Training VDOM

```
# config log
fortianalyzer/fortianalyzer2/fortianalyzer3
override-setting
```

```
# config log syslogd/syslogd2/syslogd3/syslogd4
override-setting
```

Three FortiAnalyzer devices and four syslog servers under VDOM

Training VDOM

```
(Training) # show log fortianalyzer override-setting
config log fortianalyzer override-setting
  set status enable
  set server "10.0.3.1"
end
```

© Fortinet Inc. All Rights Reserved.

28

FORTINET

On each VDOM, you can override the global settings, that allow you to configure up to three override FortiAnalyzer devices, or up to four override syslog servers, or both, for that VDOM.

The management VDOM is responsible for sending logs to FortiAnalyzer devices and syslog servers, So, if you use the `override-setting` in a VDOM, then that VDOM is responsible for sending logs to the new FortiAnalyzer or syslog server that you configured for that VDOM.

DO NOT REPRINT**© FORTINET**

Log Transmission

- FortiGate uses UDP 514 (or TCP 514, if reliable logging is enabled) for log transmission



- Log messages are stored on disk and transmitted to FortiAnalyzer as plain text in LZ4 compressed format
 - Reduces disk log size and reduces log transmission time and bandwidth usage

FORTINET

© Fortinet Inc. All Rights Reserved.

29

FortiGate uses UDP port 514 (or TCP port 514, if reliable logging is enabled) for log transmission.

Log messages are stored on disk and transmitted to FortiAnalyzer as plain text in LZ4 compressed format. This reduces disk log size and reduces log transmission time and bandwidth usage.

DO NOT REPRINT**© FORTINET**

Reliable Logging

- Changes the log transport delivery method from UDP to TCP
- TCP provides reliable data transfer
 - Guarantees the data transferred remains intact and arrives in the same order in which it was sent
 - Error checking and error recovery
 - Acknowledgement segments to ensure packet is received
 - Connection-oriented protocol (SYN, SYN-ACK, ACK handshake)
- If you enable logging to FortiAnalyzer using the GUI, reliable logging is auto-enabled
- If you enable logging to FortiAnalyzer using the CLI, reliable logging is not auto-enabled. You must manually enable using the CLI command:

```
# config log fortianalyzer setting  
set reliable [enable/disable]
```

```
# config log syslogd setting  
set mode udp | reliable | legacy-reliable
```

- FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (default setting is high)

When set to legacy-reliable mode, the default port becomes port 601

FORTINET

© Fortinet Inc. All Rights Reserved.

30

When you enable reliable logging on FortiGate, the log transport delivery method changes from UDP (User Datagram Protocol) to TCP (Transmission Control Protocol). TCP provides reliable data transfer, guaranteeing that the data transferred remains intact and arrives in the same order in which it was sent.

If you enable logging to FortiAnalyzer or FortiManager using the GUI, reliable logging is automatically enabled. If you enable logging using the CLI, you must enable reliable logging using the CLI command shown on this slide.

Logging to FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (the default setting is high).

DO NOT REPRINT

© FORTINET OFTPS

- If using reliable logging, you can encrypt communications using SSL-secured OFTP (OFTPS)

```
# config log fortianalyzer setting
  set status enable
  set enc-algorithm [high-medium | high | low]
  set reliable enable
end
```

Reliable logging
must be enabled to
use OFTPS



© Fortinet Inc. All Rights Reserved.

31

Optionally, if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can encrypt communications using SSL-secured OFTP by configuring the `enc-algorithm` setting on the CLI.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Storing and analyzing logs is the purpose of which device?
 A. FortiAnalyzer
 B. FortiManager

2. What protocol does FortiGate use to send encrypted logs to FortiAnalyzer?
 A. OFTPS
 B. SSL

3. If you enable reliable logging, which transport protocol will FortiGate use?
 A. UDP
 B. TCP



© Fortinet Inc. All Rights Reserved.

32

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand remote logging.

Now, you will learn about log settings.

DO NOT REPRINT

© FORTINET

Log Settings

Objectives

- Configure log settings
- Enable logging on firewall policies
- Hide user names in logs

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

By demonstrating competence in log settings, you will be able to successfully enable logging on your FortiGate, and ensure logs are generated on traffic caused by traffic passing through your firewall policies.

DO NOT REPRINT**© FORTINET**

Logging Preparedness Checklist

Do you want....?	Do this...
Decides if, where, and how a log is stored	<p>Do you want to store logs locally on FortiGate?</p> <p>Enable disk logging. (Log & Report> Log Settings)</p>
	<p>Do you want to be able to view historical FortiView (not just real-time)?</p> <p>Enable historical FortiView. (Log & Report> Log Settings)</p>
	<p>Do you want to enable remote logging to FortiAnalyzer, FortiManager, FortiCloud, FortiSIEM, or syslog?</p> <ul style="list-style-type: none"> • Upload time? • Encrypted log transmission? • Reliable logging? <pre># config log fortianalyzer setting set reliable [enable disable] set enc-algorithm [high-medium high low]</pre>
Decides whether logs are generated based on your firewall policies	<p>Do you want to log allowed traffic on your firewall policy? Security events or all sessions?</p> <p>Configure Log Allowed Traffic setting on your firewall policy. (Policy & Objects> Firewall Policy)</p>
	<p>Do you want to capture logs from traffic sent through your security profiles?</p> <p>Enable one or more security profiles on your firewall policy. (Policy & Objects> Firewall Policy)</p>

FORTINET

© Fortinet Inc. All Rights Reserved.

35

There are two steps involved in configuring logging. You must first configure the logging settings to determine if, where, and how a log is stored. You can configure these settings primarily on the GUI on the **Log Settings** page. You must then configure logging on your firewall policies to determine whether logs are generated. You can configure these settings on the GUI on the **Firewall Policy** page.

The logging preparedness checklist shown on this slide identifies what you need to configure for logging based on your requirements.

DO NOT REPRINT

© FORTINET

Logging Settings: If, Where, and How

The screenshot shows the FortiGate Log & Report interface. On the left, under 'Log & Report > Log Settings', there's a 'Local Log' section with options for Disk, Enable Local Reports, and Enable Historical FortiView. A red box highlights 'Local Log'. To the right, a large red double-headed arrow points between the local log settings and the 'Remote Logging and Archiving' section. This section includes fields for IP address (10.0.1.210), Logging to ADOM (root), Storage usage, Analytics usage, Archive usage, Upload option, SSL encrypt log transmission, Allow access to FortiGate REST API, and Verify FortiAnalyzer certificate. Below these are tabs for Real Time, Every Minute, and Every 5 Minutes. A red box highlights 'Send logs to FortiAnalyzer/FortiManager'. In the center, there's an 'Event Logging' section with 'Local Traffic Log' and 'Customize' buttons. It lists options like Log Allowed Traffic, Log Local Out Traffic, Log Denied Unicast Traffic, and Log Denied Broadcast Traffic. A red box highlights 'Local Traffic Log'. On the right, a list of questions and answers provides context for these settings:

- Log event logs and traffic logs?
- Local traffic logs = traffic directly to and from FortiGate (disabled by default)
- Event logs = system information generated by FortiGate

Below the event logging section is a 'GUI Preferences' box with 'Resolve Hostnames' and 'Resolve Unknown Applications' checkboxes. A red box highlights 'Resolve Hostnames'. To the right, another list of questions and answers provides context for these preferences:

- Translate IPs to host names for convenience? (Can impact CPU usage and page responsiveness.)

At the bottom left is the FORTINET logo. At the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 36.

The **Log Settings** page allows you to decide if, where, and how a log is stored.

As previously discussed, you must configure whether to store logs locally on your FortiGate disk, or remotely to an external device, such as FortiAnalyzer.

You must also configure what event logs and local traffic logs to capture. Local traffic logs provide information about traffic directly to and from FortiGate. By default, this option is disabled because of the large number of logs they can generate. Event logs provide all of the system information generated by FortiGate, such as administrator logins, configuration changes made by administrators, user activity, and daily operations of the device—they are not directly caused by traffic passing through firewall policies. For example, IPsec VPNs closing, or routing protocol activity, are not caused by traffic passing through a firewall policy. One exception might be the user log, because it does record user logon and logoff events on traffic that passes through policies. The event logs you choose to enable depend on what features you are implementing and what information you need to get from the logs.

The **Resolve Hostnames** feature resolves IP addresses to host names. This requires FortiGate to perform reverse DNS lookups for all IP addresses. If your DNS server is not available or is slow to reply, it can impact your ability to look through the logs, because the requests will time out.

DO NOT REPRINT**© FORTINET**

Log Filtering

- Can configure log filter settings to determine which logs are recorded
 - Configure up to four remote syslog or FortiSIEM logging servers:

```
# config log [syslogd | syslogd2 | syslogd3 | syslogd4] filter
```

- Configure up to three FortiAnalyzer devices:

```
# config log [fortianalyzer | fortianalyzer2 | fortianalyzer3] filter
```

- Filters include:

- Severity <level>
- Forward traffic [enable/disable]
- Local traffic [enable/disable]
- Multicast traffic [enable/disable]
- Sniffer traffic [enable/disable]
- Anomaly [enable/disable]
- VOIP [enable/disable]
- DLP archive [enable/disable]
- GTP [enable/disable]
- Filter [string]
- Filter type [include| exclude]



© Fortinet Inc. All Rights Reserved.

37

While the log settings on the GUI allow you to configure what event logs and local traffic logs to capture, you can also set more robust and granular options using the CLI.

Previously, we mentioned that you can configure up to four logging services for syslog and FortiSIEM using the command `config log syslogd` setting, and up to three FortiAnalyzer devices using the `config log fortianalyzer` setting. You can control what logs are sent to each of these devices separately, using the command `config log syslogd filter` for remote syslog or FortiSIEM, and the command `config log fortianalyzer filter` for FortiAnalyzer devices.

In this way, you can set devices to different logging levels and/or send only certain types of logs to one device and other types (or all logs) to others. For example, you can send all logs at information level and above to `fortianalyzer`, alert level and above to `fortianalyzer2`, and only traffic logs to `fortianalyzer3`.

DO NOT REPRINT**© FORTINET**

Enabling Logging on Firewall Policies

- Firewall policy settings decide if a log message caused by traffic passing through a firewall policy is generated or not

Policy & Objects > Firewall Policy

Protocol Options: PRX default

Security Profiles:

- AntiVirus: AV default
- Web Filter: WEB Category-block-and-warning
- DNS Filter: DNS default
- Application Control: APP block-high-risk
- IPS: Off
- SSL Inspection: SSL certificate-inspection

Logging Options:

- Log Allowed Traffic: Security Events (highlighted in red)
- Generate Logs when Session Starts: Off
- Capture Packets: Off

Hardware acceleration affects logging

- Traffic offloaded to NP processors does not log traffic statistics.
 - Can disable hardware acceleration
 - Can enable NP packet logging (degrades NP performance)

© Fortinet Inc. All Rights Reserved. 38

After you configure all logging settings, you can enable logging on your firewall policies. Only when enabled on a firewall policy can a log message—caused by traffic passing through that firewall policy—generate.

Generally, if you configure FortiGate to inspect traffic, you should also enable logging for that security feature to help you track and debug your traffic flow. Except for violations that you consider to be low in severity, you'll want to know if FortiGate is blocking attacks. Most attacks don't result in a security breach on the first try. A proactive approach, when you notice a persistent attacker whose methods seem to be evolving, can avoid a security breach. To get early warnings like this, enable logging for your security profiles.

To enable logging on traffic passing through a firewall policy, you must do the following:

- Enable the desired security profile(s) on your firewall policy.
- Enable **Log Allowed Traffic** on that firewall policy. This setting is vital. If disabled, you will not receive logs of any kind—even if you have enabled a security profile on your firewall policy. You can choose to log only security events, or log all sessions:
 - Security Events:** If enabled (along with one or more security profiles), security log events appear in the forward traffic log and security log. A forward traffic log generates for packets causing a security event.
 - All Sessions:** If enabled, a forward traffic log generates for every single session. If one or more security profiles is also enabled, security log events appear in the forward traffic log and security log.

DO NOT REPRINT**© FORTINET**

Testing Log Settings

```
Local-FortiGate # diagnose log test
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an botnet log message
generating an anomaly log message
generating an application control IM message with level - information
generating an IPv6 application control IM message with level - information
generating deep application control logs with level - information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating a ipv6 traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
generating a VOIP event message with level - information
generating authentication event messages
generating a Forticlient message with level - information
generating a URL block message with level - warning
generating a DNS message with level - warning
generating an ssh-command pass log with level - notification
generating an ssh-channel block with level - warning
generating an ssl-cert_blacklisted log with level - warning
```

Test if logs are generating



© Fortinet Inc. All Rights Reserved.

39

After you configure logging, you can test that the modified settings are working properly. This test is done on the CLI using the `diagnose log test` command.

On the FortiGate GUI, view the logs to see some of the recently generated test log messages. You can distinguish the test log messages from real log messages because they do not have “real” information; for example, the test log messages for the vulnerability scan contain the destination IP address of 1.1.1.1 or 2.2.2.2.

DO NOT REPRINT**© FORTINET**

Hiding User Names in Logs

- Some laws require that usernames be anonymized.
- Use the following command to hide usernames in traffic and UTM logs, so that the username appears as anonymous.

```
# config log setting
  set user-anonymize enable
end
```

```
date=2019-04-26 time=14:45:16 logid=0317013312 type=utm subtype=webfilter
eventtype=ftgd allow level=notice vd="root" policyid=2 identidx=1
sessionid=31232959 user="anonymous" group="ldap_users" srcip=192.168.1.24
srcport=63355 srcintf="port2" dstip=66.171.121.44 dstport=80 dstintf="port1"
service="http" hostname="www.fortinet.com" profiletype="Webfilter_Profile"
profile="default" status="passthrough" reqtype="direct" url="/" sentbyte=304
rcvdbyte=60135 msg="URL belongs to an allowed category in policy" method=domain
class=0 cat=140 catdesc="custom1"
```



© Fortinet Inc. All Rights Reserved.

40

On FortiGate, you can hide usernames in traffic logs and UTM logs, so that the username appears as anonymous. This is useful, because some countries do not permit non-anonymized logging.

To anonymize usernames, use the `set user-anonymize enable` CLI command.

It is assumed that logging is enabled in firewall policies and security profiles, and that identity-based policies are configured on FortiGate.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. In your firewall policy, what setting must you enable to generate logs on traffic sent through that firewall policy?
 A. Log Allowed Traffic
 B. Event Logging

2. Which log type can generate a large number of logs and is therefore disabled by default?
 A. Local Traffic Log
 B. Event Logging

3. What effect does the CLI command set user-anonymize enable have on traffic and UTM logs?
 A. It sets the user name in the logs to anonymous
 B. It sets the user IP in the logs to n/a



© Fortinet Inc. All Rights Reserved.

41

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand log settings.

Now, you will learn how to view, search, and monitor logs.

DO NOT REPRINT

© FORTINET

View, Search, and Monitor Logs

Objectives

- View and search for log messages on the GUI
- View and search for log messages on the CLI
- View logs through FortiView
- Configure alert email
- Configure threat weight

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

By demonstrating competence in viewing, searching, and monitoring logs, you will be able to efficiently locate logs to help support your investigation into any network security issue.

DO NOT REPRINT

© FORTINET

Viewing Log Messages: GUI

The screenshot shows the Fortinet GUI interface for viewing log messages. On the left, a sidebar titled "Log & Report" lists various traffic types and events. The main area displays a table of log messages with columns for Date/Time, Source, Destination, Application Name, Result, Policy, and Application Category. A filter bar at the top says "Set log filters to narrow search". A callout bubble points to the sidebar with the text "GUI menu items depend on incoming logs. Select the log type you want to search." Another callout bubble points to a log entry in the table with the text "Double-click log to view log details". On the right, a "Log location = disk" section shows a "Log Details" pane with tabs for General, Security, Source, Destination, and Application Control. The "General" tab shows details like Date (2020/03/02), Time (08:58:18), Duration (10s), Session ID (1000), and Virtual Domain (root). The "Source" tab shows IP (8.1.1.1), Source Port (10017), Country/Region (United States), Source Interface (port1), and User. The "Destination" tab shows IP (2.2.2.2), Port (20), Country/Region (France), Destination Interface (port2). The "Application Control" tab shows Sensor (default), Application Name (Dropbox_File.Upload), ID (35420), Category (Storage.Backup), Risk (detected), Control Action (detected), Protocol (6), and Service (tcp/20).

Date/Time	Source	Destination	Application Name	Result	Policy	Application Category
2020/03/02 08:58:18	8.1.1.1	2.2.2.2	Dropbox_File.Upload	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	7.1.1.1	2.2.2.2	Dropbox_File.Download	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	6.1.1.1	2.2.2.2	Dropbox_File.Download	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	5.1.1.1	2.2.2.2	Dropbox_File.Download	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	4.1.1.1	2.2.2.2	Dropbox_File.Download	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	3.1.1.1	2.2.2.2	Dropbox_File.Download	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	2.1.1.1	2.2.2.2	Dropbox_File.Download	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup
2020/03/02 08:58:18	1.1.1.1	2.2.2.2	Dropbox_File.Upload	✓ 2.00 kB / 1.00 kB	Full_Access (1)	Storage.Backup

You can access your logs on the GUI in the **Log & Report** menu. The options that appear in this menu depend on your configuration. Security logs appear only if security events exist.

Select the type of log you want to view, such as **Forward Traffic**. Logs on the GUI appear in a formatted table view. The formatted view is easier to read than the raw view, and enables you to filter information when viewing log messages. To view the log details, select the log in the table. The log details then appear in the **Log Details** pane on the right side of the window.

If archiving is enabled on security profiles that support it (such as DLP), archived information appears within the **Log Details** pane in the **Archived Data** section. Archived logs are also recorded when using FortiAnalyzer or FortiCloud.

If you configure FortiGate to log to multiple locations, you can change the log display location in this section. In the example shown on this slide, the log location is set to **Disk**. If logging to a syslog, you must view logs on the syslog instead.

DO NOT REPRINT

© FORTINET

Searching for Logs: Filters

- Add log filters to search for specific logs

Click **Add Filter** and available filter options appear in the drop-down list

Date/Time	#	Source	Device
2020/03/02 0	Action		2.2.2.2
2020/03/02 0	AP Serial		2.2.2.2
2020/03/02 0	Application Category		2.2.2.2
2020/03/02 0	Application ID		2.2.2.2
2020/03/02 0	Application Name		2.2.2.2
2020/03/02 0	Application Risk		2.2.2.2
2020/03/02 0	Archive		2.2.2.2
2020/03/02 0	Authentication Server		2.2.2.2
2020/03/02 0	Band	user (172.16.78.32)	1.1.1.32
2020/03/02 0	Channel	user (172.16.78.32)	1.1.1.32
2020/03/02 0	Date	user (172.16.78.32)	1.1.1.32
2020/03/02 0	Date/Time	user (172.16.78.88)	229.118.95.200
2020/03/02 0	Destination		2.2.2.2
2020/03/02 0	Destination Country/Region		
2020/03/02 0	Destination Device Type		
2020/03/02 0	Destination Family		
2020/03/02 0	Destination Hardware Vendor		

- If the filter you want to add is not showing as a value on the GUI, but does appear in the log itself, add the table column on the GUI

Right-click any table column to add a new column to the table

- Use quick filter options to search data already in the log table

Right-click the column of a specific log for quick filter options



FORTINET

© Fortinet Inc. All Rights Reserved.

45

Depending on your configuration, your FortiGate might record a high volume of logs. This can make it more difficult to locate a specific log, especially during an investigation.

To navigate the logs more efficiently, you can set up log filters. The more information you specify in the filter, the easier it is to find the precise log entry. Filters are configurable for each column of log data on the display. Click **Add Filter** to select the filter from the drop-down list that appears. If you see data that you want to filter on in a log in the table already, you can right-click that data to select the quick filter option. For example, if you see an antivirus log in the table with a specific botnet name, right-click the botnet name in the table and a quick filter option appears that lets you filter on all logs with that botnet name.

By default, the most common columns are shown and less common columns are hidden. Accordingly, if filtering data based on a column that is hidden, be sure to add the column as a selected column. To add columns, right-click any column field, and, in the pop-up menu that appears, select the column in the **Available Columns** section.

If your search filters don't return any results when the log data does exist, the filter may be poorly formed. FortiGate looks for an exact match in the log, so you must form the search string correctly.

DO NOT REPRINT**© FORTINET**

Viewing Logs Associated with a Firewall Policy

- Access log messages generated by individual policies

The screenshot shows the FortiGate management interface under 'Policy & Objects > Firewall Policy'. A context menu is open over a policy named 'P3_to_P1'. The menu options include 'Set Status', 'Filter by Name', 'Copy', 'Paste', 'Insert Empty Policy', and 'Show Matching Logs'. The 'Show Matching Logs' option is highlighted with a red box. The main pane displays a table of logs with columns: Date/Time, %, Source, Device, Destination, Application Name, Result, and Policy. The logs list various DNS queries from 10.0.1.10 to different destinations like dns.google and data.cnn.com.

Date/Time	%	Source	Device	Destination	Application Name	Result	Policy
2020/04/27 14:05:46		10.0.1.10		8.8.8.8 (dns.google)		✓ 69 B / 165 B	P3_to_P1 (1)
2020/04/27 14:05:46		10.0.1.10		8.8.8.8 (dns.google)		✓ 138 B / 370 B	P3_to_P1 (1)
2020/04/27 14:05:32		10.0.1.10		184.24.144.126 (data.cnn.com)			P3_to_P1 (1)
2020/04/27 14:05:23		10.0.1.10		34.213.37.14 (push.services.mozilla.com)		✓ 2.06 kB / 4.49 kB	P3_to_P1 (1)
2020/04/27 14:03:46		10.0.1.10		8.8.8.8 (dns.google)		✓ 69 B / 165 B	P3_to_P1 (1)

You can also access log messages generated by individual policies. Right-click the policy for which you want to view all associated logs and, in the pop-up menu, select **Show Matching Logs**. FortiGate takes you to the **Forward Traffic** page where a filter is automatically set based on the policy UUID.

DO NOT REPRINT**© FORTINET**

Viewing Log Message: CLI

```
# execute log filter
```

Configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view.

```
# execute log display
```

Allows you to see specific log messages that you already configured within the execute log filter command.

```
Local-FortiGate # execute log display
1333 logs found.
10 logs returned.

11: date=2020-03-02 time=08:58:18 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" eventtime=1583168298714133018 tz="-0800" srcip=1.1.1.1 srcport=14464 srcintf="port1" srcintfrule="undefined" dstip=2.2.2.2 dstport=20 dstintf="port2" dstintfrole="undefined" sessionid=80000 proto=6 vrf=32 action="accept" policyid=1 policytype="policy" service="tcp/20" dstcountry="France" srccountry="Australia" transdisp="noop" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block" countenat=1 uthref=65533-264

12: date=2020-03-02 time=08:58:18 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" eventtime=1583168298712504352 tz="-0800" srcip=10.1.1.1 srcport=10019 srcintf="port1" srcintfrule="undefined" dstip=2.2.2.2 dstport=20 dstintf="port2" dstintfrole="undefined" sessionid=10009 proto=6 vrf=32 action="accept" policyid=1 policytype="policy" service="tcp/20" dstcountry="France" srccountry="Reserved" transdisp="noop" appid=38473 app="Vimeo_Video_Play" apprisk="medium" applist="default" appcat="detected" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 uthref=65533-250

13: date=2020-03-02 time=08:58:18 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" eventtime=1583168298693010196 tz="-0800" srcip=9.1.1.1 srcport=10018 srcintf="port1" srcintfrule="undefined" dstip=2.2.2.2 dstport=20 dstintf="port2" dstintfrole="undefined" sessionid=10008 proto=6 vrf=32 action="accept" policyid=1 policytype="policy" service="tcp/20" dstcountry="France" srccountry="United States" transdisp="noop" appid=38569 app="YouTube_Video_Play" appcat="Video/Audio" apprisk="elevated" applist="default" appcat="detected" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 uthref=65533-236
```



© Fortinet Inc. All Rights Reserved.

47

You are not restricted from viewing log messages on the GUI. You can also view log messages on the CLI, using the execute log display command. This command allows you to see specific log messages that you already configured within the execute log filter command. The execute log filter command configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view.

Logs appear in the raw format view. The raw format displays logs as they appear within the log file.

Similar to the GUI, if you have configured either a syslog or SIEM server, you will not be able to view log messages on the CLI.

DO NOT REPRINT

© FORTINET

Configuring Alert Email

- Send notification to email upon detection of event
- While there is a default mail server preconfigured, it is recommended to configure your own SMTP server first

System > Settings

Email Service

Use custom settings

SMTP Server: 10.200.1.254

Port: Use default (25) Specify

Authentication:

Security Mode: Normal SMTPS STARTTLS

Default Reply To:

FORTINET

Log & Report > Email Alert Settings

Enabled

From: FortiGate@training.lab

To: admin@training.lab

Alert parameter: Events Severity

Interval: 1

Security

Intrusion detected

Virus detected

Web Filter blocked traffic

Policy denied traffic

Administrative

Disk usage exceeds

FortiGuard renewal due within

Administrator login/logout

Configuration change

Firewall authentication failure

HA status change

Configure up to three recipients

Send alert by event or severity

Set how often to send alert

If the alert parameter is set to Events, select the events to generate an alert

© Fortinet Inc. All Rights Reserved.

48

Since you can't always be physically watching the logs on the device, you can monitor events by setting up alert email. Alert emails provide an efficient and direct method of notifying an administrator of events.

Before you configure alert email, you should configure your own SMTP server on your FortiGate first. The FortiGate has an SMTP server preconfigured, but it is recommended that you use your internal email server if you have one.

You can configure alert emails on the **Email Alert Settings** page. You can trigger alert emails based on event (such as any time an intrusion is detected or the web filter blocked traffic), or on minimum log severity level (such as all logs at the Alert level or above). You can configure up to three recipients.

DO NOT REPRINT**© FORTINET**

Configuring Threat Weight

- Prioritize solving the most relevant issues by configuring severity levels for IPS signatures, web categories, and applications with a threat weight
- Set risk level values for low, medium, high, and critical

Risk Level Values	
Low	5
Medium	10
High	30
Critical	50

- View detected threats from **Dashboard > Security**

Log & Report > Threat Weight

Log Threat Weight				
Application Protection				
IPS	Low	Medium	High	Critical
Proxy	Low	Medium	High	Critical
	Off	Low	Medium	High
Intrusion Prevention Detection Severity	Low	Medium	High	Critical
Information	Low	Medium	High	Critical
Low	Off	Low	Medium	High
Medium	Off	Low	Medium	High
High	Off	Low	Medium	High
Critical	Off	Low	Medium	High
Malware Detection	Off	Low	Medium	High
Malware	Off	Low	Medium	Critical
Botnet C&C Communication	Off	Low	Medium	Critical
Packet Based Inspection	Off	Low	Medium	High
Blocked by Firewall Policy	Off	Low	Medium	Critical
Failed Connection Attempts	Off	Low	Medium	Critical
Web Activity	Off	Low	Medium	High
Blocked URLs	Off	Low	Medium	High
Malicious Websites	Low	Medium	High	Critical
Phishing	Low	Medium	High	Critical
Spare URLs	Low	Medium	High	Critical
Drug Abuse	Low	Medium	High	Critical
Hacking	Low	Medium	High	Critical
Illegal or Unethical	Low	Medium	High	Critical
Disobedient	Low	Medium	High	Critical
Explicit Violence	Low	Medium	High	Critical
Extremist Groups	Low	Medium	High	Critical
Threat Assistance	Low	Medium	High	Critical
Impersonation	Low	Medium	High	Critical
Child Abuse	Low	Medium	High	Critical
Peer-to-peer File Sharing	Low	Medium	High	Critical
Pornography	Low	Medium	High	Critical

© Fortinet Inc. All Rights Reserved.

49

In order to prioritize solving the most relevant issues easily, you can configure severity levels for IPS signatures, web categories, and applications that are associated with a threat weight (or score).

On the **Threat Weight** page, you can apply a risk value of either low, medium, high, or critical to each category-based item. Each of these levels includes a threat weight. By default, low = 5, medium = 10, high = 30, and critical = 50. You can adjust these threat weights based on your organizational requirements.

After threat weight is configured, you can view all detected threats on the **Security** page. You can also search for logs by filtering on threat score.

Note that threat weight is for informational purposes only. FortiGate will not take any action based on threat weight.

DO NOT REPRINT**© FORTINET**

Knowledge Check

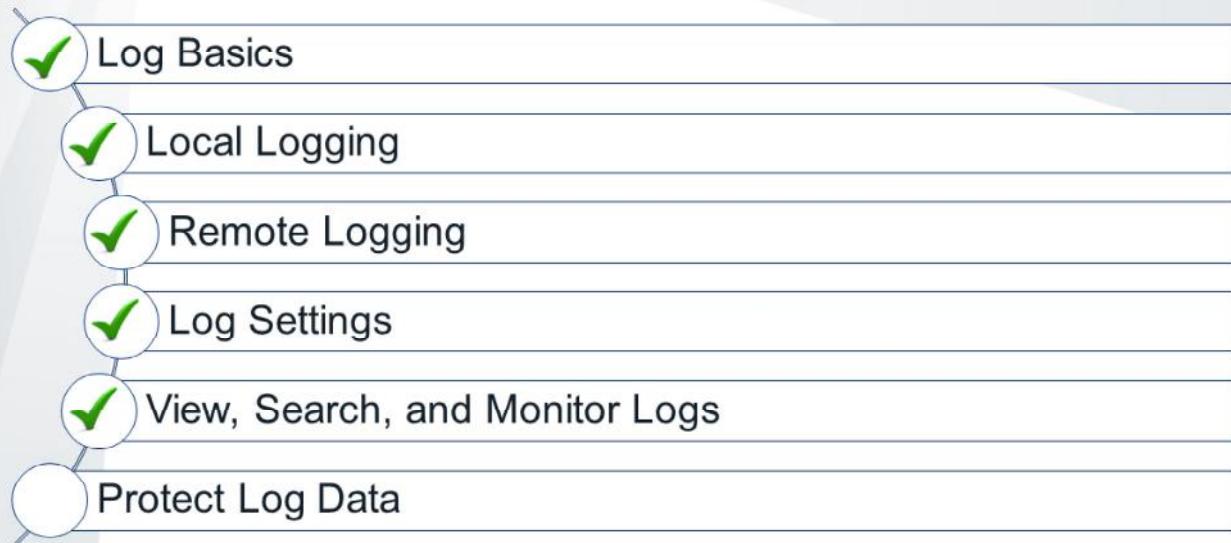
1. On the FortiGate GUI, log _____ can help you find a specific log entry more efficiently.
 A. details
 B. filters

2. With email alerts, you can trigger alert emails based on _____ or log severity level.
 A. event
 B. threat weight



DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand how to troubleshoot communication issues.

Now, you will learn how you can protect your log data.

DO NOT REPRINT

© FORTINET

Protecting Log Data

Objectives

- Perform log backups
- Configure log rolling and uploading
- Perform log downloads

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

By demonstrating competence in the using various methods to protect your logs, you will be able to meet organizational or legal requirements for logs.

DO NOT REPRINT

© FORTINET

Backing Up Logs

- Export all logs to FTP, TFTP, or USB (stored as LZ4 compressed files):

```
# execute backup disk alllogs [ftp | tftp | usb]
```

- Export specific log type to FTP, TFTP, or USB (stored as LZ4 compressed files)

```
# execute backup disk log [ftp | tftp | usb] <log_type>
```



Appears as option in GUI
when you insert a USB drive
into FortiGate's USB port

These backups cannot be
restored to another FortiGate

FORTINET

© Fortinet Inc. All Rights Reserved.

53

You can also protect your log data by performing log backups, which is to say copying log files from the database to a specified location.

The `execute backup disk alllogs` command backs up all logs to FTP, TFTP, or USB, while `execute backup disk log <log type>` backs up specific log types (such as web filter or IPS) to FTP, TFTP, or USB. These logs are stored in LZ4 format and cannot be restored to another FortiGate.

You can also back up logs to USB using the GUI. The GUI menu item appears when you insert a USB drive into FortiGate's USB port.

DO NOT REPRINT**© FORTINET**

Log Rolling and Uploading

Log rolling

- Similar to zipping a file, rolling lowers space requirements needed to contain them
- Can configure max log file size to roll (default 20 MB)
- Can configure roll schedule and time

Log uploading

- Can configure rolled log files to upload to an FTP server
- Can specify which types of log files to upload
- Can configure an upload schedule and time (command not shown—similar to log rolling example)
- Can delete log files after uploading (enabled by default)
- Can configure encrypted FTPS communication

```
# config log disk setting
  set max-log-file-size <1-100>
  set roll-schedule [daily | weekly]
  set roll-day <day of week>
  set roll-time [hh:mm]

# config log disk setting
  set upload [enable | disable]
  set upload-destination [FTP]
  set uploadip [IPv4 IP]
  set uploadport [integer]
  set source-ip [source IPv4 IP]
  set uploaduser [FTP user]
  set uploadpass [FTP user password]
  set uploaddir [remote FTP dir]
  set uploadtype [log type]
  set upload-delete-files [enable* | disable]
  set upload-ssl-conn
```

© Fortinet Inc. All Rights Reserved.

54

FORTINET

Using the `config log disk setting` command, you can configure logs to roll (which is similar to zipping a file) to lower the space requirements needed to contain them so they don't get overwritten. By default, logs roll when they reach 20 MB in size. You can also configure a roll schedule and time.

Using the same CLI command, you can also configure rolled logs to upload to an FTP server to save disk space. You can configure which types of log files to upload, when, and whether to delete files after uploading. You can also configure encrypted FTPS communication.

DO NOT REPRINT**© FORTINET**

Log Downloading

- Download logs to ensure you have a copy when they are eventually overwritten on FortiGate
- Can download logs on the GUI
 - Based on current view, including any log filters set

The screenshot shows the FortiGate GUI with a log table and a download dialog. The log table has columns for Date/Time, %, Source, Device, Destination, Application Name, Result, Policy, and Applic. The download dialog shows the file 'disk-traffic-forward-2020-03-02_0931.log' has been chosen to open. The Firefox download confirmation dialog is overlaid, asking what to do with the file, with 'Save File' selected.

Date/Time	%	Source	Device	Destination	Application Name	Result	Policy	Applic
2020/03/02 08:58:18		1.1.1.1		1.2.2.2				
2020/03/02 08:58:18		1.1.1.1		1.2.2.2				
2020/03/02 08:58:18		1.1.1.1		1.2.2.2				
2020/03/02 08:58:18		1.1.1.1		1.2.2.2				
2020/03/02 08:58:18		test user (172.16.78.32)		1.1.1.32				
2020/03/02 08:58:18		test user (172.16.78.32)		1.1.1.32				
2020/03/02 08:58:18		test user (172.16.78.32)		1.1.1.32				
2020/03/02 08:58:18		test user (172.16.78.88)		229.118.95.200				
2020/03/02 08:58:18		1.1.1.1		1.2.2.2				
2020/03/02 08:58:18		10.1.1.1		1.2.2.2				

- Downloaded in raw format

© Fortinet Inc. All Rights Reserved.

55

You can also download a copy of the logs from FortiGate and save them on a server or on a computer to view and access later. This ensures that you still have a copy when the originals are eventually overwritten on FortiGate.

You can download logs by clicking the download icon on the associated log type page (for example, **Forward Traffic** or **Web Filter**). This only downloads the logs in the results table—not all logs on disk. As such, you can add log filters if you only want to download a subset of logs. When you download the log messages on the GUI, you are downloading log messages in the raw format.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What happens when logs roll?
 - A. It lowers the space requirements needed to contain those logs.
 - B. They are uploaded to an FTP server.

2. When you download logs on the GUI, _____
 - A. all logs in the SQL database are downloaded.
 - B. only your current view, including any filters set, are downloaded.



DO NOT REPRINT**© FORTINET**

Lesson Progress



Congratulations! You have completed this lesson. Now, you will review the topics that you covered in this lesson.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand log basics (log workflow, log types and subtypes, log severity levels, and log message layout)
- ✓ Describe the effect of logging on performance
- ✓ Identify local log storage options
- ✓ Configure local logging
- ✓ Understand disk allocation and reserved space, monitor disk usage, and configure behavior when disk is full
- ✓ Identify external log storage options
- ✓ Configure remote logging
- ✓ Understand log transmission and how to enable reliable logging and OFTPS
- ✓ Configure logging settings
- ✓ Understand miglogd
- ✓ View and search for log messages on the GUI and CLI
- ✓ View logs on FortiView
- ✓ Configure alert email and threat weight
- ✓ Configure log backups, rolling, uploading, downloading

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

By mastering the topics covered in this lesson, you learned to configure local and remote logging, view logs, search logs, and protect your log data.

DO NOT REPRINT**© FORTINET****FORTINET**

FortiGate Security

Certificate Operations

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.Last Modified 29 May 2020

In this lesson, you will learn why FortiGate uses digital certificates, how to configure FortiGate to use certificates (including using certificates to inspect the contents of encrypted traffic), and how FortiGate manages certificates.

DO NOT REPRINT**© FORTINET**

Lesson Overview



Authenticate and Secure Data Using Certificates

Inspect Encrypted Data

Manage Digital Certificates on FortiGate

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

DO NOT REPRINT

© FORTINET

Authenticate and Secure Data Using Certificates

Objectives

- Describe why FortiGate uses digital certificates
- Describe how FortiGate uses certificates to authenticate users and devices
- Describe how FortiGate uses certificates to ensure the privacy of data

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

By demonstrating an understanding of how FortiGate uses certificates, you will better understand how and when certificates could be used in your own networks.

DO NOT REPRINT**© FORTINET**

Why Does FortiGate Use Digital Certificates?

- Inspection
 - FortiGate dynamically generates temporary certificates to perform full SSL inspection
 - FortiGate can inspect certificates to ensure that they are trusted and valid, before permitting a client to connect to an outside device
- Privacy
 - FortiGate uses digital certificates, and their associated private keys, to establish SSL connections with other devices, such as FortiGuard
- Authentication
 - Users who have certificates issued by a trusted certification authority (CA), can authenticate on FortiGate to access the network or to establish a VPN connection
 - Admin users can use certificates as second-factor authentication to log in to FortiGate



© Fortinet Inc. All Rights Reserved.

4

FortiGate uses digital certificates to enhance security.

FortiGate uses digital certificates for inspection. The device can generate certificates on demand for the purpose of inspecting encrypted data that is transferred between two devices; essentially, a man-in-the-middle (MITM) attack. FortiGate can also inspect certificates to identify people and devices (in the network and on the internet), before it permits a person or device to make a full connection to the entity that it is protecting. If FortiGate trusts the certificate, it permits the connection. But if FortiGate does not trust the certificate, it can prevent the connection. How you configure FortiGate determines the behavior; however, other policies that are being used may also affect whether connection attempts are accepted or rejected.

FortiGate uses digital certificates to enforce privacy. Certificates, and their associated private keys, ensure that FortiGate can establish a private SSL connection to another device, such as FortiGuard, a web browser, or a web server.

FortiGate also uses certificates for authentication. Users who have certificates issued by a known and trusted certification authority (CA) can authenticate on FortiGate to access the network or to establish a VPN connection. Administrators users can use certificates as a second-factor authentication, to log in to FortiGate.

DO NOT REPRINT**© FORTINET**

Using Certificates to Identify a Person or Device

- What is a digital certificate?
 - A digital identity produced and signed by a CA
 - Analogy: passport or driver's license
- How does FortiGate use certificates to identify devices and people?
 - The **Subject** and **Subject Alternative Name** fields in the certificate identify the device or person associated with the certificate
- FortiGate uses the X.509v3 certificate standard

Field	Value
Version	V3
Serial number	7e 9b 8a 8d 00 00 00 00 00 6b
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	fortinet-us-FGT-NPS-CA, fort...
Valid from	Tuesday, September 06, 2016...
Valid to	Wednesday, September 06, 2...
Subject	Derek Housley, Training, Otta...
Public key	RSA (1024 Bits)
Certificate Template Name	EFS
Enhanced Key Usage	Encrypting File System (1.3.6....)
Key Usage	Key Encipherment (20)
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	11 d7 43 b3 be 04 4a f9 7d a0...
Authority Key Identifier	KeyID=f3 92 ec cb 4d cf e8 d4...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=d...
Thumbprint algorithm	sha1
Thumbprint	0b ba 6a 93 8d 77 0c 93 bb fb ...

© Fortinet Inc. All Rights Reserved.

5

What is a digital certificate?

A digital certificate is a digital document produced and signed by a CA. It identifies an end entity, such as a person (example, Joe Bloggins), a device (example, webserver.acme.com), or thing (example, a certificate revocation list). FortiGate identifies the device or person by reading the value in the **Subject** field, which is expressed as a distinguished name (DN). FortiGate could also use alternate identifiers, shown in the **Subject Alternative Name** field, whose values could be a network ID or email address, for example. FortiGate can use the **Subject Key Identifier** and **Authority Key Identifier** values to determine the relationship between the issuer of the certificate (identified in the **Issuer** field) and the certificate. FortiGate supports the X.509v3 certificate standard, which is the most common standard for certificates.

DO NOT REPRINT**© FORTINET**

How Does FortiGate Trust Certificates?

- FortiGate does a number of checks against a certificate before trusting it and using it. These checks are:
 - Revocation check
 - You must download the relevant CRLs to FortiGate or configure FortiGate to use OCSP.
 - Certificates are identified by a serial number on the CRL
 - CA certificate possession
 - FortiGate uses the **Issuer** value to determine if FortiGate possesses the corresponding CA certificate
 - Without the corresponding CA certificate, FortiGate cannot trust the certificate
 - Validity dates
 - Digital signature validation
 - The verification of the digital signature on the certificate must pass

Field	Value
Version	V3
Serial number	7e 9b 8a 8d 00 00 00 00 00 00 6b
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	fortinet-us-FGT-NPS-CA, fort...
Valid from	Tuesday, September 06, 2016..
Valid to	Wednesday, September 06, 2..
Subject	Derrick Mueller Training, Ott...
Public key	RSA (1024 Bits)
Certificate Template Name	EFS
Enhanced Key Usage	Encrypting File System (1.3.6....)
Key Usage	Key Encipherment (20)
SMIME Capabilities	[1]S/MIME Capability: Object I...
Subject Key Identifier	11 d7 43 b3 be 04 4a f9 7d a0...
Authority Key Identifier	KeyID=f3 92 ec cb 4d cf e8 d4...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=d...
Thumbprint algorithm	sha1
Thumbprint	0b ba 6a 93 8d 77 0c 93 bb fb ...

© Fortinet Inc. All Rights Reserved.

6

FORTINET

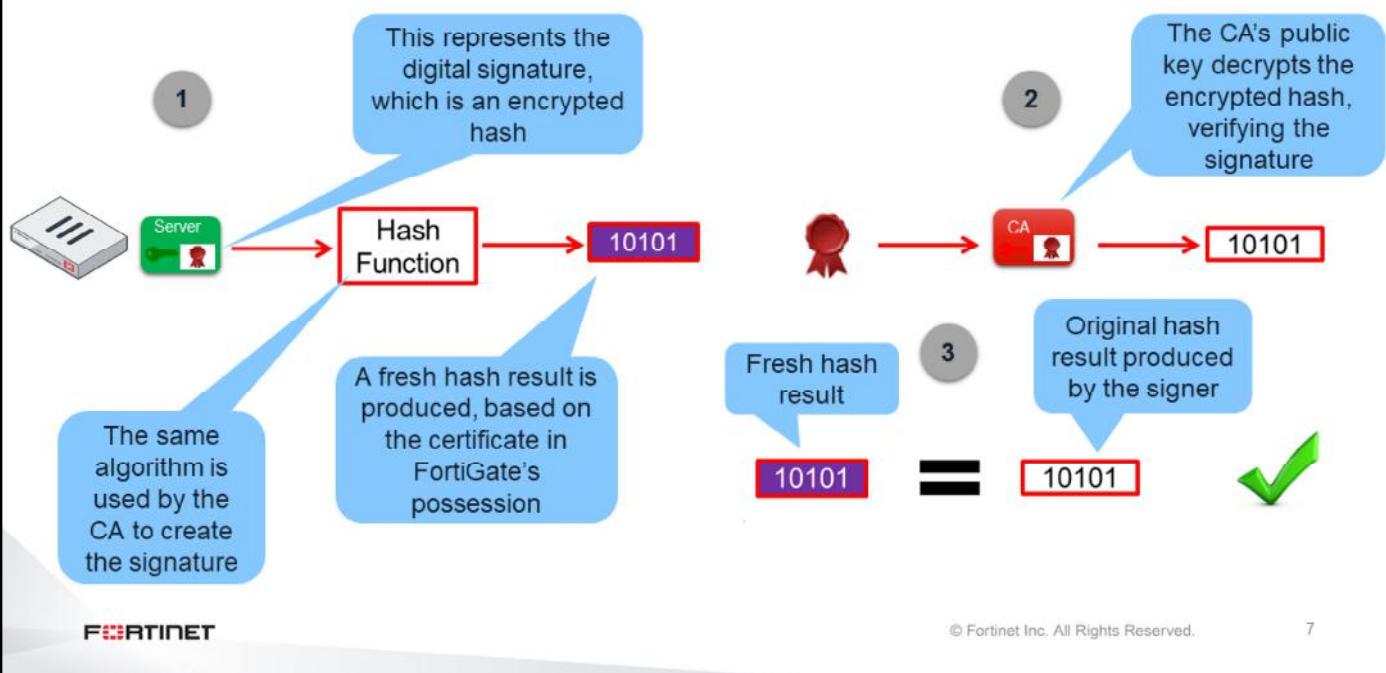
FortiGate runs the following checks before it will trust the certificate:

- Checks the certificate revocation lists (CRLs) locally (on FortiGate) to verify if the certificate has been revoked by the CA. If the serial number of the certificate is listed on the CRL, then the certificate has been revoked and it is no longer trusted. FortiGate also supports Online Certificate Status Protocol (OCSP), where FortiAuthenticator acts as the OCSP responder.
- Reads the value in the **Issuer** field to determine if it has the corresponding CA certificate. Without the CA certificate, FortiGate will not trust the certificate. FortiOS uses the Mozilla CA certificate store. You can view the list by clicking **Security Profiles > SSL Inspection > View Trusted CA List > Factory Bundles**.
- Verifies that the current date is between the **Valid From** and **Valid To** values. If it is not, the certificate is rendered invalid.
- Validates the signature on the certificate. The signature must be successfully validated. Because a valid signature is a critical requirement for trusting a certificate, it may be useful to review how FortiGate verifies digital signatures.

DO NOT REPRINT

© FORTINET

FortiGate Verifies a Digital Signature



Before it generates a digital signature, the CA runs the content of the certificate through a hash function, which produces a hash result. The hash result, which is a mathematical representation of the data, is referred to as the *original hash result*. The CA encrypts the original hash result using its private key. The encrypted hash result is the digital signature.

When FortiGate verifies the digital signature, it runs the certificate through a hash function, producing a fresh hash result. FortiGate must use the same hash function, or hashing algorithm, that the CA used to create the digital signature. The hashing algorithm is identified in the certificate.

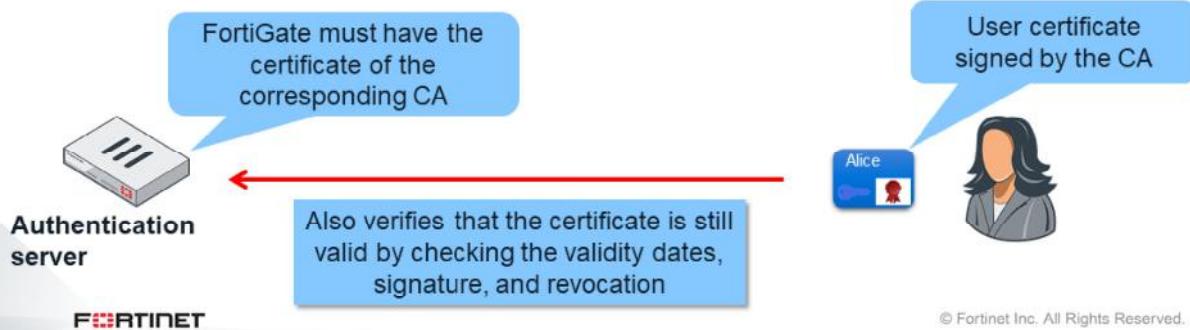
In the second part of the verification process, FortiGate decrypts the encrypted hash result (or digital signature) using the CA's public key, and applying the same algorithm that the CA used to encrypt the hash result. This process verifies the signature. If the key cannot restore the encrypted hash result to its original value, then the signature verification fails.

In the third, and final, part of the verification process, FortiGate compares the fresh hash result to the original hash result. If the two values are identical, then the integrity of the certificate is confirmed. If the two hash results are different, then the version of the certificate that FortiGate has is not the same as the one that the CA signed, and data integrity fails.

DO NOT REPRINT**© FORTINET**

Certificate-Based User Authentication

- A user certificate includes:
 - The digital signature, which is the result of the CA's private key encrypting the hash result of the certificate
 - The user's public key
- To authenticate with a user certificate, the authentication server (FortiGate) must have the CA certificate whose corresponding private key signed the user certificate
 - The CA certificate contains the CA's public key, which allows the authentication server to decrypt and validate anything encrypted and signed by the CA's private key



© Fortinet Inc. All Rights Reserved.

8

Certificate-based user authentication uses an end-entity certificate to identify the user. This certificate contains the user's public key and the signature of the CA that issued the certificate. The authentication server (for example, FortiGate) must have the CA certificate whose private key signed the user certificate. FortiGate verifies that the certificate's signature is valid, that the certificate has not expired, and that the certificate hasn't been revoked. If any of these verifications fail, the certificate-based user authentication fails.

You can configure FortiGate to require that administrators use certificates for second-factor authentication. The process for verifying administrator certificates is the same.

DO NOT REPRINT**© FORTINET**

Self-Signed SSL Certificates

- By default, FortiGate uses a self-signed SSL certificate
 - Not listed with an approved CA, therefore, by default, not trusted

**FORTINET**

© Fortinet Inc. All Rights Reserved.

9

As you can see in the example shown on this slide, trust in the web model is determined by whether or not your certificate store possesses the CA certificate that is required to verify the signature on the SSL certificate. Certificate stores come prepopulated with root and subordinate CA certificates. You can choose to add or remove the certificates, which will affect which websites you trust.

By default, FortiGate uses a self-signed certificate to authenticate itself to HTTPS clients.

Self-signed certificates can be configured to establish SSL sessions, just like those certificates issued by Verisign, Entrust Datacard, and other certificate vendors. But, because self-signed certificates do not come prepopulated in client certificate stores, your end users will get a security warning. You can choose to add the self-signed certificate to clients, or to purchase an SSL certificate from an approved CA vendor for your FortiGate.

DO NOT REPRINT**© FORTINET**

FortiGate Uses SSL for Privacy

- SSL features:
 - Privacy of data
 - Identifies one or both parties using certificates
 - Uses symmetric and asymmetric (public key) cryptography
- Symmetric cryptography
 - Uses the same key to encrypt and decrypt data
 - When FortiGate establishes an SSL session between itself and another device, the symmetric key (or rather the value to produce it) must be shared so that data can be encrypted by one side, sent, and decrypted by the other side
- Asymmetric cryptography
 - Uses a pair of keys. One key performs one function and the other key performs the opposite function. For example, if FortiGate connects to a web server to initiate an SSL session, it would use the web server's public key to encrypt a string known as the pre-master secret. The web server's private key would decrypt the pre-master secret



© Fortinet Inc. All Rights Reserved.

10

FortiGate uses SSL to ensure that data remains private when connecting with servers, such as FortiGuard, and with clients, such as a web browser. Another feature of SSL is that one or both parties can be identified using certificates. SSL uses symmetric and asymmetric cryptography to establish a secure session between two points.

It is beneficial to understand the high-level process of an SSL handshake, in order to understand how FortiGate secures private sessions.

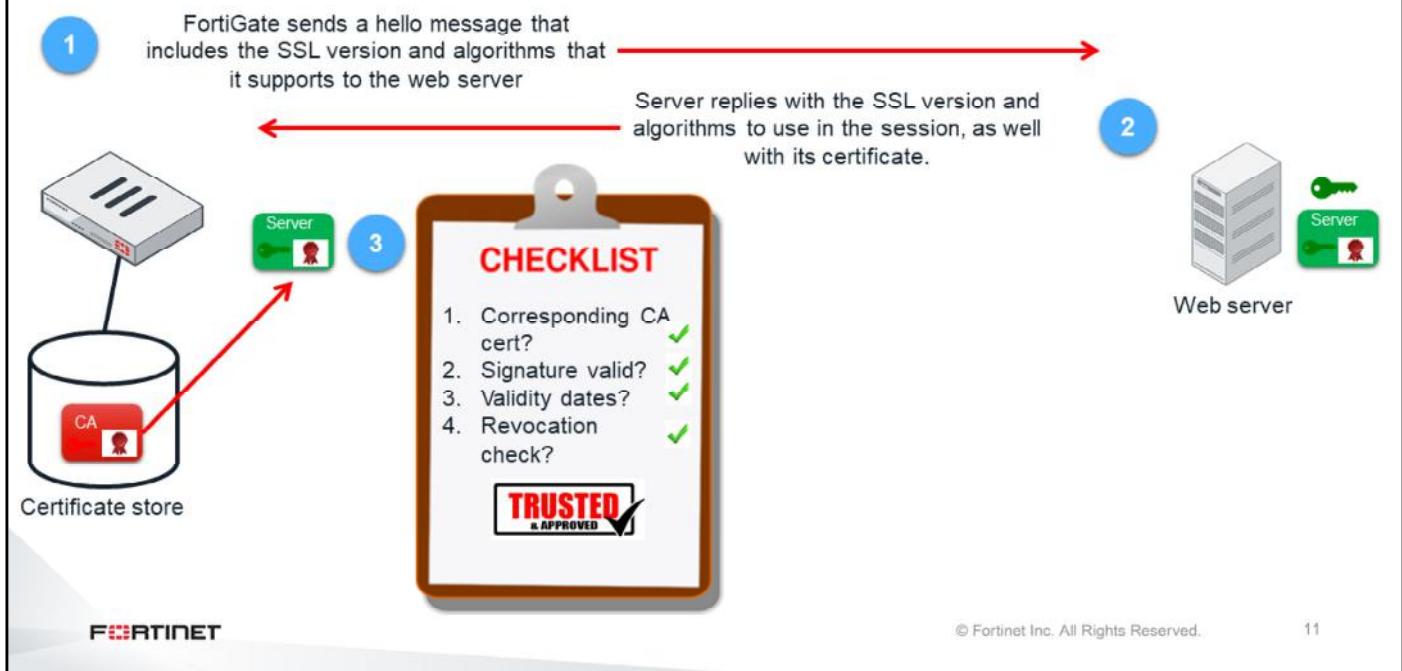
An important attribute of symmetric cryptography is that the same key is used to encrypt and decrypt data. When FortiGate establishes an SSL session between itself and another device, the symmetric key (or rather the value required to produce it), must be shared so that data can be encrypted by one side, sent, and decrypted by the other side.

Asymmetric cryptography uses a pair of keys: one key performs one function and the other key performs the opposite function. When FortiGate connects to a web server, for example, it uses the web server's public key to encrypt a string known as the pre-master secret. The web server's private key decrypts the pre-master secret.

DO NOT REPRINT

© FORTINET

SSL Between FortiGate and a Web Server—Part 1



Now, you will learn more about the process of establishing an SSL session.

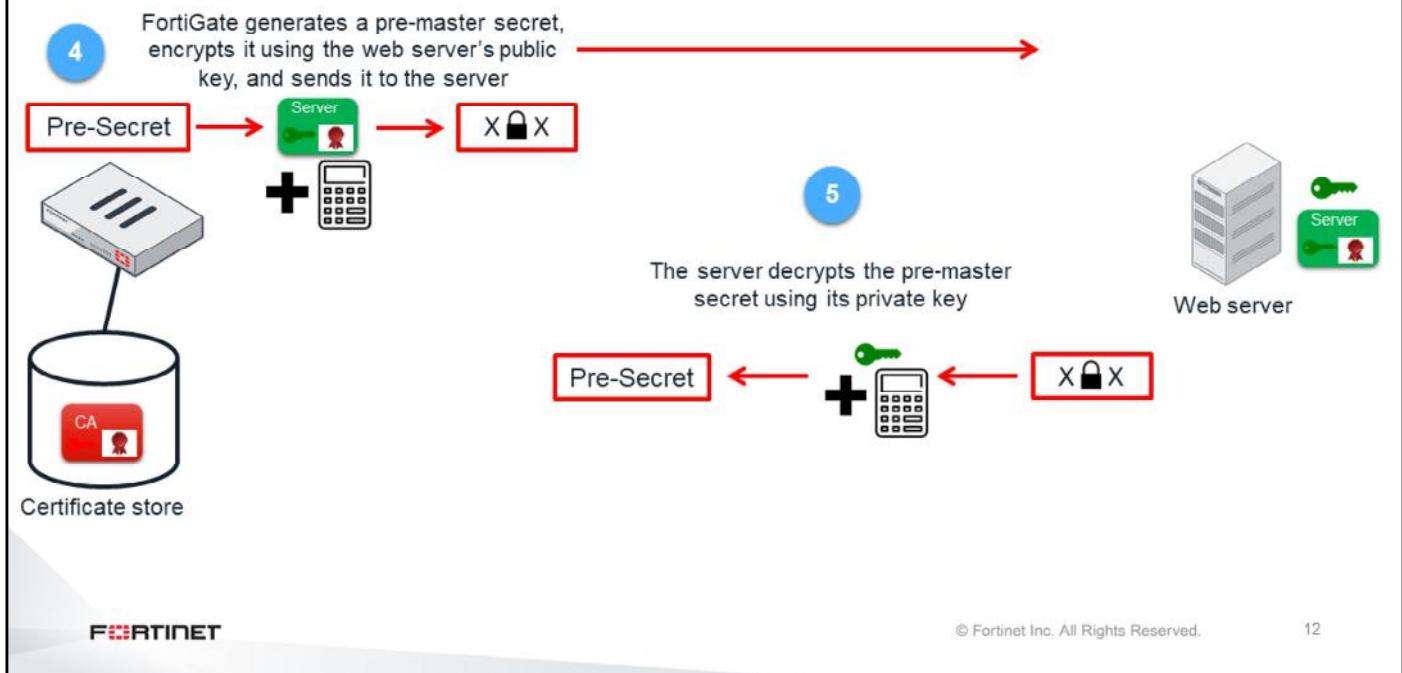
In the first step of the example shown on this slide, FortiGate connects to a web server that is configured for SSL. In the initial hello message, the browser provides critical information that is needed to communicate with the web server. This information includes the server's SSL version number and the names of the cryptographic algorithms that it supports.

In the second step, the web server receives the message from FortiGate, and chooses the first suite of cryptographic algorithms that is in FortiGate's list and that it supports. The web server sends its certificate to FortiGate. Note that the certificate information is passed as clear text over the public network. The information contained in a certificate is typically public, so this is not a security concern.

In the third step, FortiGate validates the web server's certificate. The checklist shown on the slide represents the checks that FortiGate performs on the certificate to ensure that it can be trusted. If FortiGate determines that the certificate can be trusted, then the SSL handshake continues.

DO NOT REPRINT**© FORTINET**

SSL Between FortiGate and a Web Server—Part 2



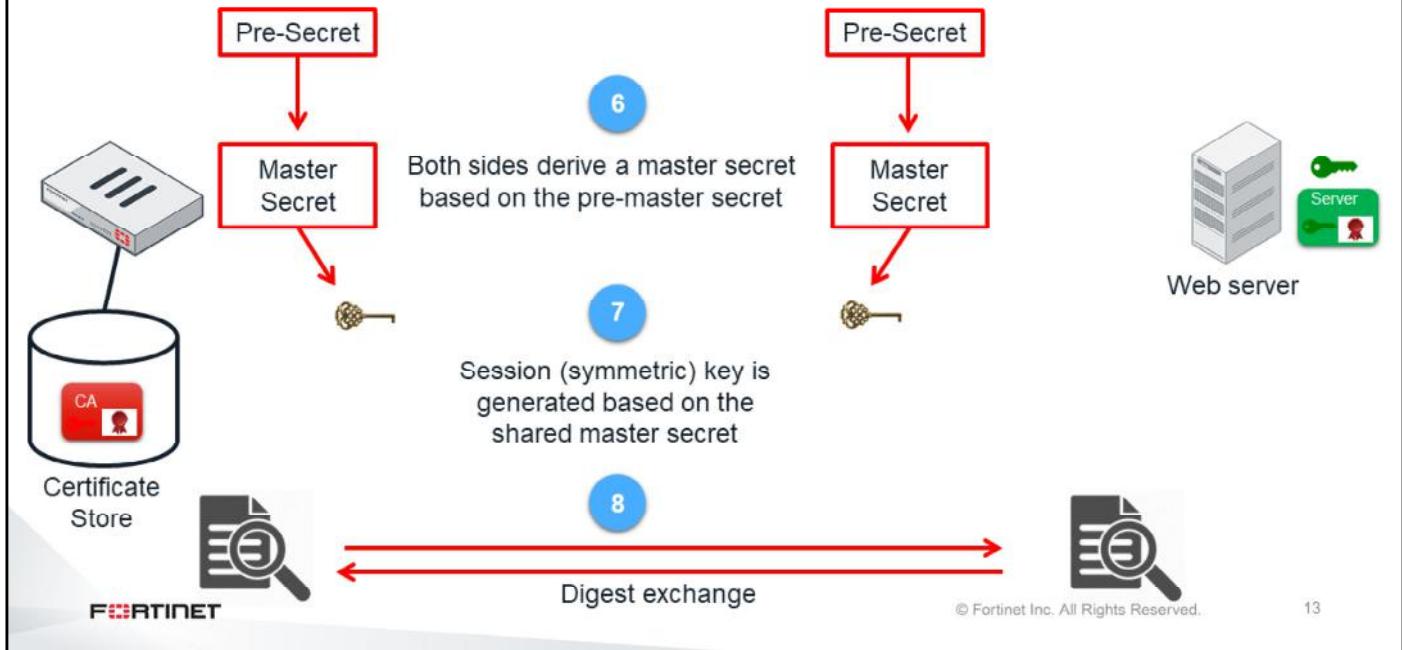
In the fourth step, FortiGate generates a value known as the pre-master secret. FortiGate uses the server's public key, which is in the certificate, to encrypt the pre-master secret. FortiGate then sends the encrypted pre-master secret to the web server. If a third-party intercepted the pre-master secret, they would be unable to read it, because they do not have the private key.

In the fifth step, the web server uses its private key to decrypt the pre-master secret. Now, both FortiGate and the web server share a secret value that is known by only these two devices.

DO NOT REPRINT

© FORTINET

SSL Between FortiGate and a Web Server—Part 3



In the sixth step, both FortiGate and the web server derive the master secret based on the pre-master secret.

In the seventh step, based on the master secret value, FortiGate and the web server generate the session key. The session key is a symmetric key. It is required to encrypt and decrypt the data. Because both sides have the session key, both sides can encrypt and decrypt data for each other.

In the eighth, and final step before these two entities establish the secure connection, both FortiGate and the web server send each other a summary (or digest) of the messages sent so far. The digests are encrypted with the session key. The digests ensure that none of the messages exchanged during the creation of the session have been intercepted or replaced. If the digests match, the secure communication channel is established.

The SSL handshake is now complete. Both FortiGate and the web server are ready to communicate securely, using the session keys to encrypt and decrypt the data they send over the network or internet.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What attribute or extension identifies the owner of a certificate?
 A. The subject name in the certificate
 B. The unique serial number in the certificate

2. How does FortiGate determine if a certificate has been revoked?
 A. It checks the CRL that resides on FortiGate
 B. It retrieves the CRL from a directory server



© Fortinet Inc. All Rights Reserved.

14

DO NOT REPRINT**© FORTINET**

Lesson Progress



Authenticate and Secure Data Using Certificates



Inspect Encrypted Data



Manage Digital Certificates on FortiGate

Good job! You now understand why and how FortiGate uses certificates to authenticate devices and people. You also understand how FortiGate uses certificates to ensure the privacy of data as it flows from FortiGate to another device, or from another device to FortiGate.

Now, you will learn how to inspect encrypted data.

DO NOT REPRINT**© FORTINET**

Inspect Encrypted Data

Objectives

- Describe certificate inspection and full SSL inspection
- Configure certificate inspection and full SSL/SSH inspection
- Identify what is required to implement full SSL inspection
- Identify the obstacles to implementing full SSL inspection and possible remedies

After completing this section, you should be able to:

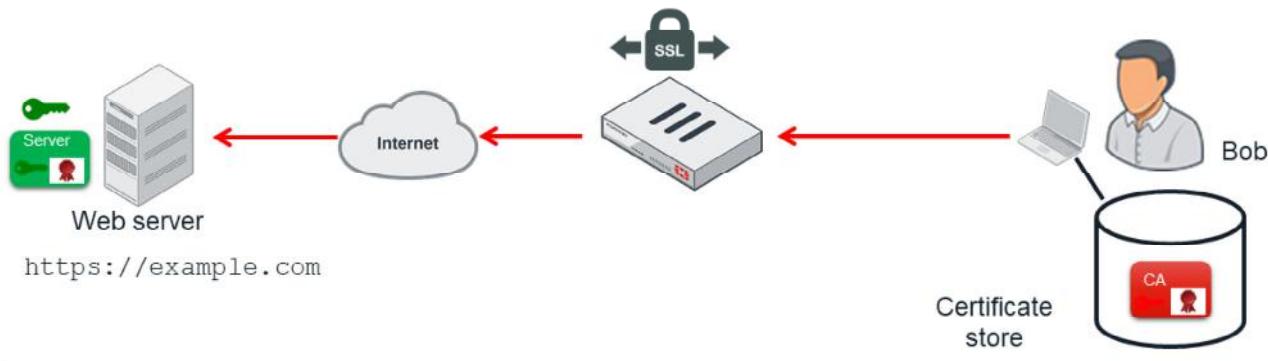
- Describe certificate inspection and full SSL inspection
- Configure certificate inspection and full SSL/SSH inspection
- Identify what is required to implement full SSL inspection
- Identify the obstacles to implementing full SSL inspection and possible remedies

By demonstrating competence in understanding and configuring full SSL inspection and certificate inspection, you will be able to implement one of these SSL inspection solutions in your network.

DO NOT REPRINT**© FORTINET**

No SSL Inspection

- Cloaked by encryption, viruses can pass through network defenses, unless full SSL inspection is enabled



© Fortinet Inc. All Rights Reserved.

17

(slide contains animation)

While there are benefits to using HTTPS, there are risks associated with its use as well, because encrypted traffic can be used to get around normal defenses. For example, if a session is encrypted when you download a file containing a virus, the virus might get past your network's security measures.

In the example shown on this slide, Bob connects to a site with a certificate issued by a legitimate CA. Because the CA is an approved CA, the CA's verification certificate is in Bob's certificate store, and Bob's browser is able to establish an SSL session with the `example.com` site. However, unknown to Bob, the `example.com` site has been infected with a virus. The virus, cloaked by encryption, passes through FortiGate undetected and enters Bob's computer. The virus is able to breach security because full SSL inspection is not enabled.

You can use full SSL inspection, also known as deep inspection, to inspect encrypted sessions.

DO NOT REPRINT**© FORTINET**

SSL Certificate Inspection

- FortiGate uses the server name indication (SNI) to discern the hostname of the SSL server at the beginning of the SSL handshake
 - If there is no SNI, FortiGate looks at the subject and subject alternative name fields
- The only security feature that can be applied using SSL certificate inspection mode is web filtering
- While offering some level of security, certificate inspection does not permit the inspection of encrypted data



© Fortinet Inc. All Rights Reserved.

18

During the exchange of hello messages at the beginning of an SSL handshake, the SSL server sends FortiGate its SNI, which is an extension to the TLS protocol. The SNI tells FortiGate the hostname of the SSL server, which is validated against the DNS name before receipt of the server's certificate. If there is no SNI exchanged, then FortiGate identifies the server by the value in the **Subject** field or **SAN** (subject alternative name) field in the server's certificate.

When certificate inspection is used, FortiGate inspects only the header information of the packets. Certificate inspection is used to verify the identity of web servers and can be used to make sure that HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

The only security feature that can be applied using SSL certificate inspection mode is web filtering. However, since only the packet is inspected, this method does not introduce certificate errors and can be a useful alternative to full SSL inspection when web filtering is used.

Certificate inspection offers some level of security, but it does *not* allow FortiGate to inspect the flow of encrypted data between the outside server and the internal client.

DO NOT REPRINT**© FORTINET**

Configure SSL Certificate Inspection

Security Profiles > SSL/SSH Inspection

Name	SSL	Lock
certificate-inspection	SSL	Locked
custom-deep-inspection	SSL	Locked
deep-inspection	SSL	Locked
no-inspection	SSL	Locked

New SSL/SSH Inspection Profile

Name: My SSL cert inspection prof
Comments: Write a comment...

SSL Inspection Options

Enable SSL inspection of: **Multiple Clients Connecting to Multiple Servers**
Protecting SSL Server

Inspection method: **SSL Certificate Inspection** (Full SSL Inspection)

CA certificate: Fortinet CA_SSL
Blacklisted certificates: Allow, Block, View, Blacklisted Certificates
Untrusted SSL certificates: Allow, Block, Ignore, Untrusted CAs List

Protocol Port Mapping

Inspect all ports:
HTTPS: Port 443

© Fortinet Inc. All Rights Reserved. 19

FortiGate has a read-only preconfigured profile for SSL certificate inspection named **certificate-inspection**. If you want to enable SSL certificate inspection, select this profile when configuring a firewall policy.

Alternatively, you can create your own profile for SSL certificate inspection by following the steps below:

1. On the FortiGate GUI, click **Security Profiles > SSL/SSH Inspection**.
2. Click **Create New** to create a new SSL/SSH inspection profile.
3. Select **Multiple Clients Connecting to Multiple Servers**, and click **SSL Certificate Inspection**.

DO NOT REPRINT**© FORTINET**

Full SSL Inspection—Certificate Requirements

- Full SSL inspection requires that FortiGate act as a CA to generate an SSL private key and certificate as a proxy web server
 - To be compliant with the Internet Engineering Task Force (IETF) RFC 5280, the CA certificate requires these two extensions to issue certificates:
 - cA=True
 - keyUsage=keyCertSign
- FortiGate devices that support full SSL inspection can get their CA certificate from a couple of sources:
 - A self-signed Fortinet_CA_SSL certificate from within FortiGate
 - A certificate issued by an internal CA (FortiGate then acts as a subordinate CA)
- The root CA certificate must be imported into the client machines



© Fortinet Inc. All Rights Reserved.

20

FortiGate must act as a CA in order for it to perform full SSL inspection. The internal CA must generate an SSL private key and certificate each time an internal user connects to an external SSL server. The key pair and certificate are generated *immediately* so the user's connection with the web server is not delayed.

Although it appears as though the user's browser is connected to the web server, the browser is connected to FortiGate. FortiGate is acting as a proxy web server. In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to **cA=True** and the value of the **keyUsage** extension set to **keyCertSign**.

The **cA=True** value identifies the certificate as a CA certificate. The **keyUsage=keyCertSign** value indicates that the certificate's corresponding private key is permitted to sign certificates. For more information, see *RFC 5280 Section 4.2.1.9 Basic Constraints*.

All FortiGate devices that support full SSL inspection can use the self-signed Fortinet_CA_SSL certificate that is provided with FortiGate, or an internal CA, to issue FortiGate a CA certificate. When FortiGate uses an internal CA, FortiGate acts as a subordinate CA. Note that your client machines and devices will need to import the root CA certificate, in order to trust FortiGate and accept an SSL session. The chain of CA certificates must be installed on FortiGate. FortiGate sends the chain of certificates to the client, so that the client can validate the signatures and build a chain of trust.

DO NOT REPRINT**© FORTINET**

Full SSL Inspection on Outbound Traffic—Part 1

- FortiGate requires the private key to decrypt and inspect SSL traffic
 - FortiGate intercepts traffic coming from the server and generates and signs a new certificate with the same subject name

Security Profiles > SSL/SSH Inspection

New SSL/SSH Inspection Profile

Name: My full SSL inspection profile

Comments: Write a comment... 0/355

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers

Inspection method: **Full SSL Inspection**

CA certificate: **Fortinet_CA_SSL**

Blacklisted certificates: Block

Untrusted SSL certificates: Block

Enforce SSL cipher compliance: Off

Enforce SSL negotiation compliance: Off

RPC over HTTPS: On

© Fortinet Inc. All Rights Reserved.

21

Some FortiGate devices offer a mechanism to inspect encrypted data that flows between external SSL servers and internal clients. Without full SSL inspection, FortiGate cannot inspect encrypted traffic, because the firewall does not have the SSL key that is required to decrypt the data, and that was negotiated between client and server during the SSL handshake.

There are two possible configurations for full SSL inspection: one for outbound traffic and one for inbound traffic.

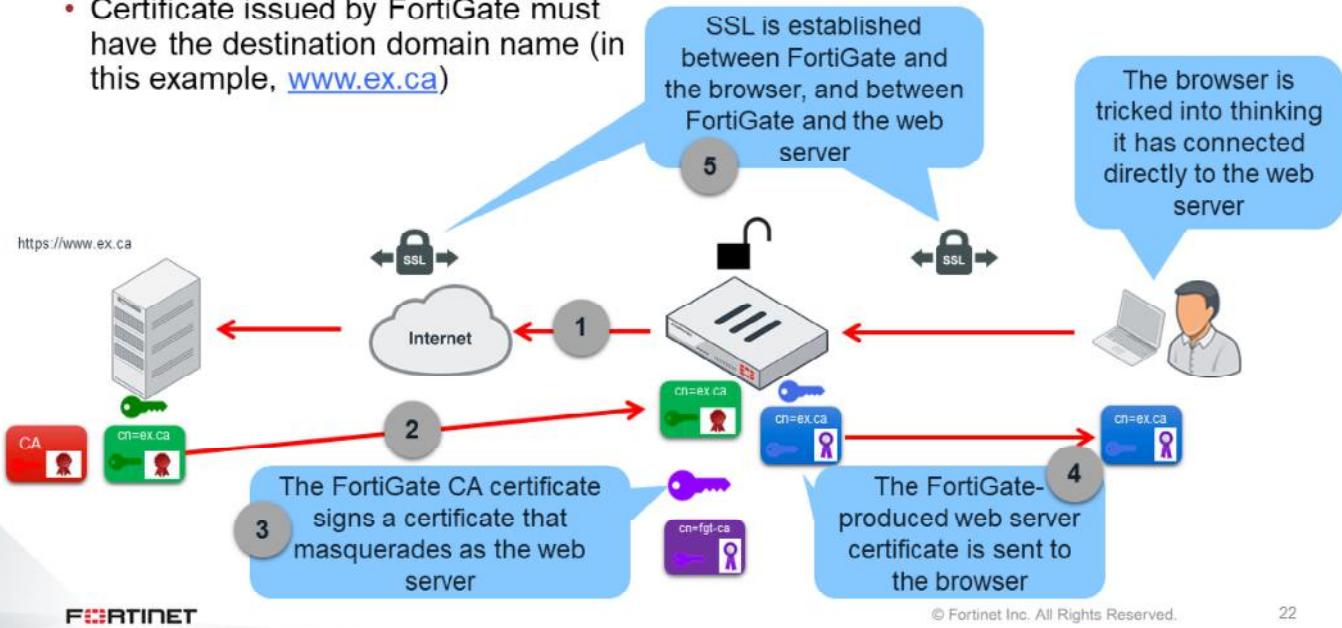
If the connection request is outbound (initiated by an internal client to an external server), you must select the option, **Multiple Clients Connecting to Multiple Servers**. Then, you must select the CA certificate that will be used to sign the new certificates. In this example, it is the built-in **FortiGate_CA_SSL** certificate, which is available on FortiGate devices that support SSL inspection. You will also learn about configuring full SSL inspection for inbound traffic, in this lesson.

DO NOT REPRINT

© FORTINET

Full SSL Inspection on Outbound Traffic—Part 2

- Certificate issued by FortiGate must have the destination domain name (in this example, www.ex.ca)



© Fortinet Inc. All Rights Reserved.

22

In step 1, an internal web browser connects to an SSL-enabled web server. Normally, when a browser connects to a secure site, the web server sends its certificate to the browser. However, in step 2, FortiGate intercepts the web server certificate. In step 3, FortiGate's internal CA generates a new key pair and certificate. The new certificate's subject name must be the DNS name of the website (for example, `ex.ca`). In steps 4 and 5, the new key pair and certificate are used to establish a secure connection between FortiGate and the web browser. A new temporary key pair and certificate are generated each time a client requests a connection with an external SSL server.

Outward facing and included in step 5, FortiGate uses the web server's certificate to initiate a secure session with the web server. In this configuration, FortiGate can decrypt the data from both the web server and the browser, in order to scan the data for threats before re-encrypting it, and sending it to its destination. This scenario is, essentially, an MITM attack.

DO NOT REPRINT**© FORTINET**

Untrusted SSL Certificates Setting

- Allow, block, or ignore untrusted certificates (only available if **Multiple Clients Connecting to Multiple Servers** is selected)
 - Allow:** Sends the browser an untrusted temporary certificate when the server certificate is untrusted
 - Block:** Blocks the connection when an untrusted server certificate is detected
 - Ignore:** Uses a trusted FortiGate certificate to replace the server certificate always, even when the server certificate is untrusted

SSL Inspection Options		
Enable SSL inspection of	Multiple Clients Connecting to Multiple Servers	
Inspection method	Protecting SSL Server	
CA certificate	SSL Certificate Inspection Full SSL Inspection	
Blacklisted certificates	Fortinet_CA_SSL Download View Blacklisted Certificates	
Untrusted SSL certificates	Allow	Block
Enforce SSL cipher compliance	Ignore	
Enforce SSL negotiation compliance	Ignore	
RPC over HTTPS	Ignore	

FORTINET

© Fortinet Inc. All Rights Reserved.

23

The browser presents a certificate warning when you attempt to access an HTTPS site that uses an untrusted certificate. Untrusted certificates include self-signed SSL certificates, unless the certificate is imported into the browser's trusted certificate store. FortiGate has its own configuration setting on the **SSL/SSH Inspection** page, which includes options to **Allow**, **Block**, or **Ignore** untrusted SSL certificates.

When the **Untrusted SSL certificates** setting is set to **Allow** and FortiGate detects an untrusted SSL certificate, FortiGate generates a temporary certificate signed by the built-in Fortinet_CA_Untrusted certificate. FortiGate then sends the temporary certificate to the browser, which presents a warning to the user indicating that the site is untrusted. If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser will complete the SSL handshake. Otherwise, the browser will also present a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser. The Fortinet_CA_Untrusted cert must not be imported.

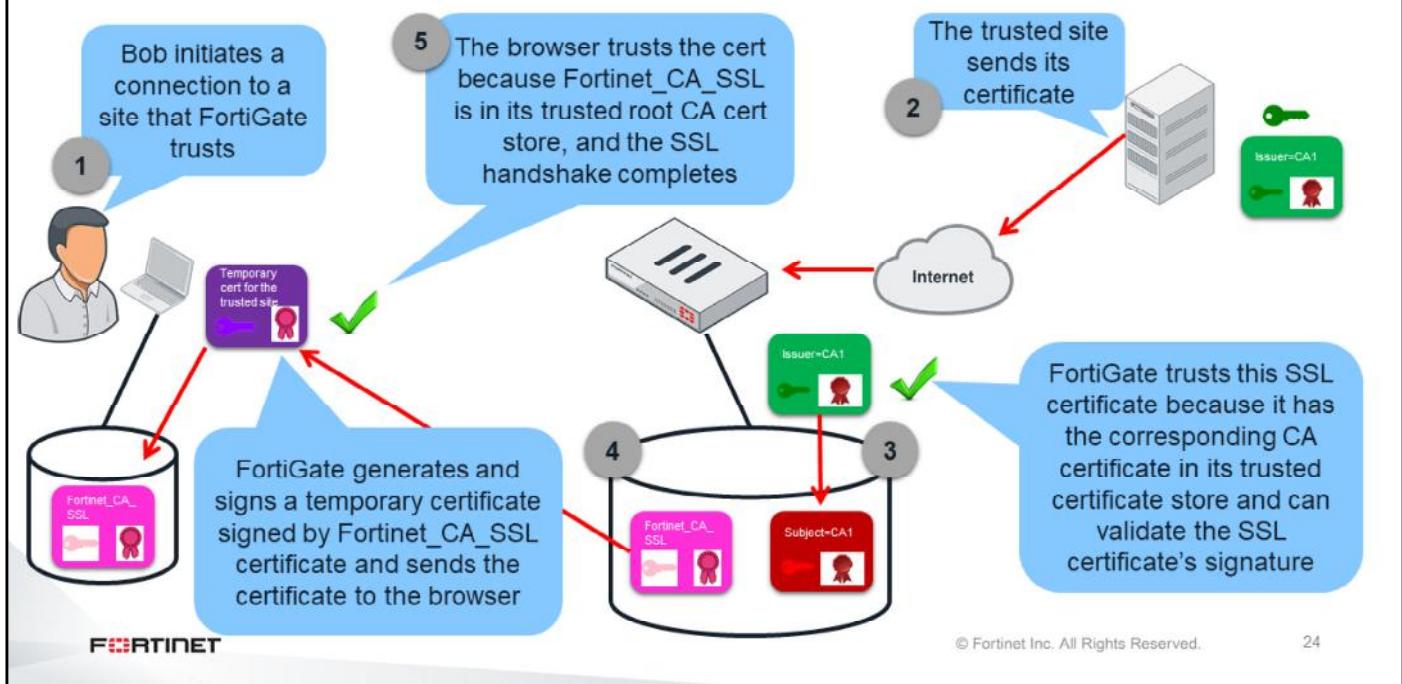
When the setting is set to **Block** and FortiGate receives an untrusted SSL certificate, FortiGate blocks the connection outright, and the user cannot proceed.

When the setting is set to **Ignore**, FortiGate sends the browser a temporary certificate signed by the Fortinet_CA_SSL certificate, regardless of the SSL certificate's status—trusted or untrusted. FortiGate then proceeds to establish SSL sessions.

DO NOT REPRINT

© FORTINET

Untrusted SSL Certificates—Trusted Site



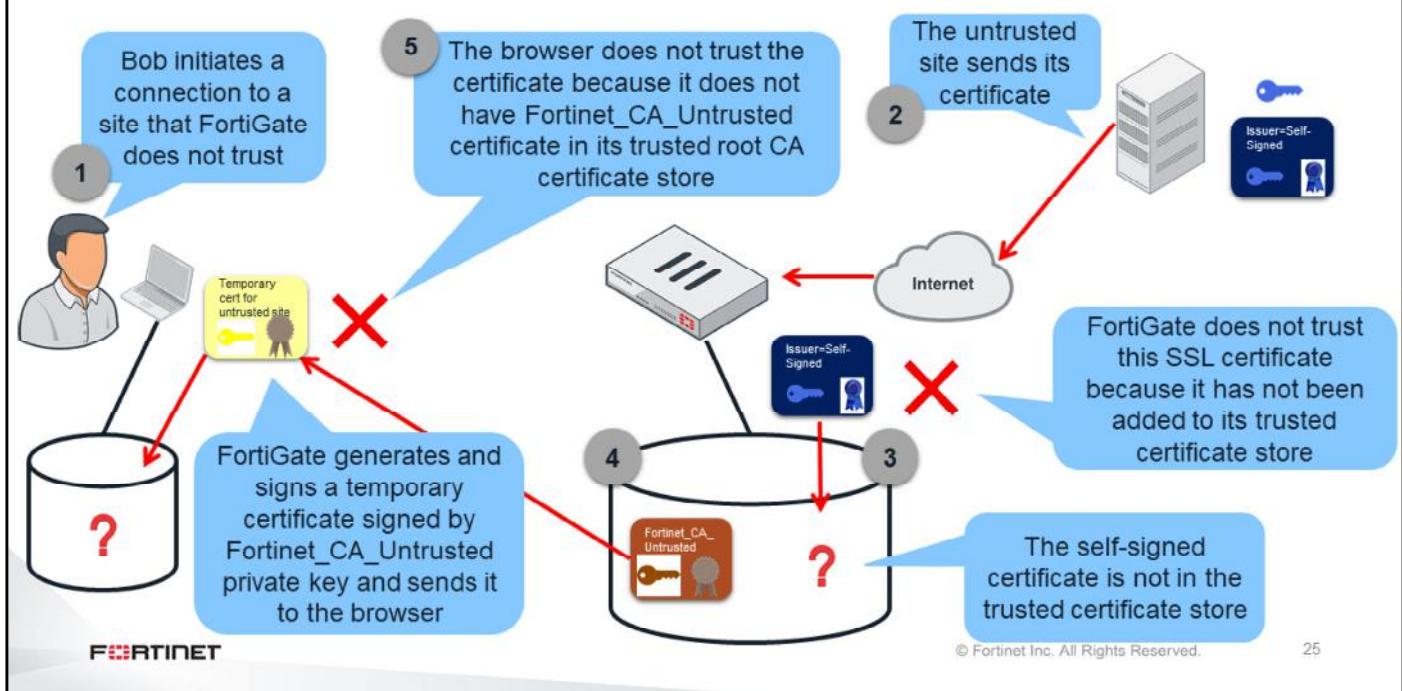
The scenario shown on this slide describes how FortiGate handles a trusted external site regardless of **Untrusted SSL Certificate** setting.

In step 1, the browser initiates a connection with an external site that is trusted by FortiGate. In step 2, the trusted server sends its SSL certificate to FortiGate. In step 3, FortiGate trusts the certificate because it has the corresponding CA certificate in its trusted certificate store. FortiGate can validate the signature on the SSL certificate. In step 4, because FortiGate trusts the SSL certificate, it generates a temporary certificate signed by Fortinet_CA_SSL certificate. FortiGate sends the temporary certificate to the browser. Finally, in step 5, the browser trusts the temporary certificate because Fortinet_CA_SSL certificate is in its trusted root CA store. After the browser finishes validating the certificate, it completes the SSL handshake with FortiGate. Next, FortiGate continues the SSL handshake with the trusted server.

DO NOT REPRINT

© FORTINET

Untrusted SSL Certificates—Allow, Untrusted Site



The scenario shown on this slide describes how FortiGate handles an untrusted external site when **Untrusted SSL Certificate** is set to **Allow**.

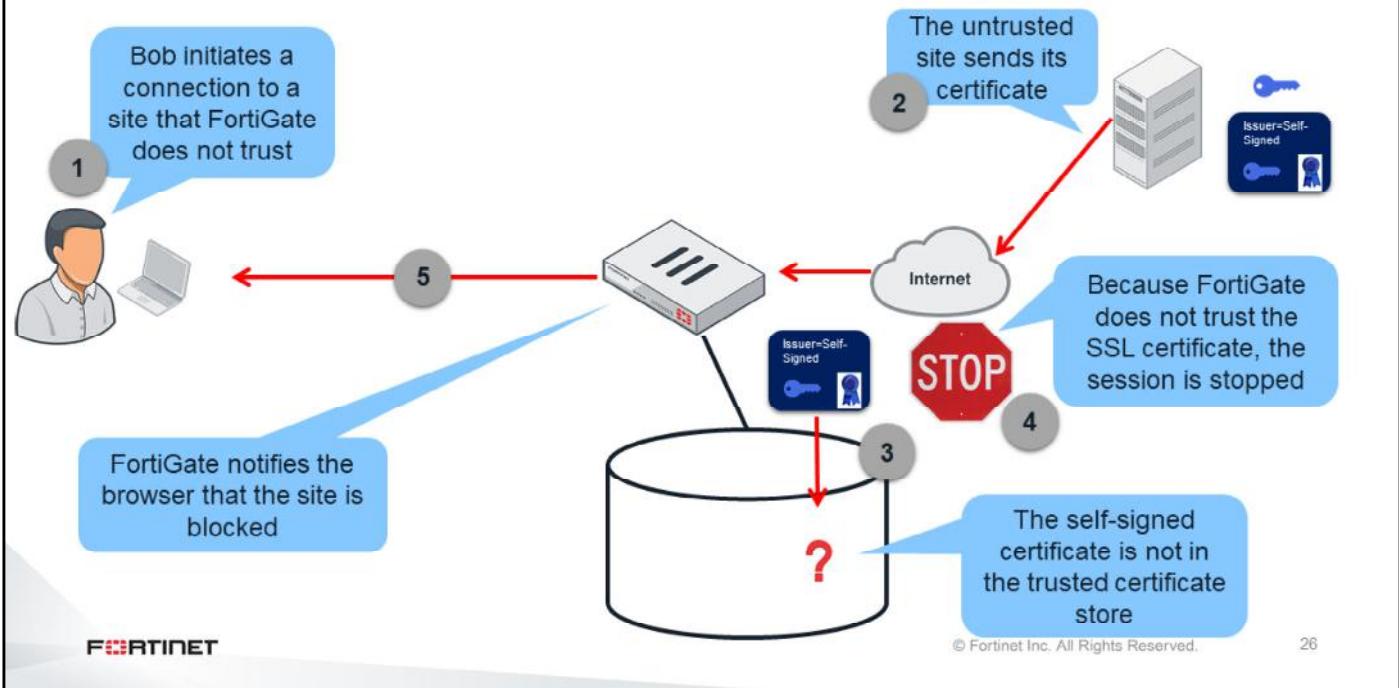
In step 1, the browser initiates a connection with an external site that is *not* trusted by FortiGate. In step 2, the untrusted server sends its self-signed SSL certificate to FortiGate. In step 3, FortiGate does not find a copy of the certificate in its trusted certificate store and, therefore, does not trust the SSL certificate. In step 4, because FortiGate does not trust the SSL certificate, it generates a temporary certificate signed by Fortinet_CA_Untrusted certificate. This temporary certificate is sent to the browser. In step 5, the browser does not trust the temporary certificate because it does not have the Fortinet_CA_Untrusted certificate in its trusted root CA store. The browser displays a warning alerting the user that the certificate is untrusted. If the user decides to ignore the warning and proceed, the browser completes the SSL handshake with FortiGate. Next, FortiGate continues the SSL handshake with the untrusted server.

The user may have the option to write this temporary certificate to the browser's trusted certificate store. However, this will have no impact going forward. The next time the user connects to the same untrusted site, a new temporary certificate will be produced for the session.

DO NOT REPRINT

© FORTINET

Untrusted SSL Certificates—Blocked, Untrusted Site



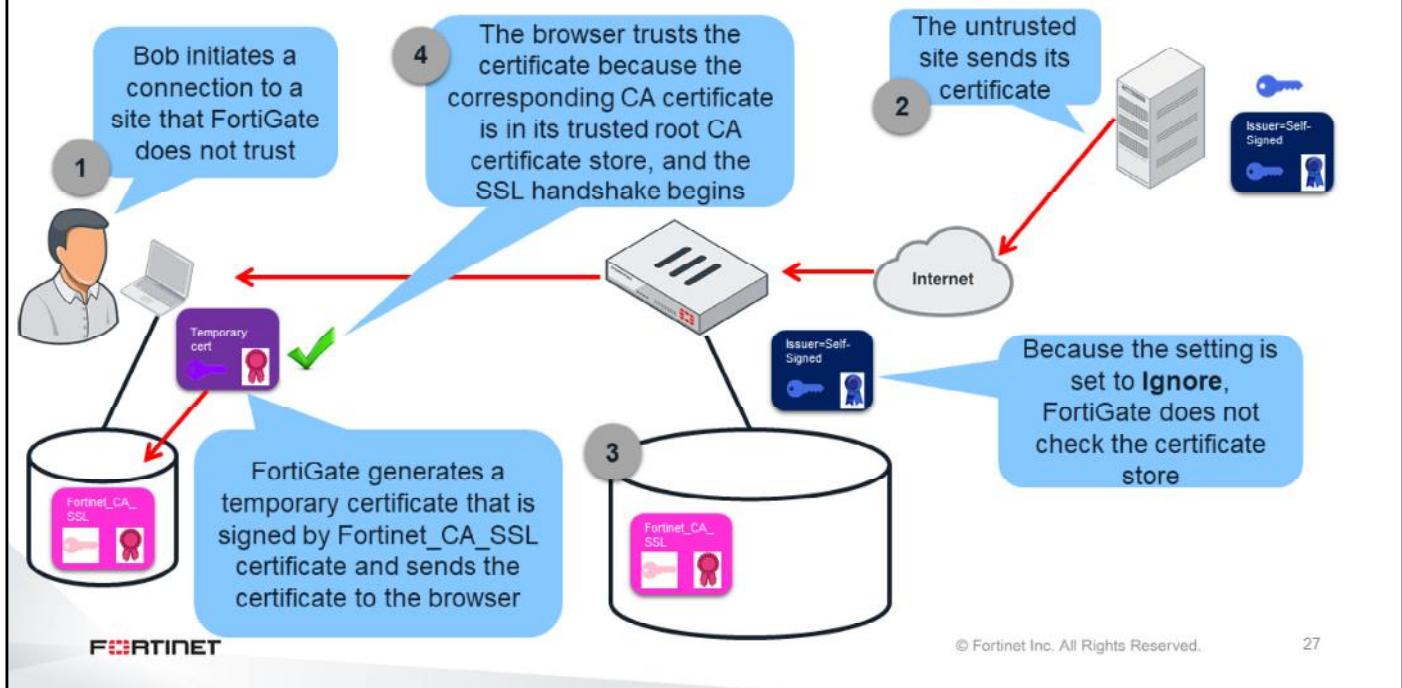
The scenario shown on this slide describes how FortiGate handles an untrusted external site when **Untrusted SSL Certificate** is set to **Block**.

In step 1, the browser initiates a connection with an external site that is *not* trusted by FortiGate. In step 2, the untrusted server sends its self-signed SSL certificate to FortiGate. In step 3, FortiGate does not find the certificate in its trusted certificate store and, therefore, does not trust the SSL certificate. In step 4, because FortiGate does not trust the SSL certificate, it stops the session. In step 5, FortiGate notifies the browser that the site is blocked.

DO NOT REPRINT

© FORTINET

Untrusted SSL Certificates—Ignore, Untrusted Site



The scenario shown on this slide describes how FortiGate handles an untrusted external site when **Untrusted SSL Certificate** is set to **Ignore**.

In step 1, the browser initiates a connection with an external site that is *not* trusted by FortiGate. In step 2, the untrusted server sends its self-signed SSL certificate to FortiGate. Because the setting is set to **Ignore**, FortiGate does not check the certificate store. In step 3, FortiGate generates a temporary certificate signed by Fortinet_CA_SSL certificate, and sends the certificate to the browser. In step 4, the browser trusts the certificate because Fortinet_CA_SSL certificate is in its trusted root CA store. Once the browser finishes checking the certificate, it completes the SSL handshake with FortiGate. Next, FortiGate continues the SSL handshake with the trusted server.

A connection to a trusted site is handled the same way.

DO NOT REPRINT**© FORTINET**

Exempting Sites From SSL Inspection

- Why exempt?
 - Problems with traffic
 - Legal issues
 - Check local laws

White list exemption as rated by
FortiGuard web filtering

The screenshot shows the 'Security Profiles > SSL/SSH Inspection' configuration. It includes sections for 'Exempt from SSL Inspection' (with a toggle switch), 'Reputable websites' (also with a toggle switch), 'Web categories', and 'Addresses'. Under 'Web categories', there is a list of exempted categories: 'Finance and Banking' and 'Health and Wellness'. Under 'Addresses', there is a list of exempted domain names: gmail.com, login.microsoft.com, login.microsoftonline.com, login.windows.net, wildcard.dropbox.com, and wildcard.google.com.

Category	Address / Category	Action
Web categories	Finance and Banking	X
	Health and Wellness	X
	+ (Add)	
	gmail.com	X
	login.microsoft.com	X
	login.microsoftonline.com	X
Addresses	login.windows.net	X
	wildcard.dropbox.com	X
	wildcard.google.com	X
	+ (Add)	

You can exempt sites by web category or address

FORTINET

© Fortinet Inc. All Rights Reserved.

28

Within the full SSL inspection profile, you can also specify which SSL sites, if any, you want to exempt from SSL inspection. You may need to exempt traffic from SSL inspection if it is causing problems with traffic or for legal reasons.

Performing SSL inspection on a site that is enabled with HTTP public key pinning (HPKP), for example, can cause problems with traffic. Remember, the only way for FortiGate to inspect encrypted traffic is to intercept the certificate coming from the server, and generate a temporary one. Once FortiGate presents the temporary SSL certificate, browsers that use HPKP will refuse to proceed. The SSL inspection profile, therefore, allows you to exempt specific traffic.

Laws protecting privacy may be another reason to bypass SSL inspection. For example, in some countries, it is illegal to inspect SSL bank-related traffic. Configuring an exemption for sites is simpler than setting up firewall policies for each individual bank. You can exempt sites based on their web category, such as finance or banking, or you can exempt them based on their address. Alternatively, you can enable **Reputable websites**, which excludes a white list of reputable domain names maintained by FortiGuard from full SSL inspection. This list is periodically updated and downloaded to FortiGate devices through FortiGuard.

DO NOT REPRINT**© FORTINET**

Invalid Certificates

- FortiGate can detect invalid certificates for a variety of reasons
 - Invalid certificates produce security warnings due to problems with the certificate details
- FortiGate can **Allow**, **Block**, or **Ignore** invalid certificates
 - ignore can be enabled only on the CLI when full SSL inspection is enabled
- Selecting **Custom** allows the user to select the action for each reason

Security Profiles > SSL/SSH Inspection

Common Options

Invalid SSL certificates	<input type="button" value="Allow"/>	<input type="button" value="Block"/>	<input checked="" type="button" value="Custom"/>
Expired certificates	<input type="button" value="Allow"/>	<input checked="" type="button" value="Block"/>	
Revoked certificates	<input type="button" value="Allow"/>	<input checked="" type="button" value="Block"/>	
Validation timed-out certificates	<input checked="" type="button" value="Allow"/>	<input type="button" value="Block"/>	
Validation failed certificates	<input type="button" value="Allow"/>	<input checked="" type="button" value="Block"/>	
Log SSL anomalies 	<input checked="" type="checkbox"/>		

```
config firewall ssl-ssh-profile
  edit "Custom-SSL-Inspection"
    config https
      set ports 443
      set status deep inspect
      set expired-server-cert ignore
      set revoked-server-cert ignore
      set cert-validation-timeout ignore
      set cert-validation-failure ignore
    end
  next
end
```

© Fortinet Inc. All Rights Reserved.

29

FORTINET

FortiGate can detect certificates that are invalid for the following reasons:

- Expired: The certificate is expired.
- Revoked: The certificate has been revoked based on CRL or OCSP information.
- Validation timeout: The certificate could not be validated because of a communication timeout.
- Validation failed: The certificate could not be validated because of a communication error.

When a certificate fails for any of the reasons above, you can configure any of the following actions:

- Allow: FortiGate allows the website and lets the browser decide the action to take. FortiGate takes the certificate as *trusted*.
- Block: FortiGate blocks the content of the site.
- Ignore: FortiGate allows the website and takes the certificate as *trusted*. This action is available only on the CLI if full SSL inspection has been enabled.

The certificate check feature can be broken down into two major checks, which are done in parallel:

- FortiGate checks if the certificate is invalid because of the four reasons described on this slide.
- FortiGate performs certificate chain validation based on the CA certificates installed locally and the certificates presented by the SSL server. This is described in this lesson.

Based on the actions configured and the check results, FortiGate will present the certificate as either trusted (signed by Fortinet_CA_SSL) or untrusted (signed by Fortinet_CA_Untrusted), and will either allow the content or block it. You can also track certificate anomalies by enabling the **Log SSL anomalies** option.

DO NOT REPRINT

© FORTINET

Configuring Full SSH Inspection

The screenshot shows the 'SSL/SSH Inspection' configuration page. In the 'SSL Inspection Options' section, under 'Enable SSL inspection of', the option 'Multiple Clients Connecting to Multiple Servers' is selected. In the 'SSH Inspection Options' section, the 'SSH deep scan' checkbox is checked. The 'SSH port' field is set to 'Any'.

You can enable **SSH deep scan** when you select **Multiple Clients Connecting to Multiple Servers**. When you enable **SSH deep scan**, FortiGate does a MITM attack for SSH traffic. A process similar to the one done for full SSL inspection takes place. FortiGate intercepts the SSH key sent by the server, generates a new one, and sends it to the client. If the SSH client had stored the original host key, then it will see a change in the host key and warn the user. The user can then replace the original host key with the new host key generated by FortiGate.

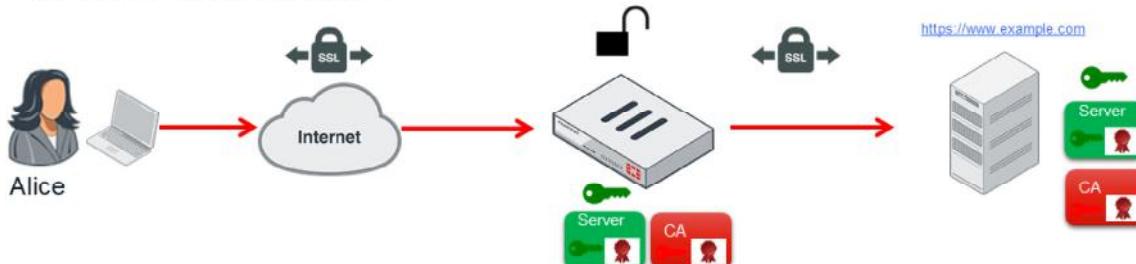
By default, **SSH deep scan** listens on TCP port 22. You can specify a different port number or select **Any** in the **SSH port** field. When you do this, FortiGate scans all connections to identify SSH traffic using different ports. Specifying a port for SSH traffic is not as comprehensive as searching all ports, but it is easier on the performance of the firewall.

Finally, note that **SSH deep scan** is a proxy-based inspection feature only. In addition, the only security features that use **SSH deep scan** are antivirus and data leak prevention.

DO NOT REPRINT**© FORTINET**

Full SSL Inspection on Inbound Traffic

- A user from the internet attempts to connect to a protected server
- The SSL connection is split into two, both terminating at FortiGate
 - FortiGate proxies the SSL traffic
 - The server's signed certificate, private key, and chain of certificates must be installed in FortiGate
 - FortiGate presents the signed certificate to the user on behalf of the server



Security Profiles > SSL/SSH Inspection

SSL Inspection Options	
Enable SSL inspection of <input checked="" type="checkbox"/> Multiple Clients Connecting to Multiple Servers <input checked="" type="checkbox"/> Protecting SSL Server	
Server certificate	<input checked="" type="checkbox"/> Cert. Webserver <input type="button" value="Download"/>
Protocol Port Mapping	
Inspect all ports <input type="checkbox"/>	
HTTPS	<input checked="" type="checkbox"/> 443

© Fortinet Inc. All Rights Reserved.

31

In this example, FortiGate is protecting a web server. This is the second configuration option for full SSL inspection. When configuring the SSL inspection profile for this server, you must select **Protecting SSL Server**, import the server's key pair to FortiGate, and then select the certificate from the **Server Certificate** drop-down list. If you have multiple servers to protect, you will need to add an SSL inspection profile for each server, unless the servers share the same certificate.

When Alice attempts to connect to the protected server, FortiGate becomes a surrogate web server by establishing the secure connection with the client using the server's key pair. FortiGate also establishes a secure connection with the server, but acting as a client. This configuration allows FortiGate to decrypt the data from either direction, scan it, and if it is clean, re-encrypt it and send it to the intended recipient.

You will need to install the server's certificate and private key plus the chain of certificates required to build the chain of trust. FortiGate sends the chain of certificates to the browser for this purpose.

DO NOT REPRINT

© FORTINET

Applying an SSL Inspection Profile to a Firewall Policy

- You must assign an SSL inspection profile to a firewall policy so FortiGate knows how to treat encrypted traffic
 - Select the **no-inspection** profile if you don't want to perform any SSL or SSH inspection—FortiGate will not scan SSL and SSH traffic through that firewall policy

Select the SSL inspection profile

Enable to mirror decrypted SSL traffic to an interface

Policy & Objects > IPv4 Policy

Profile Type	Profile Name
SSL	deep-inspection
SSL	certificate-inspection
SSL	custom-deep-inspection
SSL	deep-inspection
SSL	my-ssl-inspection-profile
SSL	no-inspection

© Fortinet Inc. All Rights Reserved.

32

After you create and configure an SSL inspection profile, you must assign it to a firewall policy so FortiGate knows how to inspect encrypted traffic. Most of the internet traffic is being encrypted nowadays. For this reason, you normally want to enable SSL inspection to protect your network from security threats transported over encrypted traffic. If you don't want to enable SSL or SSH inspection, select the **no-inspection** profile from the drop-down list. If SSL inspection is not enabled in a policy, FortiGate will not scan SSL or SSH encrypted traffic matching that policy.

If you select a profile with full SSL inspection enabled, the option **Decrypted Traffic Mirror** appears. Enable this option if you want FortiGate to send a copy of the decrypted SSL traffic to an interface. When you enable **Decrypted Traffic Mirror**, FortiGate displays a window with the terms of use for this feature. The user must agree with the terms before the feature can be used.

DO NOT REPRINT**© FORTINET**

Certificate Warnings

- The browser may display a certificate warning during SSL inspection because it does not trust the CA
- To avoid certificate warnings, do one of the following:
 - Use the Fortinet_CA_SSL certificate and install the FortiGate CA root certificate in all the browsers
 - Use an SSL certificate issued by a CA and ensure that the root CA certificate is installed in all the browsers



© Fortinet Inc. All Rights Reserved.

33

When doing full SSL inspection using the FortiGate self-signed CA, your browser displays a certificate warning each time you connect to an HTTPS site. This is because the browser is receiving certificates signed by FortiGate, which is a CA it does not know and trust. The browser also displays a certificate warning when performing SSL certificate inspection and an HTTPS website is blocked by FortiGate. Because FortiGate needs to present a replacement message to the browser, FortiGate performs MITM and signs the certificate with its self-signed CA as well.

You can avoid this warning by doing one of the following:

- Download the Fortinet_CA_SSL certificate and install it on all the workstations as a trusted root authority.
- Use an SSL certificate issued by a CA and ensure the certificate is installed in the necessary browsers.

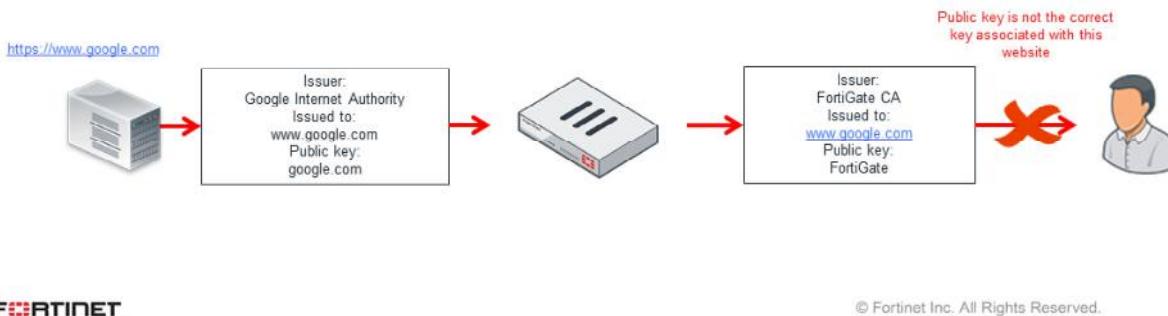
The SSL certificate must be installed on FortiGate and the device configured to use that certificate for SSL inspection. If the SSL certificate is signed by a subordinate CA, ensure that the entire chain of certificates—from the SSL certificate to the root CA certificate—is installed on FortiGate. Verify that the root CA is installed on all client browsers. This is required for trust purposes. Because FortiGate sends the chain of certificates to the browser during the SSL handshake, the intermediate CA certificates do not have to be installed on the browsers.

DO NOT REPRINT

© FORTINET

Full SSL Inspection and HSTS/HPKP

- Some web servers implement security measures to mitigate MITM attacks
 - HTTP strict transport security (HSTS)
 - A mechanism whereby websites are accessible only through secure connections—RFC 6797 (IETF)
 - HTTP public key pinning (HPKP)
 - Associates or pins a public key to a specific web server
 - For example, some browsers require a Google certificate when accessing any Google site
 - HPKP and HSTS are intended to work together



FORTINET

© Fortinet Inc. All Rights Reserved.

34

Some security measures have been introduced by the IETF to mitigate the MITM attack. Some of these measures cause problems when outbound full SSL inspection is implemented.

HTTP strict transport security (HSTS) and HTTP public key pinning (HPKP) are security features designed to thwart MITM attacks. HSTS is “a mechanism enabling websites to declare themselves accessible only through secure connections …”, according to RFC 6797 of the IETF. In other words, a user from a web browser would be forced to use HTTPS when connecting to a website with this policy; there would be no option to connect using HTTP. HPKP is a security feature imposed by the web server that associates one or more public keys with the website for a specified period of time. The public key doesn’t have to be the web server’s public key, it could be one of the intermediate or root CA public keys, as long as it exists in the certificate chain. When the web browser visits an HPKP-enabled website, hashes of the public keys associated with a website are cached on the client machine.

Going forward, each time the web browser connects to the web server, it will compare one or more of the keys presented with the cached key fingerprints. If the browser cannot match at least one of the keys, the SSL handshake terminates. This is a problem for outbound full SSL inspection. FortiGate generates a new certificate and public key to establish an SSL session with the web browser. FortiGate cannot provide an authentic certificate chain, so the connection would be rejected by the browser. Predictably, this could prevent users from connecting to a lot of legitimate sites.

DO NOT REPRINT**© FORTINET**

Resolving HPKP Issues

- Exempt those websites from full SSL inspection
- Use SSL certificate inspection instead
- Use a web browser that does not support HPKP, like Chrome, Internet Explorer or Edge
- Disable the security setting in the browser (not always an option)



© Fortinet Inc. All Rights Reserved.

35

The options available to circumvent HPKP are limited. One option is to exempt SSL inspection for those sites. Another option is to use SSL certificate inspection instead. A third option is to use a browser that does not support HPKP, like Chrome, Internet Explorer, or Edge. Last, in some browsers it is possible to disable HPKP.

DO NOT REPRINT

© FORTINET

Applications and SSL Inspection

- Any SSL application may be impacted by SSL inspection (not just the browser)
 - The solution depends on the application security design
 - Consider other SSL-based protocols such as FTPS, SMTPS, and STARTTLS (not just HTTPS)
- Microsoft Outlook 365 for Windows error after enabling full SSL inspection:



Solution: import the CA certificate into the Windows certificate store (FortiGate keeps inspecting SSL traffic)

- Dropbox for Windows error after enabling full SSL inspection:



Solution: exempt Dropbox domains from SSL inspection (FortiGate no longer inspects SSL traffic)

FORTINET

© Fortinet Inc. All Rights Reserved.

36

More and more applications are using SSL to securely exchange data over the internet. While most of the content in this lesson centers around the operation and impact of SSL inspection on browsers, the same applies to other applications using SSL as well. After all, the browser is just another application using SSL on your device.

For this reason, when you enable SSL inspection on FortiGate, you need to consider the potential impact on your SSL-based applications. For example, Microsoft Outlook 365 for Windows will report a certificate error when you enable full SSL inspection because the CA certificate used by FortiGate is not trusted. To solve this issue, you can import the CA certificate into your Windows certificate store as a trusted root certification authority. Because Microsoft Outlook 365 trusts the certificates in the Windows certificate store, then the application won't report the certificate error anymore. Another option is to exempt your Microsoft Exchange server addresses from SSL inspection. While this prevents the certificate error, you are no longer performing SSL inspection on email traffic.

There are other applications that have built-in extra security checks that prevent MITM attacks, such as HPKP or certificate pinning. For example, Dropbox uses certificate pinning to ensure that no SSL inspection is possible on user traffic. As a result, when you enable full SSL inspection on FortiGate, your Dropbox client will stop working and report that it can't establish a secure connection. In the case of Dropbox, the only way to solve the connection error is by exempting the domains Dropbox connects to from SSL inspection.

In addition, remember that SSL is leveraged by different protocols, not just HTTP. For example, there are other SSL-based protocols such as FTPS, POP3S, SMTPS, STARTTLS, LDAPS, and SIP TLS. If you have an application using any of these SSL-based protocols, and you have turned on SSL inspection along with a security profile that inspects those protocols, then the applications may report an SSL or certificate error. The solution will depend on the security measures adopted by the application.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which certificate extension and value is required in the FortiGate CA certificate in order to enable full SSL inspection?
 - A. CRL DP=ca_arl.arl
 - B. cA=True

2. Which configuration requires FortiGate to act as a CA for full SSL inspection?
 - A. Multiple clients connecting to multiple servers
 - B. Protecting the SSL server



DO NOT REPRINT**© FORTINET**

Lesson Progress



Authenticate and Secure Data Using Certificates



Inspect Encrypted Data



Manage Digital Certificates on FortiGate

Good job! You now can describe certificate and deep inspection, and you can configure FortiGate to use any one of these options.

Now, you will learn how to manage digital certificates on FortiGate.

DO NOT REPRINT

© FORTINET

Manage Digital Certificates on FortiGate

Objectives

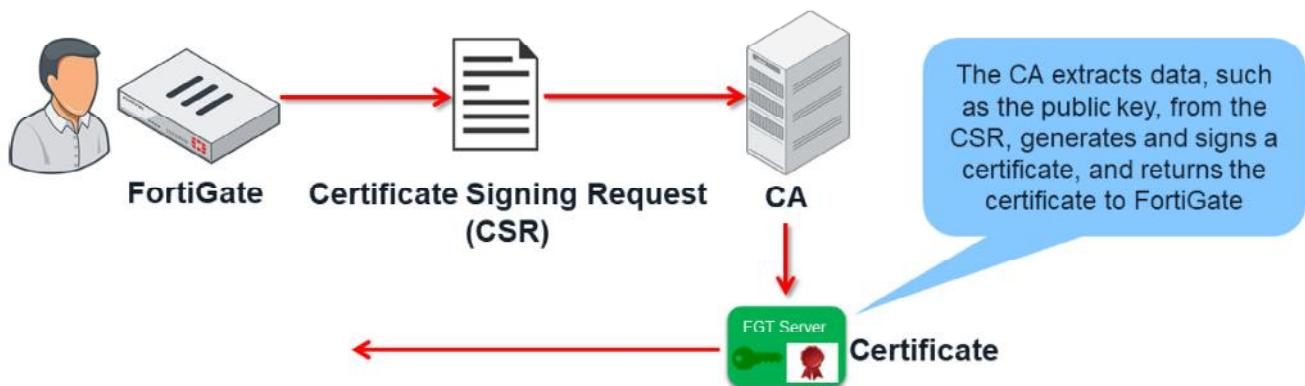
- Generate a certificate request
- Import CRLs
- Back up and restore certificates

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

By demonstrating competence in generating certificate requests, importing CRLs, and backing up and restoring certificates, you will be able to manage certificates in FortiGate.

DO NOT REPRINT**© FORTINET**

Generating a CSR for a CA



- A certificate signing request (CSR) that includes the public key and is signed by the private key is submitted to a CA
 - File is usually a *.CSR (certificate signing request)
 - User information and key data is verified
 - Data is published in industry-standard format and the digital signature of the CA is applied
 - The signature guarantees the integrity of the data and that the data has been verified by a trusted authority

FORTINET

© Fortinet Inc. All Rights Reserved.

40

The process of obtaining a digital certificate for FortiGate begins with creating a certificate signing request (CSR). The process is as follows:

1. FortiGate generates a CSR. A private and public key pair is created for FortiGate. The CSR is signed by FortiGate's private key.
2. FortiGate submits the CSR to a CA. The CSR includes the FortiGate public key and specific information about FortiGate (IP address, distinguished name, email address, and so on). Note that the private key remains confidential on FortiGate.
3. The CA verifies that the information in the CSR is valid, and then creates a digital certificate for FortiGate. The certificate is digitally signed using the CA's private key. The CA also publishes the certificate to a central repository. The certificate binds the public key to FortiGate.
4. The certificate is returned to install on FortiGate.

DO NOT REPRINT**© FORTINET**

Generating a CSR

The screenshot shows the FortiGate Management Interface. On the left, under 'System > Certificates', there is a list of certificates. A red box highlights the 'Generate' button. An arrow points from this button to a larger 'Generate Certificate Signing Request' dialog box on the right.

Certificates List:

Name	Subject	Comments
Local CA Certificate (2)		
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA cert
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA cert
Local Certificate (18)		
Cert_Webserver	ST = Alberta, L = Edmonton, O = Office, OU = Lab, CN ...	
Cluster4_SSL_Inspect	ST = Alberta, L = Edmonton, O = Home, OU = Lab, CN ...	
Cluster4_SSL_Inspection	C = CA, ST = Alberta, L = Edmonton, O = Office, OU = L...	
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embed

Generate Certificate Signing Request Dialog:

- Certificate Name:** [Input field]
- Subject Information:**
 - ID Type:** Host IP (selected), Domain Name, E-Mail
 - IP:** 0.0.0.0
- Optional Information:**
 - Organization Unit:** [Input field]
 - Organization:** [Input field]
 - Locality(City):** [Input field]
 - State / Province:** [Input field]
 - Country / Region:** [Input field]
 - E-Mail:** [Input field]
 - Subject Alternative Name:** [Input field]
 - Password for private key:** [Input field]
- Key Type:** RSA (selected), Elliptic Curve
- Key Size:** 1024 Bit, 1536 Bit, 2048 Bit (selected), 4096 Bit
- Enrollment Method:** File Based (selected), Online SCEP

FORTINET

© Fortinet Inc. All Rights Reserved.

41

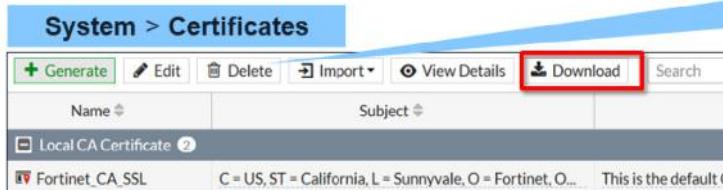
You can generate a CSR on the **Certificates** page of the GUI by clicking **Generate**. Enter all of the required information, such as the IP address (or FQDN) and company name. Ensure the key type and size fit your requirements. You can submit the CSR to a CA using either of the following methods:

- Select **File Based** to generate the CSR as a .csr file, which is then sent to the CA.
- Select **Online SCEP** to submit the CSR to the CA online using the Simple Certificate Enrollment Protocol (SCEP). For example, if you are using FortiAuthenticator as your CA, you can enable and configure SCEP on FortiAuthenticator and use this method.

DO NOT REPRINT**© FORTINET**

CSR Enrollment Types

- File-based method
 - Select CSR and click **Download**
 - Submit file to CA



Note that if you delete the CSR, you will not be able to import the signed certificate and you will have to start over

- Online SCEP method
 - Enter the CA server URL used for SCEP and the challenge password provided by the CA administrator
 - A CSR is automatically submitted online



FORTINET

© Fortinet Inc. All Rights Reserved.

42

If you are using the file-based method, the CSR is added to your list of certificates on the **Certificates** page. Select the CSR and click **Download**. The administrator can now submit the file (.csr), which is a PKCS#10 request, to the CA. PKCS#10 is the most common format for a certificate request. The CA uses this file to generate a signed certificate.

If using the online SCEP method, enter the CA server URL used for SCEP and the challenge password provided by the CA administrator. The CSR is automatically submitted online.

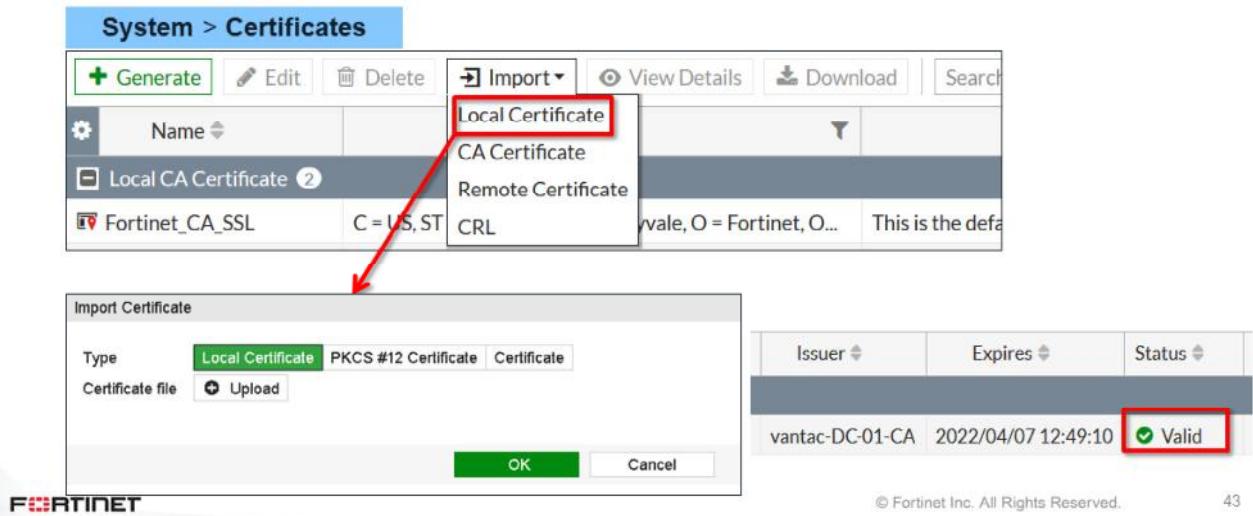
After the CSR is submitted using either method, FortiGate shows the certificate status as **Pending** until the certificate is returned by the CA and imported into FortiGate. At this point, the status changes to **Valid** and the digital certificate can be used.

Note that if you delete the CSR, you will not be able to install the certificate and you will have to start over.

DO NOT REPRINT**© FORTINET**

Importing a Local Certificate

- To import a local certificate:
 - Click **Import > Local Certificate**
 - Browse for the CER file provided by CA



The file-based method of submitting a CSR is a manual process. The SCEP process, which occurs automatically online, requires no manual file import.

You can import the certificate from the **Certificates** page. Click **Import** and select **Local Certificate**. On the **Import Certificate** dialog, in the **Type** field, select **Local Certificate** and browse to the CER file provided by the CA.

Once you import the certificate, the status changes from **Pending** to **Valid**. Note that it is possible to add a certificate that FortiGate will use in SSL communications without generating and signing a CSR. The CA can create a certificate for your FortiGate without a CSR (though the CA is responsible for providing all the certificate details for your FortiGate). In this way, you can add a certificate using the following methods:

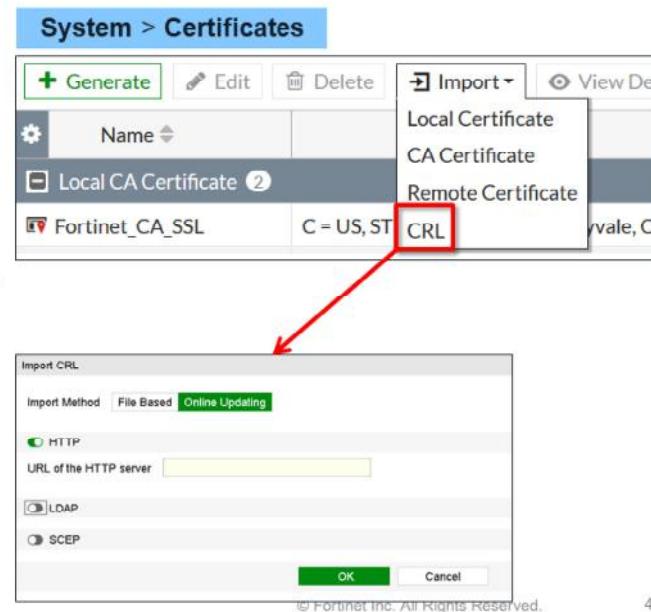
- Upload a PKCS#12 file, which is a single file that includes the signed certificate file and the key file
- Upload both a certificate file and the key file

An administrator user with the super_admin profile can put a password on a certificate and control access to its private key.

DO NOT REPRINT**© FORTINET**

Importing a CRL

- FortiGate administrators can manually import CRLs
- Upload options:
 - HTTP
 - LDAP
 - SCEP
 - Local PC
- FortiGate automatically updates CRLs before they expire



FORTINET

44

When FortiGate is validating a certificate, it checks that the certificate's serial number is not listed in a CRL imported to FortiGate.

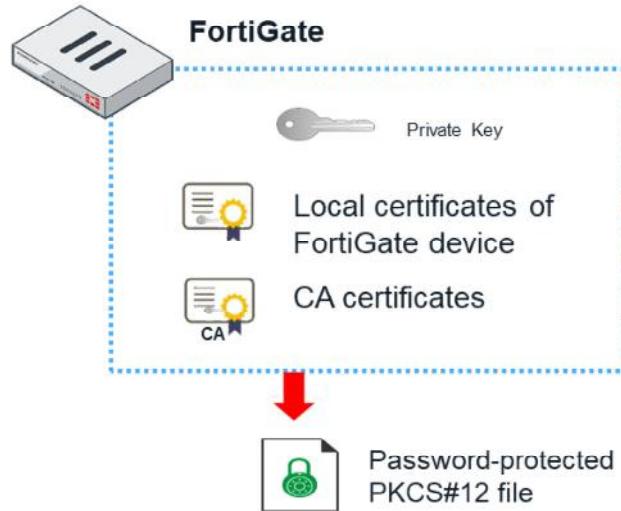
You can import a CRL from the **Certificates** page by clicking **Import > CRL**. In the **Import CRL** dialog, you can select one of these four import options: **HTTP**, **LDAP**, **SCEP**, and **Local PC**. The first three options point to external repositories and require you to connect to the repositories to upload the CRL to FortiGate. The last option, **Local PC**, requires you to have the CRL file locally stored before you can upload the CRL to FortiGate.

Before the CRL expires, FortiGate will automatically retrieve the latest iteration using the protocol specified in the configuration.

DO NOT REPRINT**© FORTINET**

Backing Up and Restoring Certificates

- Back up keys and certificates through the CLI (TFTP server required for import and export):
 - execute vpn certificate local import tftp <file-name_str> <tftp_ip>.
 - execute vpn certificate local export tftp <certificate-name_str> <file-name_str> <tftp_ip>.
- Keys and certificates are stored in the PKCS#12 file
- Configuration backup also contains the keys and certificates



FORTINET

© Fortinet Inc. All Rights Reserved.

45

When you back up the FortiGate configuration, the keys and certificates are backed up as well.

FortiGate also provides the option to store digital certificates as a PKCS#12 file, which includes the private and public keys as well as the certificate. You can restore the PKCS#12 file to a FortiGate device of any model or firmware version, or to a non-FortiGate device.

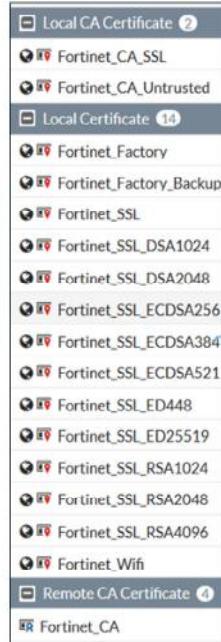
You can perform the backup and restore from the CLI only, which requires the use of a TFTP server.

DO NOT REPRINT**© FORTINET**

Certificate Configuration—VDOM and Global

- You can configure CA and local certificates per VDOM

```
config certificate local
edit Fortinet_Factory
set range <global/vdom>
set source <factory/user/bundle/fortiguard>
end
```



FortiGate certificates,
some identified with
specific signature
algorithms and key
lengths identified in
their names

FORTINET

© Fortinet Inc. All Rights Reserved.

46

You can configure a CA and local certificate globally or for a VDOM. If you upload a certificate to a VDOM, it is accessible only inside that VDOM. If you upload a certificate globally, it is accessible to all VDOMs and globally.

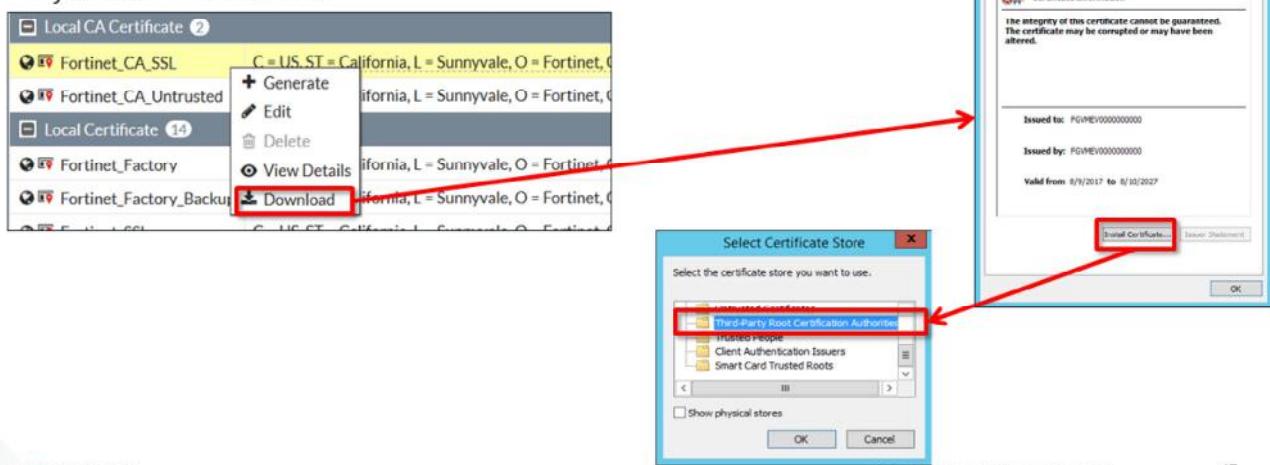
Global and VDOM-based certificate configuration includes the ability to view certificate details, as well as to download, delete, and import certificates.

Note that some of the FortiGate certificates have specific signature algorithms and key lengths in their names, such as Elliptic Curve Digital Signature Algorithm 256 (ECDSA256) and RSA2048. Policy and technical requirements may determine which certificates you use.

DO NOT REPRINT**© FORTINET**

Installing an SSL Certificate Issued by a Private CA

- Private CA certificates used by SSL should be installed on endpoints
 - Avoids certificate warnings
 - Strict SSL will fail with no override option if CA is untrusted
- System > Certificates



FORTINET

© Fortinet Inc. All Rights Reserved.

47

If you are using an SSL certificate issued by a private CA, you must install the CA certificate in the list of trusted CAs. If you fail to do this, a warning message will appear in your web browser any time you access an HTTPS website. Encrypted communications may also fail, simply because the CA that issued and signed the certificate is untrusted.

Once you download the SSL certificate from FortiGate, you can install it on any web browser or operating system. Not all browsers use the same certificate repository. For example, Firefox uses its own repository, while Internet Explorer and Chrome store certificates in a system-wide repository. In order to avoid certificate warnings, you need to install the SSL certificate as a trusted root CA.

When you install the certificate, make sure that it is saved to the certificate store for root authorities.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which CSR enrollment method is supported by FortiGate?
 - A. Enrollment over Secure Transport (EST)
 - B. Simple Certificate Enrollment Protocol (SCEP)

2. After a CSR has been enrolled and imported into FortiGate, the status of the certificate should change to:
 - A. Valid
 - B. Pending



© Fortinet Inc. All Rights Reserved.

48

DO NOT REPRINT**© FORTINET**

Lesson Progress



Authenticate and Secure Data Using Certificates



Inspect Encrypted Data



Manage Digital Certificates on FortiGate

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe why FortiGate uses digital certificates
- ✓ Describe how FortiGate uses certificates to authenticate users and devices
- ✓ Describe how FortiGate uses certificates to ensure the privacy of data
- ✓ Describe certificate inspection and full SSL inspection
- ✓ Configure certificate inspection and full SSL/SSH inspection
- ✓ Identify what is required to implement full SSL inspection
- ✓ Identify the obstacles to implementing full SSL inspection and possible remedies
- ✓ Generate a certificate request
- ✓ Import CRLs
- ✓ Back up and restore certificates

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

By mastering the objectives covered in this lesson, you have learned the basics of how FortiGate uses certificates, and how to manage and work with certificates in your network.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Web Filtering

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified: 29 May 2020

In this lesson, you will learn how to configure web filtering on FortiGate to control web traffic in your network.

DO NOT REPRINT

© FORTINET

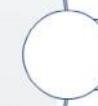
Lesson Overview



Inspection Modes



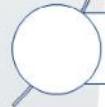
Web Filtering Basics



Additional Proxy-Based Web Filtering Features



DNS Filtering



Best Practices and Troubleshooting

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

DO NOT REPRINT

© FORTINET

Inspection Modes

Objectives

- Describe FortiGate inspection modes
- Review NGFW operation modes

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

By demonstrating competence in understanding inspection modes, you will be able to implement the appropriate inspection modes to support the desired security profiles.

DO NOT REPRINT**© FORTINET**

Inspection Modes

- Per firewall policy setting
- Two inspection modes:
 - Flow based
 - Default inspection mode is flow based (in policy)
 - Only supports flow-based security profiles
 - Proxy based
 - Allow both inspection modes security profiles
 - More thorough and covers more protocols over flow based

Policy & Objects > Firewall Policy

Inspection Mode Flow-based Proxy-based



© Fortinet Inc. All Rights Reserved.

4

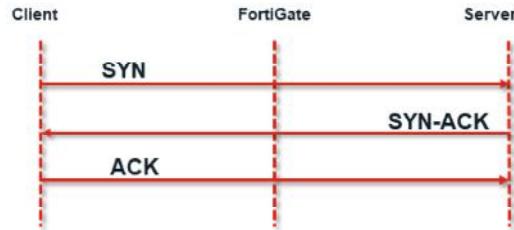
Each inspection component plays a role in processing traffic on its way to its destination. Having control over flow-based and proxy-based mode is helpful if you want to be sure that only flow-based inspection mode is used. In most cases, proxy mode is preferred because more security profile features and more configuration options are available. However, some implementations require all security profile scanning to use only flow-based inspection mode for the highest possible throughput. You can configure the firewall policy to use flow-based mode (which is the default option for a new policy), and vice versa. While both modes offer significant security, proxy-based mode is more thorough while flow-based mode is designed to optimize performance.

You can select the inspection mode in a firewall policy. Switching from flow-based to proxy-based mode will not require removing the selected security profiles on the policy. However, switching from proxy-based to flow-based mode will remove any security profiles configured to use proxy-based inspection mode.

DO NOT REPRINT**© FORTINET**

Flow-Based Inspection

- Default inspection mode
- Uses single-pass direct filter approach (DFA) pattern matching to identify possible attacks or threats
- File is scanned on a flow basis as it passes through FortiGate
- Requires fewer processing resources
- Faster scanning

**FORTINET**

© Fortinet Inc. All Rights Reserved.

5

Flow-based inspection mode examines the file as it passes through FortiGate, without any buffering. As each packet arrives, it is processed and forwarded without waiting for the complete file or web page. If you are familiar with the TCP flow analysis of Wireshark, then that is essentially what the flow engine sees. Packets are analyzed and forwarded as they are received. Original traffic is not altered. Therefore, advanced features that modify content, such as safe search enforcement, are not supported.

The advantages of flow-based mode are:

- The user sees a faster response time for HTTP requests compared to proxy based
- There is less chance of a time-out error because of the server at the other end responding slowly

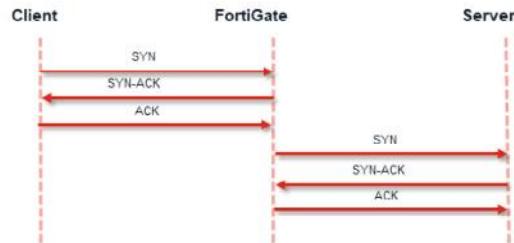
The disadvantages of flow-based mode are:

- A number of security features that are available in proxy-based mode are not available in flow-based mode
- Fewer actions are available based on the categorization of the website by FortiGuard services

DO NOT REPRINT**© FORTINET**

Proxy-Based Inspection

- More thorough inspection
- Adds latency
 - Complete content is scanned
- Two TCP connections
 - From client to FortiGate acting as proxy server
 - From FortiGate to server
- Communication is terminated on Layer 4
- More resource intensive
- Provides a higher level of threat protection



Policy & Objects > Firewall Policy

Inspection Mode Flow-based Proxy-based

FORTINET

© Fortinet Inc. All Rights Reserved.

6

Proxy-based scanning refers to transparent proxy. It's called transparent because, at the IP layer, FortiGate is not the destination address, but FortiGate *does* intercept the traffic. When proxy-based inspection is enabled, FortiGate buffers traffic and examines it as a *whole*, before determining an action. Because FortiGate examines the data as a whole, it can examine more points of data than it does when using flow-based.

In TCP connections, FortiGate's proxy generates the SYN-ACK to the client, and completes the three-way handshake with the client, before creating a second, new connection to the server. If the payload is less than the oversize limit, the proxy buffers transmitted files or emails for inspection, before continuing transmission. The proxy analyzes the headers and may change the headers, such as HTTP host and URL, for web filtering. If a security profile decides to block the connection, the proxy can send a replacement message to the client. This adds latency to the overall transmission speed.

Proxy-based inspection is more thorough than flow-based, yielding fewer false positives and negative results.

DO NOT REPRINT**© FORTINET**

Configuring Inspection Mode

The screenshot shows the 'Policy & Objects > Firewall Policy' section. At the top, there are three tabs: 'Inspection Mode' (disabled), 'Flow-based' (disabled), and 'Proxy-based' (selected). A callout bubble points to the tabs with the text 'Customizable at the policy level'. Below the tabs is a large input field. To the right, under 'Protocol Options', is a table titled 'Protocol Port Mapping' showing port mappings for various protocols.

Protocol	Source Port	Destination Port
HTTP	any	Specify 80
SMTP	any	Specify 25
POP3	any	Specify 110
IMAP	any	Specify 143
FTP	any	Specify 21
NNTP	any	Specify 119
MAPI		135
DNS		53
CIFS		445

Protocol ports can be customized

© Fortinet Inc. All Rights Reserved. 7

FortiGate web filters are also security profiles. The security profiles are customizable, according to the selected inspection mode. So, the first step, before setting up a web filter, is to configure the inspection mode.

The protocol options profile determines the protocols your security profiles use, for example, to inspect web or DNS traffic.

Note that HTTPS inspection port numbers, and other settings related to the handling of SSL, are defined separately in the SSL/SSH inspection profile.

DO NOT REPRINT**© FORTINET**

NGFW Mode

- Features two modes:
 - Profile based
 - Requires application control and web filtering profiles
 - Apply the profiles to the policy
 - Applicable to proxy-based and flow-based inspection modes
 - Policy based
 - Application control and web filtering applied directly to the policy
 - Does not require application control and web filtering profiles
 - Applicable only to flow-based inspection mode
- Antivirus configuration is always profile based, regardless of the NGFW mode selection
- Set the NGFW policy-based mode in the system settings of FortiGate or VDOM

System > Settings

**FORTINET**

© Fortinet Inc. All Rights Reserved.

8

FortiGate, or the individual VDOM, has two next-generation firewall (NGFW) modes available:

1. Profile-based mode: Requires administrators to create and use application control and web filter profiles and apply them to a firewall policy. Profile-based mode is applicable to use flow-based or proxy-based inspection mode as per the policy.
2. Policy-based mode: Administrators can apply application control and web filter configuration directly to a security policy. Flow-based inspection mode is the only applicable process available in policy-based NGFW mode.

Antivirus scanning is available as a security profile that you can apply in a profile-based NGFW mode firewall policy or policy-based NGFW mode security policy.

You can change NGFW mode in the system settings of FortiGate or the individual VDOM. Note that the change will require you to remove all existing policies in either mode.

DO NOT REPRINT

© FORTINET

NGFW Mode—Policy-Based

- Security policy and SSL Inspection & Authentication (consolidated) policy must be configured
- Traffic to match SSL Inspection & Authentication policy first
 - If allowed, then to inspect applications and URL configured on security policy
 - Inspect traffic with additional security profiles if enabled such as IPS and AV
 - Users and groups can be used if authentication is required
- Available actions in security policy: Accept or Deny
- SSL inspection profile to be selected in the consolidated policy

The screenshot displays two side-by-side policy configuration interfaces from the FortiGate management console.

Left Panel: Policy & Objects > SSL Inspection & Authentication

New Policy	
Name	Access Inspection
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Service	ALL

Right Panel: Policy & Objects > Security Policy

New Policy	
Name	Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	Specify
Application	Facebook
URL Category	Social Networking, Streaming Media and Download
Action	ACCEPT (highlighted)

At the bottom left is the FORTINET logo, and at the bottom right are the copyright notice "© Fortinet Inc. All Rights Reserved." and the page number "9".

If you configured FortiGate to use NGFW policy-based mode or created a VDOM specifically to provide NGFW policy-based mode, you must configure a few policies to allow traffic.

SSL Inspection & Authentication (consolidated) policy: This allows traffic from a specific user or user group to match the criteria specified within the consolidated policy and inspect SSL traffic using the SSL inspection profile selected. FortiGate can either accept or deny the traffic.

Security policy: If the traffic is allowed as per the consolidated policy, FortiGate will then process it based on the security policy to analyze additional criteria, such as URL categories for web filtering and application control. Also, if enabled, the security policy further inspects traffic using security profiles such as IPS and AV.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which of the following is the default inspection mode on a firewall policy?
 - A. Proxy-based
 - B. Flow-based

2. How does NGFW policy-based mode differ from profile-based mode?
 - A. Policy-based flow inspection supports web profile overrides.
 - B. Policy-based flow inspection defines URL filters directly in the firewall policy.

3. Which of the following statements about proxy-based web filtering is true?
 - A. It requires more resources than flow-based
 - B. It transparently analyzes the TCP flow of the traffic

DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes



Web Filtering Basics



Additional Proxy-Based Web Filtering Features



DNS Filtering



Best Practices and Troubleshooting

Good job! You now understand inspection modes.

Now, you will learn about web filtering basics.

DO NOT REPRINT

© FORTINET

Web Filtering Basics

Objectives

- Describe web filter profiles
- Work with web filter categories
- Configure web filter overrides
- Configure custom categories
- Submit a FortiGuard rating request

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

By demonstrating competence in web filtering basics, you will be able to describe web filter profiles, use FortiGuard web filter profiles, configure web filter overrides, define custom categories, and submit FortiGuard rating requests.

DO NOT REPRINT**© FORTINET**

Why Apply Web Filtering?

- Mitigate the negative effects of inappropriate web content
- Preserve employee productivity
- Prevent network congestion
- Prevent data loss and exposure of confidential information
- Decrease exposure to Web-based threats
- Prevent copyright infringement
- Prevent viewing of inappropriate or offensive material

**FORTINET**

© Fortinet Inc. All Rights Reserved.

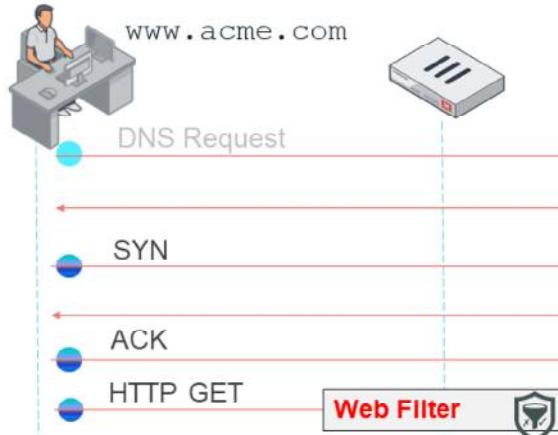
13

Web filtering helps to control, or track, the websites that people visit. There are many reasons why network administrators apply web filtering, including to:

- Preserve employee productivity
- Prevent network congestion, where valuable bandwidth is used for non-business purposes
- Prevent loss or exposure of confidential information
- Decrease exposure to web-based threats
- Limit legal liability when employees access or download inappropriate or offensive material
- Prevent copyright infringement caused by employees downloading or distributing copyrighted materials
- Prevent children from viewing inappropriate material

DO NOT REPRINT**© FORTINET**

When Does Web Filtering Activate?



Filtering is based on request

- Web Filter:
 - HTTP GET

FORTINET

© Fortinet Inc. All Rights Reserved.

14

(slide contains animation)

The example on this slide shows the flow of an HTTP filter process.

FortiGate looks for the `HTTP GET` request to collect URL information and perform web-filtering.

So, as shown, in HTTP the domain name and URL are separate pieces. The domain name might look like this in the header: `Host: www.acme.com`, and the URL might look like this in the header: `/index.php?login=true`.

If we filter by domain, sometimes it blocks too much. For example, the blogs on `tumblr.com` are considered different content, because of all the different authors. In that case, you can be more specific, and block by the URL part, `tumblr.com/hacking`, for example.

DO NOT REPRINT

© FORTINET

Web Filter Profiles—Flow Based

- Profile based
 - Configure web filter profile
 - FortiGuard categories
 - Static URL
 - Rating option
 - Apply profile to firewall policy
- Policy based
 - Apply application control and URL categories directly in a security policy

Security Profiles > Web Filter

Policy & Objects > Security Policy

FORTINET

© Fortinet Inc. All Rights Reserved.

15

Now, you will look at the web filter profile.

This security profile can be configured to use a feature set for proxy-based or flow-based inspection modes. However, depending on the mode you select, the available settings are different. The flow-based inspection has fewer available options.

In the examples shown on this slide, the web filter profile has a FortiGuard category-based filter that categorizes the websites based on categories and sub-categories by FortiGuard. Also, in a flow-based inspection firewall and security policy, FortiGate offers two additional NGFW options:

- **Profile-Based (default)**
 - Web filters are defined as security profiles and applied to the firewall policy
- **Policy-Based**
 - URL categories are defined directly under the firewall policy

Other profile-based options include:

- **File Filter**
- **Search Engines**
- **Static URL Filter**
- **Rating Options**
- **Proxy Options**

DO NOT REPRINT**© FORTINET**

Web Filter Profiles—Proxy Based

- Proxy-based options
 - Configure web filter profile
 - Local categories
 - Remote categories
 - File Filter
 - Search engines
 - Proxy option
 - Apply profile to firewall policy
 - Proxy-based inspection mode type

Security Profiles > Web Filter

New Web Filter Profile

Name	Web Filter Profile
Comments	Write a comment... 0/255
Feature set	Flow-based Proxy-based
<input type="checkbox"/> FortiGuard category based filter	
<input type="checkbox"/> Allow users to override blocked categories	
<input type="checkbox"/> File Filter	
<input checked="" type="checkbox"/> Search Engines	
<input checked="" type="checkbox"/> Static URL Filter	
<input checked="" type="checkbox"/> Rating Options	
<input checked="" type="checkbox"/> Proxy Options	

FORTINET

© Fortinet Inc. All Rights Reserved.

16

In this example shown on this slide, the security profile is configured to use a proxy-based feature set. The profile is available to a firewall policy configured to use proxy-based inspection mode. Other local options include:

- **File Filter**
- **Search Engines**
- **Static URL Filter**
- **Proxy Options**

Once you have configured your web filter profile, apply this profile to your firewall policy so the filtering is applied to your web traffic.

DO NOT REPRINT**© FORTINET**

FortiGuard Category Filter

- Split into multiple categories and subcategories
 - Release new categories and subcategories compatible with updated firmware
 - Older firmware has new values mapped to existing categories
- Live connection to FortiGuard
 - Active contract required
 - Two-day grace period on expiry
- FortiManager can be used instead of FortiGuard

**FORTINET**

© Fortinet Inc. All Rights Reserved.

17

Rather than block or allow websites individually, FortiGuard category filtering looks at the category that a website has been rated with. Then, FortiGate takes action based on that category, not based on the URL.

FortiGuard category filtering is a live service that requires an active contract. The contract validates connections to the FortiGuard network. If the contract expires, there is a two-day grace period during which you can renew the contract before the service cuts off. If you do not renew, after the two-day grace period, FortiGate will report a rating error for every rating request made. In addition, by default, FortiGate blocks web pages that return a rating error. You can change this behavior by enabling **Allow websites when a rating error occurs** setting. You will learn more about this setting in this lesson.

FortiManager can be configured to act as a local FortiGuard server. To do this, you must download the databases to FortiManager, and configure FortiGate to validate the categories against FortiManager, instead of FortiGuard.

DO NOT REPRINT**© FORTINET**

How Are Categories Decided?

- FortiGate queries the FortiGuard Distribution Network (FDN) to determine a website category
- The web filter rating is determined by:
 - Human rater
 - Text analysis
 - Exploitation of web structure
- Description of categories:
 - www.fortiguard.com

**FORTINET**

© Fortinet Inc. All Rights Reserved.

18

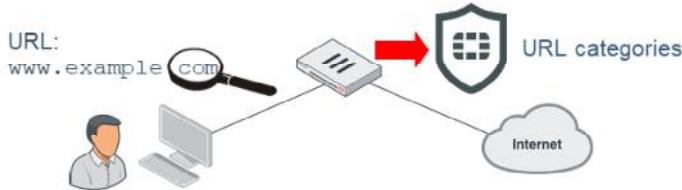
Website categories are determined by both automatic and human methods. The FortiGuard team has automatic web crawlers that look at various aspects of the website in order to come up with a rating. There are also people who examine websites and look into rating requests to determine categories.

To review the complete list of categories and subcategories, go to www.fortiguard.com.

DO NOT REPRINT

© FORTINET

How Does It Work?



Categories action:

Proxy-Based	Flow-Based (Profile)	Flow-Based (Policy)
Allow	Allow	Security policy action
Block	Block	
Monitor	Monitor	
Warning	Warning	
Authenticate	Authenticate	

© Fortinet Inc. All Rights Reserved.

19

So, how does it work?

FortiGate queries the FDN—or FortiManager, if it has been configured to act as a local FortiGuard server—to determine the category of a requested webpage.

When users visit websites, FortiGate uses the FortiGuard live service to determine the category that the URL belongs to and take a configured action for that category, such as allow or block access. Using this feature, you can perform bulk URL filtering, without individually defining each website.

You can enable the FortiGuard category filtering on the web filter, or DNS filter profiles. Categories and subcategories are listed, and the actions to perform can be individually customized.

The actions available will depend on the mode of inspection:

- Proxy: Allow, Block, Monitor, Warning, and Authenticate.
- Flow-based, profile-based: Allow, Block, Monitor, Warning, and Authenticate.
- Flow-based, policy-based: Action defined in a security policy.

DO NOT REPRINT**© FORTINET**

Web Filter FortiGuard Category Action—Warning

- Category Action =

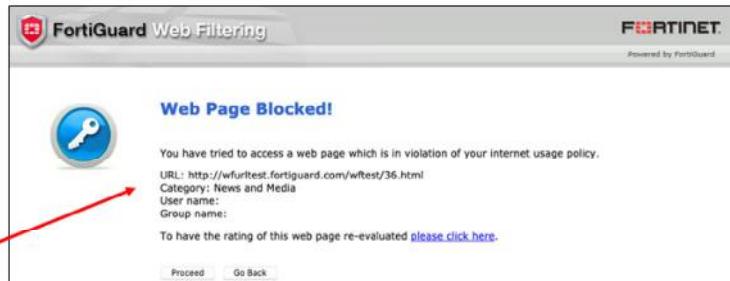


- Exclusive for web filtering

- Proxy mode
- Flow mode (profile-based only)
- Not available in:
 - Static URL filtering feature
 - DNS filter profile

- FortiGuard warning page

- Customizable warning interval

**FORTINET**

© Fortinet Inc. All Rights Reserved.

20

The warning action informs users that the requested website is not allowed by the internet policies. However, the action does give the user the option to proceed to the requested website or return to the previous website.

The warning interval can be customized, so you can present this warning page at specific times, according to the configured period.

DO NOT REPRINT

© FORTINET

Web Filter FortiGuard Category Action—Authenticate

Security Profiles > Web Filter

Category	Action
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Authenticate
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow

Edit Filter

Warning Interval: 0 hours(s) 5 minutes(s) 0 second(s)

Selected User Groups: Guest-group

OK Cancel

WebFilter_Group

1. Define **Users and Group**
2. Set Action = **Authenticate**
3. Select **User Group**

Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.

Username: _____

Password: _____

www.youtube.com

© Fortinet Inc. All Rights Reserved.

21

The authenticate action blocks the requested websites, unless the user enters a successful username and password.

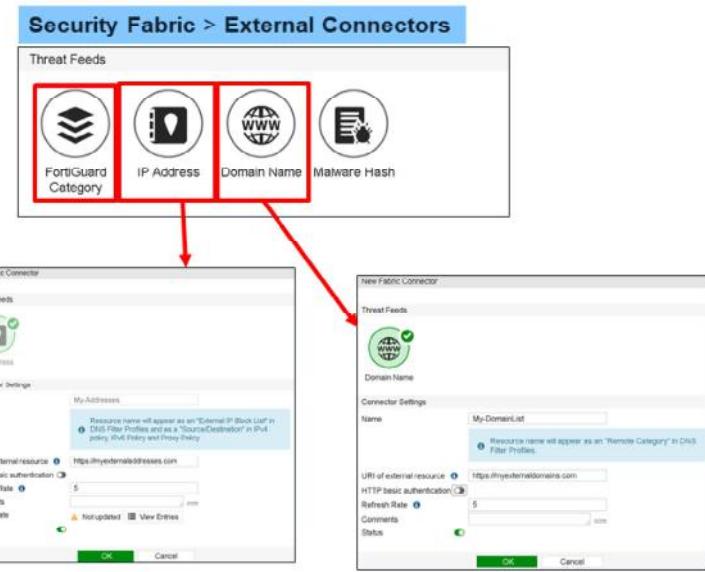
You can customize the interval of time to allow access. Users are not prompted to authenticate again if they access other websites in the same category, until the timer expires.

Choosing this action will prompt you to define user groups that will be allowed to override the block.

DO NOT REPRINT

© FORTINET Threat Feeds

- Dynamically import external block lists from an HTTP server
 - Block list to enforce special security requirements
 - Long-term or short-term policies
 - Dynamically imported, any new changes are instantly imported by FortiOS



FORTINET

© Fortinet Inc. All Rights Reserved.

22

The threat feeds feature enables FortiGate to dynamically import external block lists from an HTTP server. You can use the block lists to enforce special security requirements specified by your organization. These requirements can include long-term policies to always block access to specific websites, or short-term requirements to block access to known compromised locations. These block lists are text files that are in plain text format, where each line contains a single URL to be blocked.

Because the lists are dynamically imported, any changes made to the list are instantly imported by FortiOS using the Security Fabric feature.

FortiGuard Category: This resource name will appear as a “Remote Category” in web filter profiles and SSL inspection exemptions.

Firewall IP Address: This resource name will appear as an “External IP Block List” in DNS filter profiles and as a “Source/Destination” in IPv4 policy, IPv6, and Proxy policy.

Domain Name: This resource name will appear as a “Remote Category” in DNS filter profiles.

Refresh Rate: Using this setting, you can specify how often, in minutes, block lists can be refreshed from the external source.

The size of the block list file can be 10 MB or 128,000 lines of text, whichever is most restrictive.

Note that the DNS profile supports only IPv4 addresses and will ignore IPv6 addresses.

DO NOT REPRINT**© FORTINET**

Using Threat Feeds

- Where can it be used?
 - **FortiGuard Category**
 - Web filter profile – Under **Remote Categories**
 - SSL/SSH Inspection profile – Under **Exempt from SSL Inspection** in **Web Categories**
 - **Firewall IP Address**
 - DNS filter profile – Under **External IP Block Lists**
 - Source/destination in firewall policy
 - **Domain Name**
 - DNS filter profile – Under **Remote Categories**

Security Profiles > Web Filter

Name	Action
Local Categories	
Remote Categories	
Fabric 1	Allow
Potentially Liable	
Adult/Mature Content	

Security Profiles > DNS Filter

Domain Filter	
External IP Block Lists	Fabric 2

Security Profiles > DNS Filter

Name	Action
Remote Categories	
Fabric 3	Allow
Sensitivity Risk	
Unrated	

FORTINET

© Fortinet Inc. All Rights Reserved.

23

Dynamic block lists can be added to:

- Web filter profiles and SSL inspection exemptions
- DNS filter profiles and source/destination addresses in firewall policies

DO NOT REPRINT**© FORTINET**

Web Rating Override

- Override the rating applied to a host name by FortiGuard service
 - Host name reassigned to a completely different category and uses that action
 - Rating overrides are checked prior to contacting FortiGuard for a rating
- Override applies to FortiGate device only
 - Changes are not submitted to FortiGuard subscription services
- Host names only
 - google.com ✓
 - www.google.com ✓
 - www.google.com/index.html ✗
 - google.* ✗



© Fortinet Inc. All Rights Reserved.

24

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names—no URLs or wildcard characters are allowed.

If the contract expires, and the two-day grace period passes, web rating overrides will not be effective. All website category rating requests will be returned with a rating error.

DO NOT REPRINT

© FORTINET

Web Rating Override—Configuration

- Changes a website category, not the category action
 - Make an exception

The screenshot shows the 'Security Profiles > Web Rating Overrides' page. A modal window titled 'New Web Rating Override' is displayed. In the modal, the 'URL' field contains 'www.fortinet.com'. Below it, the 'Category' is set to 'General Interest - Business' and the 'Sub-Category' is set to 'Information Technology'. Under the heading 'Override to', the 'Category' dropdown is set to 'General Interest - Business' and the 'Sub-Category' dropdown is set to 'Information and Computer Security'. The 'Category' and 'Sub-Category' dropdowns in the 'Override to' section are highlighted with red boxes.

FORTINET

© Fortinet Inc. All Rights Reserved.

25

If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, just change the website to an allowed category. The reverse can also be performed, you can block a website that belongs to an allowed category.

Remember that changing categories does not automatically result in a different action for the website. This will depend on the settings within the web filter profile.

DO NOT REPRINT**© FORTINET**

Custom Categories

Security Profiles > Web Rating Overrides

The screenshot shows the 'Custom Categories' section of the FortiGuard Web Rating Overrides interface. At the top, there are buttons for 'Create New', 'Edit', 'Delete', 'Status', and a search bar. A red box highlights the 'Status' button. Below this is a table with columns for 'URL', 'Original Category', and 'Status'. The table lists several predefined categories like 'Finance and Banking', 'Search Engines and Portals', 'Games', etc., each with an 'Enable' checkbox. A second table below shows 'Name', 'Number of Override URLs', 'Number of Web Filter Profile References', and 'Status' for two custom categories: 'custom1' and 'custom2', both of which are enabled.

Name	Number of Override URLs	Number of Web Filter Profile References	Status
custom1	0	0	Enable
custom2	0	0	Enable

- Additional customized categories can be added
- Categories in use cannot be deleted

FORTINET

© Fortinet Inc. All Rights Reserved.

26

If the predefined categories in FortiGuard are not suitable for the situation, you can add additional custom categories.

You can add and delete custom categories as needed, as long as they are not in use.

DO NOT REPRINT

© FORTINET

URL Filtering

URL	Type	Action	Status
^\something\.{org biz}	Regular Expression	<input checked="" type="radio"/> Exempt	<input checked="" type="checkbox"/> Enable
somewhere.*	Wildcard	<input checked="" type="radio"/> Monitor	<input checked="" type="checkbox"/> Enable
www.somesite.com/someURL	Simple	<input checked="" type="radio"/> Block	<input checked="" type="checkbox"/> Enable

URL: www.somesite.com/someURL

Block

FORTINET

- Check against configured URLs in URL filter
 - Entries are checked from top to bottom
- Four possible actions:
 - **Allow:** Access is permitted. Traffic is passed to remaining operations, including FortiGuard web filter, web content filter, web script filters, and antivirus scanning.
 - **Block:** Attempts are denied. User given a replacement message.
 - **Monitor:** Traffic is allowed through. Log entries are created. Also subject to all other security profile inspections.
 - **Exempt:** Allows traffic from trusted sources to bypass all security inspections.
- Types of URL patterns:
 - Simple, wildcards, or regular expressions

© Fortinet Inc. All Rights Reserved.

27

Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, wildcard, and regular expressions.

Let's look at how it works.

When a user visits a website, FortiGate looks at the URL list for a matching entry. In this example, the website matches the third entry in the table, which is set as type **Simple**. This type means that the match must be exact—there is no option for a partial match with this pattern. Also, the action is set to **Block**, thus FortiGate will display a block page message.

DO NOT REPRINT

© FORTINET

FortiGuard Rating Submissions

- Request to re-evaluate a website's rating:

System > FortiGuard

Filtering

Web Filter Cache Clear cache after 60 Minutes

Anti-Spam Cache Clear cache after 30 Minutes

FortiGuard

udp 8888

Test Connectivity

Filtering Services Availability

Web Filtering

Anti-Spam

Request re-evaluation of a URL's category

Live URL Rating Support

URL:

Verify:

Submit

- Request for a website rating: www.fortiguard.com

At a glance

Web Filter Classification Rating Request

Rating Suggestion

URL:

Enter a url or full link to be re-classified

Suggest a category: Please Choose a Category No file chosen

Attach a screenshot image file

© Fortinet Inc. All Rights Reserved.

28

There is always the possibility for errors in ratings, or a scenario where you simply do not agree with the rating given. In that case, you can use the web portal to contact the FortiGuard team to submit a website for a new rating, or get it rated if it is not already in the database.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following is a valid action for FortiGuard web category filtering?
 A. Allow
 B. Deny

2. Which of the following is a valid action for static URL filtering?
 A. Exempt
 B. Warning



© Fortinet Inc. All Rights Reserved.

29

DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes



Web Filtering Basics



Additional Proxy-Based Web Filtering Features



DNS Filtering



Best Practices and Troubleshooting

Good job! You now understand the basics of web filtering.

Now, you will learn about additional proxy-based web filtering features.

DO NOT REPRINT

© FORTINET

Additional Proxy-Based Web Filtering Features

Objectives

- Configure usage quotas
- Configure web profile overrides
- Configure web filter to support search engines
- Configure web content filtering

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

By demonstrating competence in additional proxy-based web filtering features, you will be able to configure usage quotas, web profile overrides, search engine filters, and web content filtering.

DO NOT REPRINT

© FORTINET

FortiGuard Quotas

- Can only apply to the actions:
 - Monitor, Warning, or Authenticate
- Assign quota for each source IP or for each user, if authentication is enabled
- Dedicated monitor feature

- Configuration:

Security Profiles > Web Filter

Category Usage Quota	
<input type="button" value="Create New"/>	<input type="button" value="Edit"/>
<input type="button" value="Delete"/>	
Category	Total quota
Streaming Media and Download	5 minute(s)

- Monitor:

Monitor > FortiGuard Quota

<input type="button" value="Refresh"/>	<input checked="" type="button" value="View"/>	<input type="button" value="Reset Quota"/>
Category Usage Quota		
192.168.1.3	User	192.168.1.3
	Web Filter Profile	Test
	Category	Used Quota
	Streaming Media and Download	54 second(s)
		4 minute(s) and 6 second(s)

FORTINET

© Fortinet Inc. All Rights Reserved.

32

FortiGate also includes a feature to customize the quotas of time to access the categories that are set to monitor, warning, or authenticate in the web filter profile.

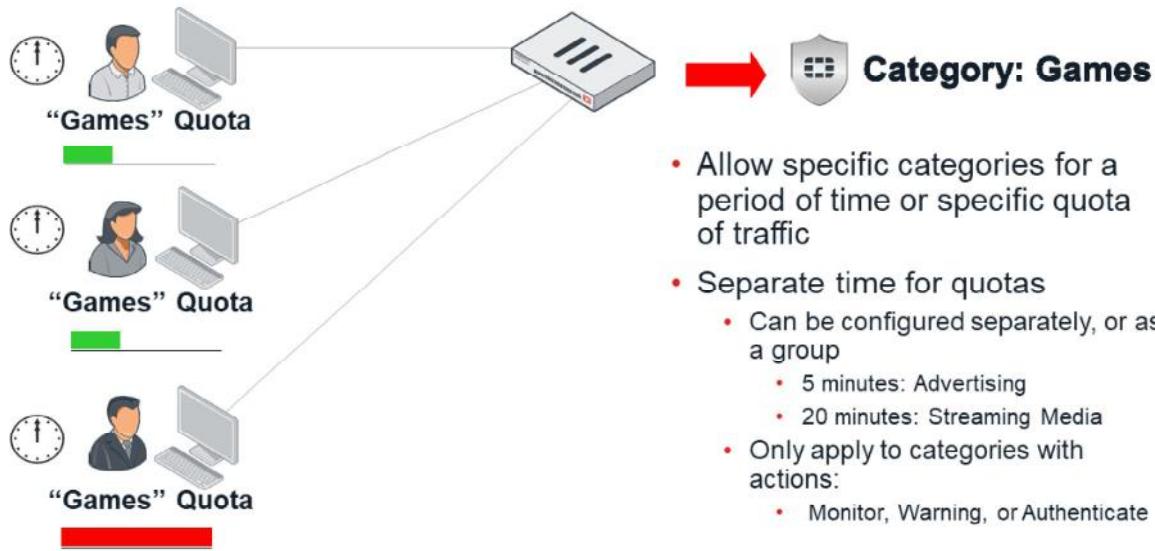
You can customize multiple quotas (timers). Each quota can be applied to either a single category or multiple categories. If the quota applies to multiple categories, the timer is shared among all the categories instead of having a single timer for each individual category.

If the authentication action is not enabled, FortiGate automatically assigns quotas for each source IP, as the monitor feature shows.

Now, let's take a look at how quotas work.

DO NOT REPRINT**© FORTINET**

FortiGuard Usage Quotas



FORTINET

© Fortinet Inc. All Rights Reserved.

33

As shown on this slide, the FortiGuard quota limits the time users spend on websites, based on category. You can also set a quota, on the amount of traffic that can be allowed to a particular category.

A quota cannot redirect the user once the website is loaded in their browser. For example, if the user has 45 seconds left in their quota, and they access a website from the specified category, the selected website will likely finish loading before the remaining 45 seconds are up. Then, the user can stay on that website, and that website won't be blocked until the browser is refreshed. This scenario occurs because the connection to the website is not, generally, a live stream. Once you receive the information, the connection is closed.

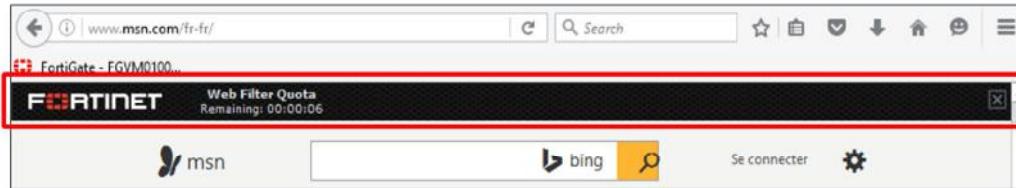
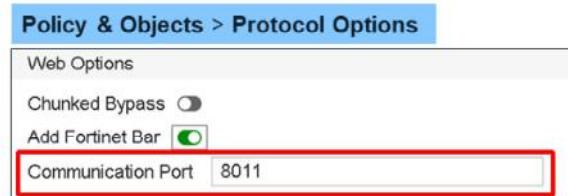
Note that the quota is reset every 24 hours at midnight.

DO NOT REPRINT

© FORTINET

Fortinet Bar

- Only supported for HTTP
- Provides direct feedback to users
- Related to security profiles
 - FortiGuard quota, application control, and so on
- A protocol option profile setting
 - Default communication port: 8011
- Proxy-based firewall policy



FORTINET

© Fortinet Inc. All Rights Reserved.

34

Some FortiGate features can't provide direct feedback to users. For example, FortiGuard quota doesn't provide any feedback until users exceed the quota and refresh the browser, unless the Fortinet bar is enabled.

The Fortinet bar injects a Java applet that communicates with FortiGate and gets additional information from features that would otherwise provide no direct feedback.

The Fortinet bar provides a countdown for FortiGuard quotas. Other features that can't block pages (for example, application control) will show block events in the top bar.

It is important to note that the Fortinet bar can be configured for proxy-based inspection mode, and is only supported for sites using HTTP (not HTTPS).

DO NOT REPRINT

© FORTINET

File Filter

- Web filter profile to inspect files over HTTP and FTP
- Block files based on file type
- Choose which direction of traffic
 - Incoming
 - Outgoing
 - Any
- Work only on proxy-based inspection

The screenshot shows the 'Security Profiles > Web Filter' section. At the top, there are three buttons: 'File Filter' (selected), 'Log', and 'Scan Archived Contents'. Below these are two checkboxes: 'Log' and 'Scan Archived Contents', both of which are checked. A red arrow originates from the 'Create New' button in the main list area and points to the 'Create New File Filter Rule' dialog box.

Name	Comments	Action	Direction	Protocol	File Types	Match Password-Protected Files
PDF files		Block	Any	HTTP FTP	pdf	<input checked="" type="radio"/> Any

Create New File Filter Rule

Name	Images
Comments	Write a comment... 0/255
Protocols	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> FTP
File Types	gif jpeg png
Action	<input type="button" value="Log"/> <input type="button" value="Block"/>
Direction	Incoming Outgoing Any
Match Password-Protected Files	<input type="checkbox"/>

FORTINET

© Fortinet Inc. All Rights Reserved.

35

The web filter security profile can provide file filtering when enabled onto proxy-based inspection mode firewall policies. It inspects files traversing over HTTP and FTP protocols.

You can select supported file types, such as compressed files and javascript content, when creating a new file filter rule. The rule can also specify whether to log or block files entering or leaving the network, or both.

DO NOT REPRINT**© FORTINET**

Web Profile Overrides

- Override web filter profile for:
 - User
 - User group
 - Source IP
- Requires authentication
 - FortiGuard block page link
- Customize override expiration

The screenshot shows two parts of the Fortinet Security Profiles interface:

Security Profiles > Web Filter

Name	Comments	Ref
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

Security Profiles > Web Profile Overrides

New Administrative Override

Scope range	<input checked="" type="radio"/> User <input type="radio"/> User group <input type="radio"/> Source IP
User	<input checked="" type="radio"/> student <input type="radio"/>
Original profile	WEB default
New profile	WEB monitor-all
Expires	02/11/2020 10:22:00.000 AM
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable



© Fortinet Inc. All Rights Reserved.

36

You can also override the filter profile. Web profile overrides change the rules that are used to inspect traffic. Overrides authorize specified users, user groups, or predefined source IPs, to use a different web filter profile to inspect their traffic.

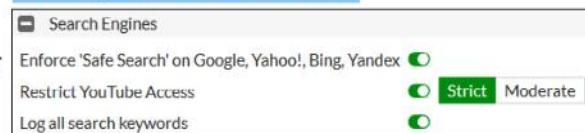
In the example shown on this slide, the new profile applied to the user **student**, inspects all of that user's web traffic from the time that the new profile is applied, until the timer expires. To use this override, you need to enable an override authentication. When you enable the web profile override, the FortiGuard block page shows a link that you can select to activate the override.

DO NOT REPRINT**© FORTINET**

Search Engine Filtering

- Requires FortiGate to use deep SSL inspection
 - Not supported when using certificate inspection
 - FortiGate requires full access to the application layer data
- Restricts websites or images from search results
 - Rewrites the search URL to enable safe search
 - For Google, Yahoo, Bing, and Yandex
- Restricts YouTube access
 - Available in proxy-based inspection mode
 - Set for strict or moderate access control
 - For more information, go to support.google.com
- Logs all search keywords

Security Profiles > Web Filter



```
config webfilter profile
  edit "default"
    config web
      set safe-search url header
    end
  next
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

37

Search engine filtering provides two important features: safe search and restrict YouTube access.

- Safe search is an option that some browsers support. It applies internal filters to the search results. When you enable safe search for the supported search sites, FortiGate appends code to the URL to enforce the use of safe search. For example, on a Google search, FortiGate adds the string `&safe=active` to the URL in the search. So, even if it is not locally enabled in the browser, FortiGate will apply safe search to the requests when they pass through. Safe search is supported for Google, Yahoo, Bing, and Yandex.
- When inspection mode is set to proxy-based, you can set **Strict** or **Moderate** access to YouTube in a web filter profile. For more information about strict and moderate access control, go to support.google.com.
- Only supported when using full SSL inspection because FortiGate requires access to the full header.

DO NOT REPRINT**© FORTINET**

Web Content Filtering

- Requires FortiGate to use SSL deep inspection
- Controls access to web pages containing specific patterns
- Scans the content of every website accepted by security policies
- Matches content from wildcards or Perl regular expressions
- The maximum number of web content patterns in a list is 5000
- Actions:
 - Exempt
 - Block

Pattern Type	Pattern	Language	Action	Status
Wildcard	something*	Western	<input checked="" type="radio"/> Exempt	<input checked="" type="checkbox"/> Enable
Regular Expressi...	.*(quelque...	French	<input checked="" type="radio"/> Block	<input checked="" type="checkbox"/> Enable

FORTINET

© Fortinet Inc. All Rights Reserved.

38

You can also control web content in the web filter profile by blocking access to websites containing specific words or patterns. This helps to prevent access to sites with questionable material.

You can add words, phrases, patterns, wildcards, and Perl regular expressions to match content on websites. You configure this feature on a per-web-filter-profile basis, not at the global level. So, it is possible to add multiple web content filter lists and then select the best list for each web filter profile.

The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases in the page. If the sum is higher than the threshold set in the web filter profile, FortiGate blocks the site.

The maximum number of web content patterns in a list is 5000.

Like search engine filtering, web content filtering requires that FortiGate is using deep SSL inspection because FortiGate will require full access to the packet headers.

DO NOT REPRINT**© FORTINET**

Advanced Web Filter Settings

- Rating options:

1

Allow access to websites that return a rating error from the FortiGuard Web Filter service.

2

Add additional security. The URL and IP address are rated separately.

Security Profiles > Web Filter

Rating Options

Allow websites when a rating error occurs

Rate URLs by domain and IP Address

Rate images by URL

Blocked Images will be replaced with blanks

3

Retrieve ratings for individual images in addition to websites (GIF, JPEG, PNG, BMP, and TIFF).

FORTINET

© Fortinet Inc. All Rights Reserved.

39

You can use advanced web filtering settings to improve the web filter.

The rating options are as follows:

- If a rating error occurs from the FortiGuard web filter service, users will have full unfiltered access to all websites.
- Rate URLs by domain and IP address. This option sends both the URL and the IP address of the requested site for checking, providing additional security against attempts to bypass the FortiGuard system.
- Rate images by URL. This option replaces blocked images with blanks, even if they are part of a website in an allowed category.

DO NOT REPRINT

© FORTINET

Advanced Web Filter Settings

- Feature set proxy based
- Proxy options:

1

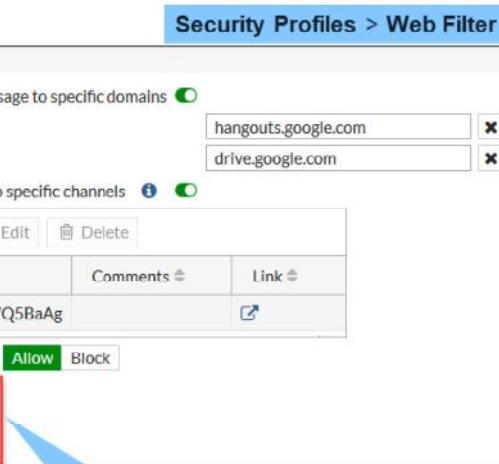
Restrict Google account usage to specific domains by configuring the Google domains you want to allow

2

Block access to specific YouTube channels

3

Limit users from sending information and files to websites



FORTINET

© Fortinet Inc. All Rights Reserved.

40

If the web filter profile is configured to use a proxy-based feature set, the advanced proxy option settings for web filtering are as follows:

1. Block access to some Google accounts and services. You can include an exception list.
2. FortiGate is now able to block access to specific YouTube channels based on Channel IDs.
3. HTTP POST is the command used by your browser when you send information, so you can limit the information and files to websites. The **Allow** option prevents a server timeout when scanning, or when other filtering processes are performed for outgoing traffic.
4. Filter Cookies, Java Applets, and ActiveX scripts from web traffic.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following actions can be used with the FortiGuard quota feature?
 A. Monitor
 B. Shape

2. Which of the following statements about web profile overrides is true?
 A. It is used to change the website category.
 B. Configured users can activate this setting through an override link on the FortiGuard block page.



© Fortinet Inc. All Rights Reserved.

41

DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes



Web Filtering Basics



Additional Proxy-Based Web Filtering Features



DNS Filtering



Best Practices and Troubleshooting

Good job! You now understand additional web filtering features.

Now, you will learn about DNS filtering.

DO NOT REPRINT

© FORTINET

DNS Filtering

Objectives

- Apply a DNS filter

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

By demonstrating competence in DNS filtering, you will be able to apply a DNS filter on FortiGate.

DO NOT REPRINT**© FORTINET**

DNS-Based Web Filtering

- Uses FortiGuard SDNS ratings of DNS queries to decide access
- FortiGate must use FortiGuard SDNS service for DNS lookups
 - DNS queries redirected to FortiGuard SDNS server
- Lightweight
 - Lacks the precision of HTTP filtering
- SSL inspection never required
 - DNS is plain text
- Cannot inspect a URL, only a host name
 - DNS resolves host name
- Supports URL filtering and FortiGuard category only



© Fortinet Inc. All Rights Reserved.

44

You can also inspect DNS traffic using the DNS filter security profile.

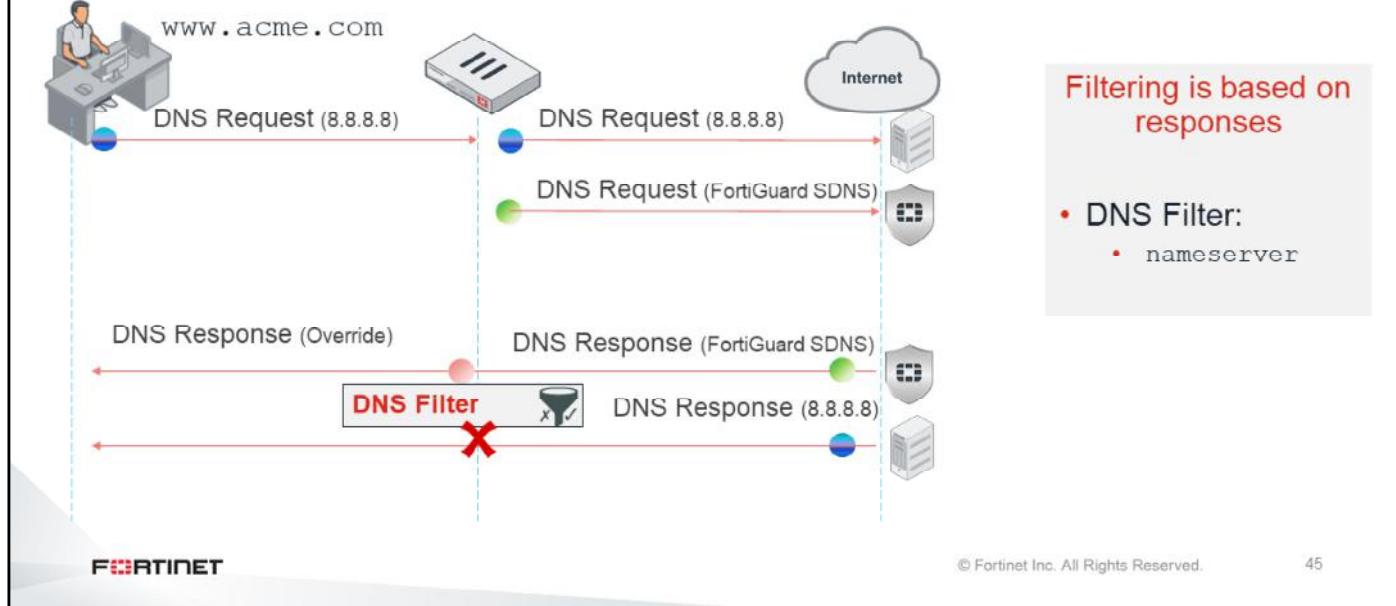
Rather than looking at the HTTP protocol, this option filters the DNS request that occurs prior to an HTTP GET request. This has the advantage of being very lightweight, but at a cost, because it lacks the precision of HTTP filtering.

Every protocol will generate DNS requests in order to resolve a host name; therefore, this kind of filtering will impact all of the higher level protocols that depend on DNS, not just web traffic. For example, it could apply FortiGuard categories to DNS requests for FTP servers. Very few web filtering features are possible beyond host name filtering because of the amount of data available at the point of inspection.

DO NOT REPRINT

© FORTINET

When Does Filtering Activate?



(slide contains animation)

This example illustrates filtering at the DNS lookup process.

DNS filtering looks at the `nameserver` response, which typically occurs when you connect to a website.

As discussed previously, in HTTP, the domain name and URL are separate pieces. The domain name might look like this in the header: `Host: www.acme.com`, and the URL might look like this in the header: `/index.php?login=true`.

When a device initiates a DNS lookup, it sends the FQDN information in the initial request. The DNS lookup occurs before the HTTP request can be sent.

When FortiGate receives the DNS request from the client, it sends a simultaneous request to the FortiGuard SDNS servers. With FortiGuard SDNS service, there are two possible results:

1. Category is allowed: The original DNS response is passed and the remainder of the connection flow continues normally through to the HTTP 200 response. At this point, other web filters might be applied.
2. Category is blocked: FortiGate overrides the site's IP address with the FortiGuard override address and presents a DNS error to the client.

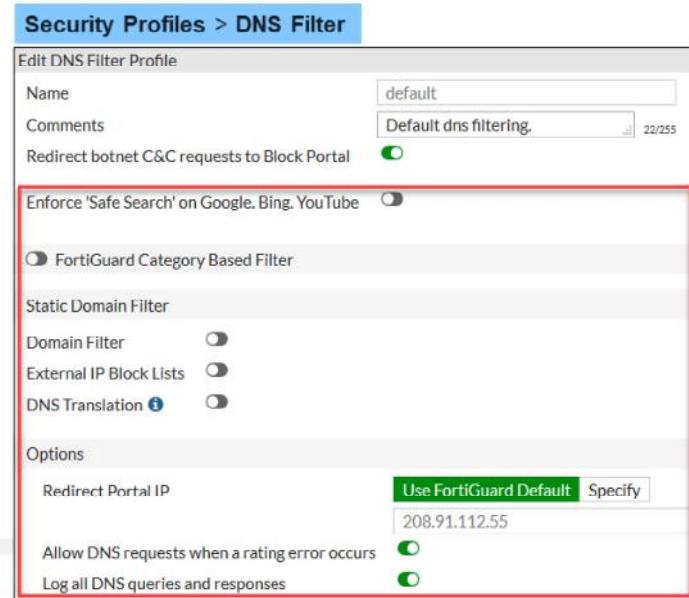
As a result, if you are using DNS filter, and the domain is being blocked, the connection will be blocked before the HTTP request is even sent.

DO NOT REPRINT

© FORTINET

DNS Filter

- DNS filter settings:
 - Enable and disable FortiGuard category-based filter
 - Enable and disable static domain filter
 - Redirect botnet C&C to Block Portal
 - Translate a DNS resolved IP address to another IP address
 - Allow access when rating error occurs
 - Redirect blocked requests to a specific portal
- Apply profile to firewall policy



FORTINET

© Fortinet Inc. All Rights Reserved.

46

Here's a look at the DNS filter profile.

The DNS filter includes various configuration settings. You can enable or disable the FortiGuard category-based filter and the static domain filter. You also have the option to:

- Redirect botnet command and control requests to block portal
- Allow DNS requests when a rating error occurs from the FortiGuard web filter service
- Redirect blocked requests to a specific portal (the **Use FortiGuard Default** setting is recommended)

Using **DNS Translation** feature, you can translate a DNS resolved IP address to another IP address you specify on a per-policy basis.

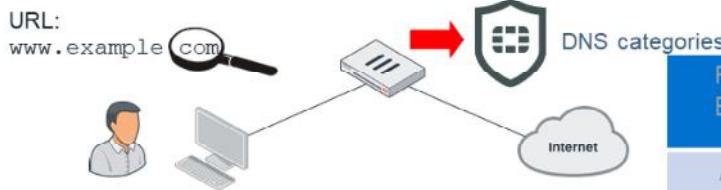
Once you have enabled and saved the settings you require, remember to apply this profile to your firewall policy to activate the options. Any traffic being examined by the policy will have those operations applied to it.

DO NOT REPRINT

© FORTINET

How Does It Work?

```
config system fortiguard
    set sdns-server-ip "208.91.112.220"
end
```



Security Profiles > DNS Filter

This screenshot shows the configuration of a FortiGuard Category Based Filter. It includes sections for 'Allow', 'Monitor', and 'Redirect to Block Portal'. The 'Allow' section lists categories like 'Adult/Mature Content', 'Bandwidth Consuming', 'General Interest - Business', 'General Interest - Personal', 'Potentially Unwanted', 'Remote Categories', 'Security Risk', and 'Unrated'. Each item has a count and a status indicator.

FORTINET

Categories action:

Proxy-Based	Flow-Based (Profile)	Flow-Based (Policy)	DNS Based
Allow	Allow	Security policy action	Allow
Block	Block		Redirect to Block Portal
Monitor	Monitor		Monitor
Warning	Warning		
Authenticate	Authenticate		

© Fortinet Inc. All Rights Reserved.

47

So, how does it work?

FortiGate queries the FortiGuard SDNS servers—or FortiManager, if it has been configured to act as a local FortiGuard server—to identify the category of a requested website.

When users visit websites, FortiGate uses the FortiGuard SDNS service to identify the category that the URL belongs to and take a configured action for that category, such as allow, or redirect to a block portal. Using this feature, you can perform bulk URL filtering, without individually defining each website.

You can enable the FortiGuard category filtering on DNS filter profiles, just as for web filter profiles. Categories and subcategories are listed, and you can customize the actions to perform individually.

DNS filtering supports the following actions:

- Allow
- Redirect to block portal
- Monitor

DO NOT REPRINT

© FORTINET

Static Domain Filter

- Inspects DNS requests
- Actions to DNS requests
 - Redirect to Block Portal, Allow, and Monitor
- Patterns
 - Simple, wildcards, and regex

Security Profiles > DNS Filter			
Static Domain Filter			
Domain Filter <input checked="" type="radio"/>			
Domain	Type	Action	Status
something.com	simple	<input checked="" type="radio"/> Redirect to Block Portal	<input checked="" type="checkbox"/> Enable
*/somesites\$	regex	<input checked="" type="radio"/> Monitor	<input checked="" type="checkbox"/> Enable
*goodsites.	wildcard	<input checked="" type="radio"/> Allow	<input checked="" type="checkbox"/> Enable



© Fortinet Inc. All Rights Reserved.

48

You can configure DNS filtering to allow, redirect to a block portal, or monitor access to websites through the static domain filter. Entries in the domain list are checked against the DNS requests. If a match is found, the configured action is taken.

Patterns set to **Simple** are exact text matches. Patterns set to **Wildcard** allow for some flexibility in the text pattern by allowing wildcard characters and partial matching to occur. Patterns set to **Reg. Expression** allow for the use of PCRE regular expressions.

With this feature, you can prevent many HTTP requests from ever being made, because the initial lookup fails.

DO NOT REPRINT

© FORTINET

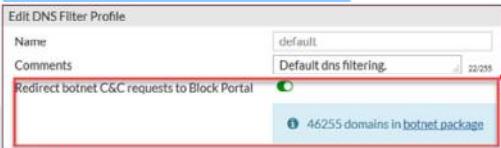
DNS—Botnet Command and Control Database



- Block botnet command and control
 - Imports FortiGuard botnet database
 - Requires FortiGuard IPS license
 - Requires FortiGuard web filter license for DNS filtering

Botnet C&C Domain Definitions	
FQDN	Name
oauth.stashshunt.tk	Other
ulrxketrljzclw.com	Other
imedia.com.mt	Other
a-la-fontaine.com	Other
softbank.c.com	Other
bfbupllfjsf.cn	Other
scotiabank-update.com	Other
tudouo.com	Other
latam.com-voucher-barato.com	Other
amazn.de-vorgangsnummer-secure-bb2.bid	Other
rwweigh.com	Other
rqcfwoxdtlcvl.co.uk	Other
ewblecouvheopuox.com	Other
kzfajhqonpbopfpgerwuotqiv.org	Other
ankarasogulkavadepo.com	Other
purloined-restraint.000webhostapp.com	Other
qnbcardifnans.com	Other
ukpaubfa.org	Other

Security Profiles > DNS Filter



When you enable **Block DNS requests to known botnet C&C** from your DNS filter profile, DNS lookups are checked against the botnet command and control database. This database is dynamically updated from FortiGuard and stored on FortiGate.

All matching DNS lookups are blocked. Matching uses a reverse prefix match, so all subdomains are also blocked.

This service requires an active IPS and web filtering license.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following statements about blocking the known botnet command and control domains is true?
 A. DNS lookups are checked against the botnet command and control database.
 B. The botnet command and control domains can be enabled on the web filter profile.

2. Which of the following security profiles inspects only the fully qualified domain name?
 A. Web Filter
 B. DNS Filter



© Fortinet Inc. All Rights Reserved.

50

DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes

Web Filtering Basics

Additional Proxy-Based Web Filtering Features

DNS Filtering

Best Practices and Troubleshooting

Good job! You now understand DNS filtering.

Now, you will learn about best practices and troubleshooting.

DO NOT REPRINT

© FORTINET

Best Practices and Troubleshooting

Objectives

- Understand HTTP inspection order
- Troubleshoot filter issues
- Investigate FortiGuard connection issues
- Apply web filter cache best practices
- Monitor logs for web filtering events

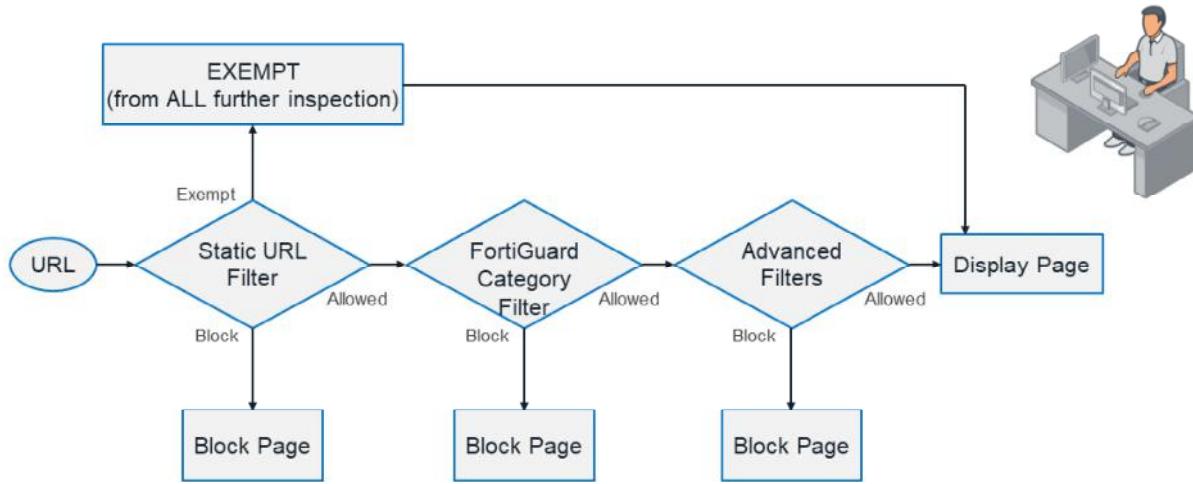
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in best practices and troubleshooting, you will be able to apply various best practices and troubleshooting techniques to avoid and investigate common issues.

DO NOT REPRINT

© FORTINET

HTTP Inspection Order



FORTINET

© Fortinet Inc. All Rights Reserved.

53

Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows:

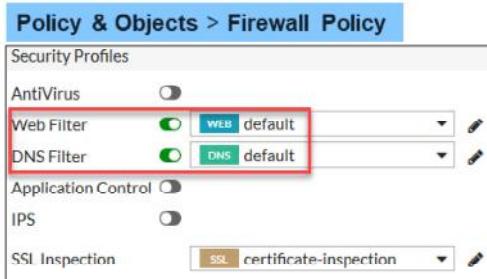
1. The local static URL filter
2. FortiGuard category filtering (to determine a rating)
3. Advanced filters (such as safe search or removing Active X components)

For each step, if there is no match, FortiGate will move on to the next check enabled.

DO NOT REPRINT**© FORTINET**

Apply the Filters

- It's not working? Why?
 - Did you apply the security profiles to the firewall policies?
 - Did you apply the SSL inspection profile, if needed?
 - Is FortiGuard SDNS service accessible for DNS filters?



```

config firewall policy
edit 1
set dnsfilter-profile <profile>
set webfilter-profile <profile>
next
end

config firewall profile-group
edit <group name>
set dnsfilter-profile <profile>
set webfilter-profile <profile>
next
end

```

FORTINET

© Fortinet Inc. All Rights Reserved.

54

You have configured your security profiles, but they are not performing web or DNS inspection. Why?

Check to see if you have applied the security profiles to your firewall policies. Also, make sure that the SSL inspection profile is applied as needed.

Additionally, to use the FortiGate DNS filter, you must use the FortiGuard SDNS service for DNS lookups. DNS lookup requests sent to the FortiGuard SDNS service return with an IP address and a domain rating that includes the FortiGuard category of the website. As a result, for this mechanism to work, the FortiGuard SDNS service must be reachable by FortiGate.

DO NOT REPRINT**© FORTINET**

FortiGuard Connection

- FortiGuard category filtering requires a live connection
- Weight Calculation: default = (difference in time zone) x 10
 - Goes down over time (never below default)
 - Goes up if packets are lost

```

Local # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract
--- Server List (Tue Feb 1 12:00:25 2020) ---
IP          Weight   RTT   Flags  TZ    Packets Curr Lost Total Lost           Updated Time
173.243.138.210    10     85   DI    -8      868      0      0 Tue Feb 1 12:00:23 2020
96.45.33.68        10    270      -8      868      0      0 Tue Feb 1 12:00:23 2020
173.243.138.211    10    340      -8      859      0      0 Tue Feb 1 12:00:23 2020

```



© Fortinet Inc. All Rights Reserved.

55

Category-based filtering requires a live connection to FortiGuard.

You can verify the connection to FortiGuard servers by running the `diagnose debug rating` CLI command. This command displays a list of FortiGuard servers you can connect to, as well as the following information:

- **Weight:** Based on the difference in time zone between the FortiGate and this server (modified by traffic)
- **RTT:** Return trip time
- **Flags:** D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)
- **TZ:** Server time zone
- **Curr Lost:** Current number of consecutive lost packets (in a row, resets to 0 when one packet succeeds)
- **Total Lost:** Total number of lost packets

The list is of variable length depending on the FortiGuard Distribution Network.

DO NOT REPRINT

© FORTINET

Web Filter Cache

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

System > FortiGuard

Cache Type	Action	Value
Web Filter Cache	Clear cache after	60 Minutes
Anti-Spam Cache	Clear cache after	30 Minutes
FortiGuard	Protocol	https
FortiGuard	Port	443

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



© Fortinet Inc. All Rights Reserved.

56

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

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

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

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

DO NOT REPRINT

© FORTINET

Web Filter Log

- Record HTTP traffic activity, such as:
 - Action, profile used, category, URL, quota info, and so on

Log & Report > Web Filter

Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
2020/02/11 12:00:19		192.168.1.2	passthrough	/success.txt?ipv4			
2020/02/11 12:00:19		192.168.1.2	passthrough	/success.txt			
2020/02/11 12:00:19							
2020/02/11 12:00:19		192.168.1.2	blocked	http://detectportal.firefox.com/success.txt			302 B / 0 B
2020/02/11 12:00:19		192.168.1.2	blocked	http://detectportal.firefox.com/success.txt			302 B / 0 B
2020/02/11 12:00:19		192.168.1.2	blocked	http://detectportal.firefox.com/success.txt			302 B / 0 B
2020/02/11 12:00:19		192.168.1.2	blocked	http://detectportal.firefox.com/success.txt			302 B / 0 B

```

date=2020-02-11 time=12:00:19 logid="0317013312" type="utm" subtype="webfilter"
eventtype="ftqd_allow" level="notice" vd="root" logtime=1516299603 policyid=1
sessionid=1839 srcip=10.0.1.10 srcport=56542 srcintf="port3"
srcintfrole="undefined" dstip=205.250.85.48 dstport=80 dstintf="port1"
dstintfrole="undefined" proto=6 service="HTTP"
hostname="detectportal.firefox.com" profile="default" action="passthrough"
reqtype="direct" url="/" sentbyte=367 rcvdbyte=0 direction="outgoing" msg="URL
belongs to an allowed category in policy" method="domain" cat=52
catdesc="Information Technology"
  
```



© Fortinet Inc. All Rights Reserved.

57

Now, take a look at the web filter log and report feature.

This slide shows an example of a log message. Access details include information about the FortiGuard quota and category (if those are enabled), which web filter profile was used to inspect the traffic, the URL, and more details about the event.

You can also view the raw log data by clicking the download icon at the top of the GUI. The file downloaded is a plain text file in a Syslog format.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. You have configured your security profiles, but they are not performing web or DNS inspection. Why?
 - A. The certificate is not installed correctly
 - B. The profile is not associated with the correct firewall policy



© Fortinet Inc. All Rights Reserved.

58

DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes



Web Filtering Basics



Additional Proxy-Based Web Filtering Features



DNS Filtering



Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe FortiOS inspection modes
- ✓ Implement NGFW operation modes
- ✓ Describe web filter profiles
- ✓ Work with web filter categories
- ✓ Configure web filter overrides
- ✓ Configure custom categories
- ✓ Submit a FortiGuard rating request
- ✓ Configure usage quotas
- ✓ Configure web profile overrides
- ✓ Configure web filter to support search engines
- ✓ Configure web content filtering
- ✓ Apply DNS filter
- ✓ Configure SSL/SSH inspection profiles
- ✓ Exempt traffic from SSL inspection
- ✓ Apply SSL inspection profile to a firewall policy
- ✓ Monitor logs for web filtering events

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

By mastering the objectives covered in this lesson, you learned how to configure web filtering on FortiGate to control web traffic in your network.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Application Control

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified 29 May 2020

In this lesson, you will learn how to monitor and control network applications that may use standard or non-standard protocols and ports—beyond simply blocking or allowing a protocol, port number, or IP address.

DO NOT REPRINT

© FORTINET

Lesson Overview



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

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

DO NOT REPRINT

© FORTINET

Application Control Basics

Objectives

- Understand application control
- Detect types of applications
- Understand the FortiGuard application control services database
- Use application control signatures

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

By demonstrating competence in application control basics, you will be able to understand how application control works on FortiGate.

DO NOT REPRINT**© FORTINET**

What is Application Control and How Does It Work?

- Detects and acts on network application traffic
 - Such as Facebook, Skype, Gmail, LogMeIn, and so on
 - Supports many applications and categories, including P2P and proxy
 - Can scan secure protocols
 - Requires SSL/SSH inspection profile in the firewall policy
- How does it work?
 - Uses the IPS engine
 - Uses flow-based scan (not proxy-based)
 - Compares traffic to known application patterns
 - Only reports packets that match an enabled pattern
 - Can detect even if users try to circumvent through an external proxy

**FORTINET**

© Fortinet Inc. All Rights Reserved.

4

Application control detects applications—often applications that consume a lot of bandwidth—and allows you to take appropriate action related to application traffic, such as monitoring, blocking, or applying traffic shaping.

Application control identifies applications, such as Google Talk, by matching known patterns to the application's transmission patterns. Therefore, an application can be accurately identified, only if its transmission pattern is unique. However, not every application behaves in a unique way. Many applications reuse pre-existing, standard protocols and communication methods. For example, many video games, such as *World of Warcraft*, use the BitTorrent protocol to distribute game patches.

Application control can be configured in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, inspection is always flow-based. By comparison, when applying web filtering and antivirus through an HTTP proxy, the proxy first parses HTTP and removes the protocol, and then scans only the payload inside.

Why does FortiGate use a flow-based scan for application control?

Unlike other forms of security profiles, such as web filtering or antivirus, application control is not applied by a proxy. It uses an IPS engine to analyze network traffic and detect application traffic, even if the application is using standard or non-standard protocols and ports. It doesn't operate using built-in protocol states. It matches patterns in the entire byte stream of the packet, and then looks for patterns.

DO NOT REPRINT**© FORTINET**

Detecting Peer-to-Peer Applications

- Why is peer-to-peer (P2P) traffic so difficult to detect?
 - Traditional protocols (HTTP, FTP) have a client-server architecture
 - It uses a single server with large bandwidth for many clients
 - It requires predictable port numbers, NAT/PAT, and firewall policies
 - Peer-to-peer protocols (BitTorrent, Skype) have a distributed architecture
 - Each peer is a server with small bandwidth to share
 - They are difficult to manage multiple firewall policies to block them
 - They do not depend on port forwarding
 - They use evasive techniques to bypass these limitations

**FORTINET**

© Fortinet Inc. All Rights Reserved.

5

When HTTP and other protocols were designed, they were designed to be easy to trace. Because of that, administrators could easily give access to single servers behind NAT devices, such as routers and, later, firewalls.

But when P2P applications were designed, they had to be able to work without assistance—or cooperation—from network administrators. In order to achieve this, the designers made P2P applications able to bypass firewalls and incredibly hard to detect. Port randomization, pinholes, and changing encryption patterns are some of the techniques that P2P protocols use.

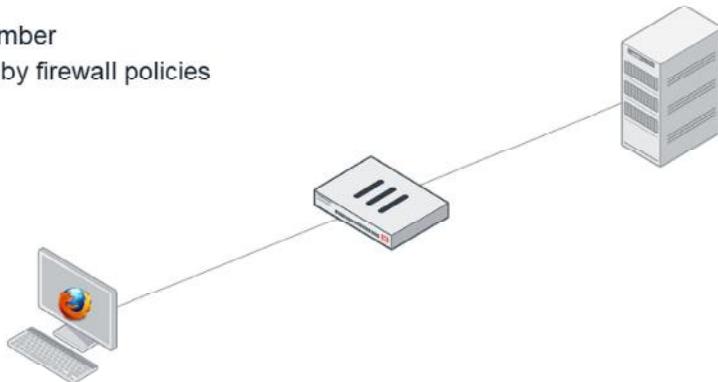
These techniques make P2P applications difficult to block using a firewall policy, and also make them difficult to detect by proxy-based inspection.

Flow-based inspection using the IPS engine can analyze packets for pattern matching and then look for patterns to detect P2P applications.

DO NOT REPRINT**© FORTINET**

Client-Server Architecture

- Traditional download
 - One client
 - One server
 - Known port number
 - Easily blocked by firewall policies

**FORTINET**

© Fortinet Inc. All Rights Reserved.

6

This slide shows a traditional, client-server architecture. There may be many clients of popular sites, but often, such as with an office file server, it's just one client and one server.

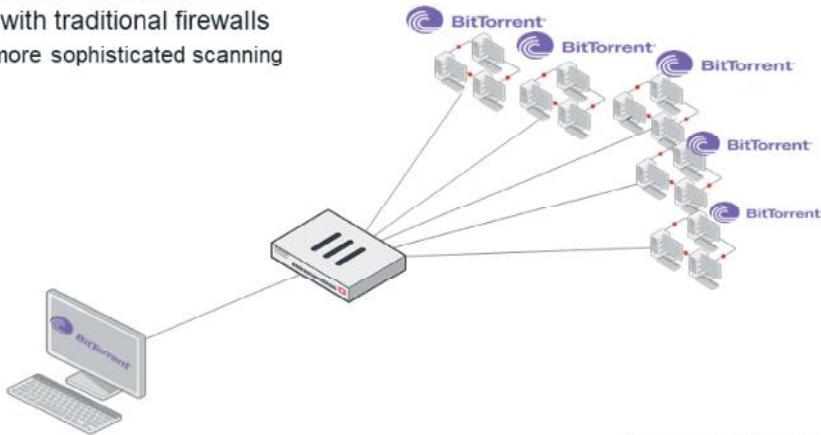
Traditional downloads use a defined protocol over a standard port number. Whether it's from a web or FTP site, the download is from a single IP address, to a single IP address. So, blocking this kind of traffic is easy: you only need one firewall policy.

But, it's more difficult to block traffic from peer-to-peer downloads. Why?

DO NOT REPRINT**© FORTINET**

Peer-to-Peer Architecture

- Peer-to-peer (P2P) download
 - One client
 - Many servers
 - Dynamic port numbers
 - Optionally, dynamic encryption
 - Hard to block with traditional firewalls
 - Requires more sophisticated scanning

**FORTINET**

© Fortinet Inc. All Rights Reserved.

7

Peer-to-peer (P2P) downloads divide each file among multiple (theoretically unlimited) peers. Each peer delivers part of the file. While having many clients is a disadvantage in client-server architectures, it is an advantage for P2P architecture because, as the number of peers increases to n, the file is delivered n times faster.

Because popularity increases the speed of delivery—unlike traditional client-server architecture where popularity could effectively cause a denial of service (DoS) attack on the server—some software, such as BitTorrent distributions of Linux, and games distributing new patches, leverage this advantage. Even if each client has little bandwidth, together they can offer more bandwidth for the download than many powerful servers.

Consequently, in order to download the file, the requesting peer can consume much more bandwidth per second than it would from only a single server. Even if there is only one peer in your network, it can consume unusually large amounts of bandwidth. Because the protocols are usually evasive, and there will be many sessions to many peers, they are difficult to completely block.

DO NOT REPRINT

© FORTINET

Application Control Signatures

- Application control requires a FortiGuard subscription
 - The database of application control signatures is separate from the IPS database.

Entitlement	Status
Firmware & General Updates	Licensed - expires on 2020/05/06 Version 15.00774
Device & OS Identification	Version 1.00093
Internet Service Database Definitions	Version 6.00076

System > FortiGuard

FortiGuard Distribution Network

AntiVirus & IPS Updates

Accept push updates

Scheduled Updates Every 2 Hour

Improve IPS quality

Use extended IPS signature package

Update AV & IPS Definitions

Push updates can also be enabled

Configuring scheduled updates

Forcing FortiGate to check for latest updates

FORTINET

© Fortinet Inc. All Rights Reserved.

8

Before you try to control applications, it's important to understand the signatures used by application control.

How does application control detect the newest applications and changes to application protocols?

Application control requires a subscription to FortiGuard application control. The database for application control signatures is separate from the intrusion prevention system (IPS) database. You can configure FortiGate to automatically update its application control signature database on the FortiGuard page. The application control signature database information is also displayed on the FortiGuard page. You can also enable push updates so that FortiGate receives updates as soon as they are available from the FortiGuard server.

DO NOT REPRINT

© FORTINET

Application Control Database

- A complete list of applications supported by FortiGuard application control can be viewed on <https://fortiguard.com/>
 - You can review the application category or request a signature for a new application from the same website.

ID	Released	Description	Updated
18007	Dec 03, 2009	Ultrasurf is an attempt to access UltraSurf version 9.6 and above. This indicates an attempt to access UltraSurf version 9.6 and above. Ultrasurf is an Internet censorship circumvention product developed by UltraReach Internet Corporation, to bypass Internet censorship and firewalls using various protocols like HTTP Proxy, SSL, cloud servers and DNS. It was initially developed to bypass the Great Firewall of China. Ultrasurf is one of the most popular proxy application used today. It is a closed source software and the security assessments are done by third party experts.	Jul 11, 2019

Category: Proxy

Vendor: UltraReach Internet Corporation

Risk: High

Popularity: High

Deep App: No

Crl: No

Language: English

Deprecated: No

Technology: Client-Server

Behavior: Evasive Tunneling

Refine
search using
filters

© Fortinet Inc. All Rights Reserved.

9

You can view the latest version of the application control database on the FortiGuard website, or by clicking an individual application signature in the application control profile.

The application control database provides details about application control signatures based on category, popularity, and risk, to name a few.

When building an application control signature, the FortiGuard security research team evaluates the application and assigns a risk level. The assigned risk level is based on the type of security risk. The rating is Fortinet-specific, and not related to the common vulnerability scoring system (CVSS) or other external systems. If you aren't aware of the specific application, this information can help you to decide if it would be wise to block an application or not.

On the FortiGuard website, you can read details about each signature's related application.

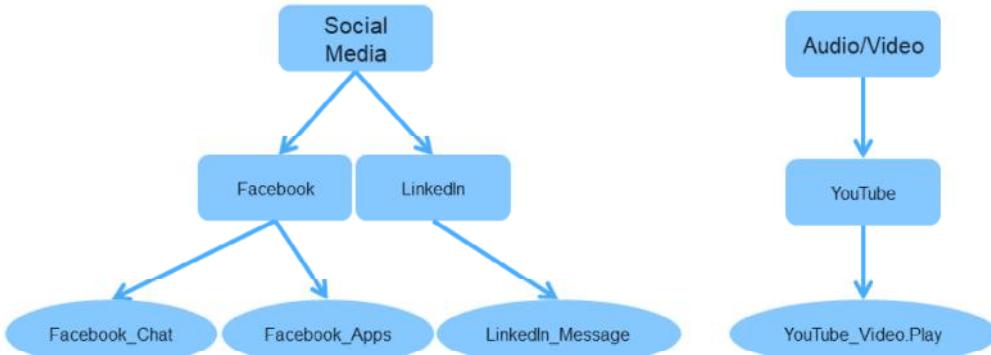
On this slide, you can see an example article for Ultrasurf_9.6+. Ultrasurf_9.6+ is a web proxy, so it belongs in the proxy category. It is a good practice to create test policies that you can use to observe policy behavior.

If there are new applications that you need to control, and the latest update doesn't include definitions for them, you can go to the FortiGuard website and submit a request to have the new applications added. You can also submit a request to re-evaluate an application category, if you believe an application should belong to a different category.

DO NOT REPRINT**© FORTINET**

Hierarchical Structure

- Application control signatures are organized in a hierarchical structure
 - The parent signature takes precedence over the child signature

**FORTINET**

© Fortinet Inc. All Rights Reserved.

10

Many web applications offer functionality that can be embedded in third-party websites or applications. For example, you can embed a Facebook **Like** button at the end of an article or reference a YouTube video on an educational website. FortiOS gives administrators all the tools they need to inspect sub-application traffic. The FortiGuard application control signature database is organized in hierarchical structure. This gives you the ability to inspect the traffic with more granularity. You can block Facebook apps while allowing users to collaborate using Facebook chat.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which statement about application control is true?
 A. Application control uses the IPS engine to scan traffic for application patterns.
 B. Application control is unable to scan P2P architecture traffic.

2. Which statement about the application control database is true?
 A. The application control database is separate from the IPS database.
 B. The application control database must be updated manually.



© Fortinet Inc. All Rights Reserved.

11

DO NOT REPRINT

© FORTINET

Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

Good job! You now understand basic application control functionality.

Now, you will learn about application control configuration.

DO NOT REPRINT

© FORTINET

Application Control Configuration

Objectives

- Configure application control in profile mode
- Configure application control in next generation firewall (NGFW) policy mode
- Use the application control traffic shaping policy

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

By demonstrating competence in configuring the application control operation modes that are available on FortiOS, you will be able to use application control effectively in both profile mode and in NGFW policy mode.

DO NOT REPRINT**© FORTINET**

Application Control Profiles

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



© Fortinet Inc. All Rights Reserved.

14

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

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

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

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

DO NOT REPRINT

© FORTINET

Configuring an Application Control Profile

- The application control profile is available only when NGFW mode is set to profile-based inspection mode

Security Profiles > Application Control

Edit Application Sensor

97 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: wifi-default
Comments: Default configuration for offloading WiFi traffic.

Categories:

- All Categories (selected)
- Business (143, △ 6)
- Email (78, △ 12)
- Mobile (3)
- Proxy (168)
- Storage/Backup (162, △ 16)
- VoIP (24)
- Cloud.IT (47, △ 1)
- Game (84)
- Network.Service (330)
- Remote.Access (84)
- Update (49)
- Web.Client (24)
- Collaboration (255, △ 10)
- General.Interest (229, △ 7)
- P2P (56)
- Social.Media (116, △ 31)
- Video/Audio (154, △ 14)
- Unknown Applications

Firmware & General Updates License
Licensed - expires on 2021/06/06

Application Control Signatures Package
Version 15.00796

Application Signatures
[View Application Signatures](#)

Documentation
[Online Help](#) [Video Tutorials](#)

Displays list of application control signatures

Applies an action to all categories at once

Matches traffic to unidentified applications

© Fortinet Inc. All Rights Reserved. 15

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

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

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

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

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

DO NOT REPRINT**© FORTINET**

Configuring Additional Options

- Application control profiles include additional options

The number to the right of the cloud symbol indicates the number of cloud applications in the category

Categories

- All Categories
 - Business (142, □ 6)
 - Email (78, □ 12)
 - Mobile (3)
 - Proxy (168)
 - Storage/Backup (162, □ 16)
 - VoIP (24)
- Cloud.IT (47, □ 1)
- Game (84)
- Network.Service (330)
- Remote Access (84)
- Update (49)
- WebClient (23)
- Collaboration (255, □ 10)
- GeneralInterest (228, □ 7) (highlighted)
- P2P (56)
- Social.Media (114, □ 31)
- Video/Audio (154, □ 14)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Create New	Edit	Delete	
Priority	Details	Type	Action
No results			

Options

- Block applications detected on non-default ports Allow
- Allow and Log DNS Traffic
- QUIC Allow Block (highlighted)
- Replacement Messages for HTTP-based Applications

FORTINET

© Fortinet Inc. All Rights Reserved.

16

The number listed to the right of the cloud symbol indicates the number of cloud applications within a specified category.

If you need to enable **Allow and Log DNS Traffic**, you should enable it only for short periods, such as during an investigation. Depending on the application and how often it queries DNS servers, enabling this setting can use significant system resources.

QUIC is a protocol from Google. Instead of using the standard TCP connections for web access, QUIC uses UDP, which is not scanned by web filtering. Allowing QUIC instructs FortiGate to inspect Google Chrome packets for a QUIC header, and generate logs as a QUIC message. Blocking QUIC forces Google Chrome to use HTTP2/TLS1.2 and FortiGate to log QUIC as blocked. The default action for QUIC is **Block**.

The **Replacement Messages for HTTP-based Applications** setting allows you to replace blocked content with an explanation (for the user's benefit). However, for non-HTTP/HTTPS applications, you can only drop the packets or reset the TCP connection.

After you've configured the application control profile, select the profile in the firewall policy. Like any other security profile, the settings you configure in the application control profile are not applied globally. FortiGate applies the application control profile settings to only traffic governed by the firewall policy in which you've selected the application control profile. This allows granular control.

DO NOT REPRINT

© FORTINET

Protocol Enforcement on HTTP and DNS Ports

- Allows blocking or monitoring of known services on unknown ports

The screenshot shows the 'Edit Application Sensor' screen under 'Security Profiles > Application Control'. On the left, there's a tree view of application categories like Business, Mobile, and Network. In the center, a table lists network protocol enforcement rules for ports 53 and 80. Port 53 has 'DNS' listed under 'Enforce Protocols' with 'Monitor' as the violation action. Port 80 has 'HTTP' listed under 'Enforce Protocols' with 'Block' as the violation action. A red arrow points from the 'Create New' button in the table to a modal dialog titled 'New Default Network Service'. This dialog has 'Port' set to '80', 'Enforce protocols' set to 'PROT HTTP', and 'Violation action' set to 'Block'. A red box highlights the 'PROT HTTP' option in the dropdown. A blue callout labeled 'List of known services' points to a sidebar on the right containing a list of services: DNS, FTP, HTTPS, IMAP, NTP, POP3, SMTP, SNMP, SSH, and TELNET. The 'HTTPS' entry is highlighted.

FORTINET

© Fortinet Inc. All Rights Reserved.

17

Protocol enforcement is added to the application control profile, allowing the administrator to configure network services (for example, FTP, HTTP, and HTTPS) on known ports (for example, 21, 80, and 443), while blocking those services on other ports.

The feature takes action in the following scenarios:

- When one protocol dissector confirms the service of network traffic, protocol enforcement can check whether the confirmed service is whitelisted under the server port. If it is not, then the traffic is considered a violation and IPS can take the action (for example, block) specified in the configuration.
- There is no confirmed service for network traffic. It would be considered a service violation if IPS dissectors rule out all the services enforced under its server port.

DO NOT REPRINT**© FORTINET**

Scanning Order

- The IPS engine identifies the application
- The application control profile scans for matches in this order:
 - Application and filter overrides
 - Categories

The screenshot shows the 'Edit Application Sensor' configuration page. At the top, there are fields for 'Name' (set to 'default') and 'Comments' (set to 'Monitor all applications, 25/255'). A 'View Application Signatures' button is also present. Below these, the 'Categories' section is highlighted with a red box and a green number 2. It contains a list of application categories with their counts: Business (142), Email (78), Mobile (3), Proxy (160), Storage/Backup (162), VoIP (24), Cloud/IT (47), Game (84), Network/Service (330), Remote/Access (84), Update (49), Web/Client (23), Collaboration (255), General/Interest (228), P2P (56), Social/Media (114), Video/Audio (154), and Unknown Applications. Below the categories is a 'Network Protocol Enforcement' section. The 'Application and Filter Overrides' section is highlighted with a red box and a green number 1. It includes a table with columns: Priority, Details, Type, and Action. The table displays the message 'No results'. At the bottom, there are several 'Options' settings: 'Block applications detected on non-default ports' (radio button selected), 'Allow and Log DNS Traffic' (checkbox checked), 'QUIC' (radio button selected), and 'Replacement Messages for HTTP-based Applications' (checkbox checked).

© Fortinet Inc. All Rights Reserved.

18

The IPS engine examines the traffic stream for a signature match.

Then, FortiGate scans packets for matches, in this order, for the application control profile:

- Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies.
- Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories.

DO NOT REPRINT

© FORTINET

Order of Scan and Blocking Behavior (Scenario 1)

1. **Application Overrides:** Battle.Net and Dailymotion applications are set to **Allow**
2. **Filter Overrides:** Excessive bandwidth consuming applications are set to **Block**
 - Will contain applications from different categories – BitTorrent (P2P), Adobe.Update (Update), FaceTime (VOIP), Flickr (Social.Media)
3. **Categories:** The **Game** and **Video/Audio** categories are set to **Block** and all other categories set to **Monitor**

Priority	Details	Type	Action
1	Battle.Net	Application	Allow
2	Excessive.Bandwidth	Filter	Block

FORTINET

© Fortinet Inc. All Rights Reserved.

19

In the example profile shown on this slide, the application control profile blocks the **Game** and **Video/Audio** categories. For applications in these categories, FortiGate responds with the application control HTTP block message. (It is slightly different from the web filtering HTTP block message.) All other categories are set to **Monitor**, except **Unknown Applications**, and are allowed to pass traffic.

In the **Application Overrides** section, you can see that some exceptions are specified. Instead of being set to **Block**, **Battle.Net (Game)** and **Dailymotion (Video/Audio)** are set to **Monitor**. Because application overrides are applied first in the scan, these two applications will be allowed, and will generate logs.

Next, the scan will check for **Application and Filter Overrides**. Because a filter override is configured to block applications that use excessive bandwidth, it will block all applications using excessive bandwidth, regardless of categories that allow these applications.

This slide shows an example of how several security profile features could work together, overlap, or work as substitutes, on the same traffic.

After the application control profile scan is done, FortiGate begins other scans, such as web filtering. The web filtering scan could block Battle.Net and Dailymotion, but it would use its own block message. Also, web filtering doesn't check the list of application control overrides. So, even if an application control override allows an application, web filtering could still block it.

Similarly, static URL filtering has its own exempt action, which bypasses all subsequent security checks. However, application control occurs before web filtering, so that the web filtering exemption cannot bypass application control.

DO NOT REPRINT

© FORTINET

Order of Scan and Blocking Behavior (Scenario 2)

1. **Filter Overrides:** Excessive bandwidth consuming applications are set to **Block**
 - Will contain applications from different categories – BitTorrent (P2P), Adobe.Update (Update), FaceTime (VOIP), Flickr (Social.Media)
2. **Application Overrides:** Battle.Net and Dailymotion applications are set to **Allow**
3. **Categories:** The **Game** and **Video/Audio** categories are set to **Block** and all other categories set to **Monitor**

The screenshot shows the 'Edit Application Sensor' screen under 'Security Profiles > Application Control'. The 'Categories' section lists various application categories with their counts: Business (142), Email (70), Mobile (3), Proxy (168), Storage/Backup (162), VoIP (24), Game (54), Network/Service (930), Remote Access (84), Update (49), WebClient (23), Collaboration (255), General Interest (229), PEP (54), Social Media (114), Video/Audio (154), and Unknown Applications. The 'Application and Filter Overrides' section contains two entries: entry 1 is a 'Filter' for 'Excessive Bandwidth' with a priority of 1 and an action of 'Block'; entry 2 is an 'Application' override for 'Battle.Net' and 'Dailymotion' with a priority of 2 and an action of 'Allow'. A green circle with the number 3 points to the 'Game' category, which is highlighted with a red border. A green circle with the number 2 points to the 'Video/Audio' category, also highlighted with a red border. A green circle with the number 1 points to the first entry in the overrides table.

FORTINET

© Fortinet Inc. All Rights Reserved.

20

In the example profile shown on this slide, the filter override has been moved above the application override. In this scenario, the filter override (**Excessive-Bandwidth**) will be blocked and since **Dailymotion** falls under the excessive bandwidth category, Dailymotion will be blocked even though it is set to **Allow** under the **Application and Filter Overrides** section.

The priority in which application and filter overrides are placed takes precedence.

DO NOT REPRINT

© FORTINET

Actions

- Allow
 - Continue to next scan or feature and do not log
- Monitor
 - Allow but log
 - Good for the initial study of your network traffic
- Block
 - Drop packets and log
- Quarantine
 - Block and log traffic from attacker IP address until the expiration time
 - Can set duration to days, hours, or minutes



View the list of signatures of native or cloud applications for a specific category

FORTINET

© Fortinet Inc. All Rights Reserved.

21

For each filter in the application control profile, you must indicate an action—what FortiGate does when traffic matches. Actions include the following:

- **Allow:** Passes the traffic and does not generate a log
- **Monitor:** Passes the traffic, but also generates a log message
- **Block:** Drops the detected traffic and generates a log message
- **Quarantine:** Blocks the traffic from an attacker IP until the expiration time is reached and generates a log message

The **View Signature** action allows you to view signatures from a particular category only and is *not a* configurable action. The **View Cloud Signatures** action allows you to view application signatures for cloud applications from a particular category.

Which is the correct action to choose?

If you're not sure which action to choose, **Monitor** can be useful initially, while you study your network. Later, after you have studied your network traffic, you can fine-tune your filter selection by choosing the most appropriate action. The action you choose also depends on the application. If an application requires feedback to prevent instability or other unwanted behavior, then you might choose **Quarantine** instead of **Block**. Otherwise, the most efficient use of FortiGate resources is to block.

DO NOT REPRINT**© FORTINET**

Applying an Application Control Profile

- Application control profile must be applied on a firewall policy to scan the passing traffic
 - SSL/SSH Inspection profile must also be selected

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. On the left, under 'Security Profiles', the 'Application Control' and 'SSL Inspection' checkboxes are selected. Both dropdown menus are open, showing 'default' and 'deep-inspection' respectively. A red box highlights the 'SSL Inspection' dropdown. A blue callout bubble points to the 'deep-inspection' option in the dropdown, with the text 'Use deep-inspection profile to scan encrypted traffic'. On the right, a separate window shows the 'SSL inspection' profile list, where 'deep-inspection' is highlighted in yellow.

Profile Type	Profile Name
APP	default
SSL	deep-inspection
SSL	certificate-inspection
SSL	custom-deep-inspection
SSL	no-inspection

FORTINET

© Fortinet Inc. All Rights Reserved.

22

After an application control profile is configured, it must be applied to a firewall policy. This will instruct FortiGate to start scanning application traffic that is subject to the firewall policy.

DO NOT REPRINT

© FORTINET

Block Page

- Application control in profile mode will display similar HTTP block pages
- HTTP block page includes:
 - Category
 - Website host and URL
 - User name (if authentication is enabled)
 - Group name (if authentication is enabled)
 - Policy UUID



FORTINET

© Fortinet Inc. All Rights Reserved.

23

For HTTP-based applications, application control can provide feedback to the user about why their application was blocked. This is called a block page, and it is similar to the one you can configure for URLs that you block using FortiGuard web filtering.

It is also worth mentioning that, if deep inspection is enabled in the firewall policy, all HTTPS-based applications will provide this block page.

The block page contains the following information:

- Signature that detected the application (in this case, Dailymotion)
- Signature's category (Video/Audio)
- URL that was specifically blocked (in this case, the index page of www.dailymotion.com), since a web page can be assembled from multiple URLs
- User name (if authentication is enabled)
- Group name (if authentication is enabled)
- UUID of the policy governing the traffic

The last item in this list can help you to identify which policy on FortiGate blocked the page, even if you have a large number of policies with many FortiGate devices securing different segments.

DO NOT REPRINT**© FORTINET**

NGFW Policy-Based Mode

- Available in flow-based inspection mode only
- Application control is configured directly on the security policy
 - Cannot configure application control profile
- SSL inspection profile must be selected on an SSL Inspection & Authentication (consolidated) policy
- Requires the use of central SNAT policy

Policy & Objects > Central SNAT

The screenshot shows the Central SNAT configuration. It includes fields for Incoming Interface (port2), Outgoing Interface (port1), Source Address (all), Destination Address (all), and a NAT section. The NAT section has options for IP Pool Configuration (Use Outgoing Interface Address, Use Dynamic IP Pool), Protocol (any, TCP, UDP, SCTP, Specify), and Explicit port mapping.

Policy & Objects > SSL Inspection & Authentication

Edit Policy

The screenshot shows the SSL Inspection & Authentication configuration for a policy named 'Default'. It includes sections for Source (all), Destination (all), Service (ALL), and SSL Inspection (certificate-inspection). There are also tabs for Policy Details, Firewall Rules, and Object Groups.

© Fortinet Inc. All Rights Reserved.

24

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

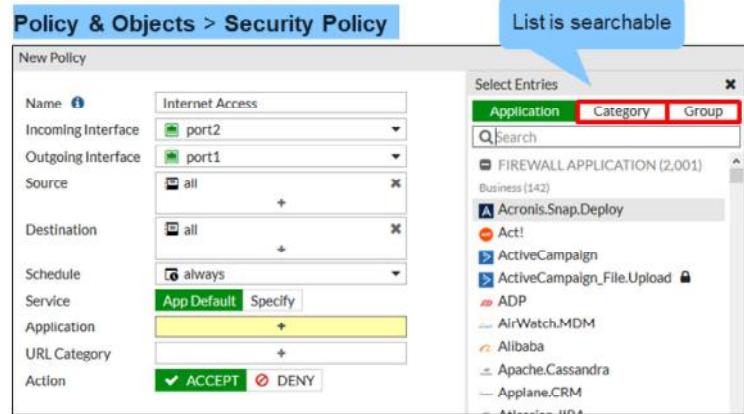
It is important to note that all security policies in an NGFW policy-based mode VDOM or FortiGate must specify an SSL/SSH inspection profile on a consolidated policy. NGFW policy-based mode also requires the use of central source NAT (SNAT), instead of NAT settings applied within the firewall policy.

DO NOT REPRINT

© FORTINET

NGFW Policy-Based Mode (Contd)

- You can select applications, application categories, or groups directly on a security policy
- You can apply the **ACCEPT** or **DENY** actions to allow or block selected application traffic
- If a **URL Category** is set, then applications that you add to the policy must be within the browser-based technology category
- You can apply the **AntiVirus** and **IPS** security profiles to a security policy with the action set to **ACCEPT**



FORTINET

© Fortinet Inc. All Rights Reserved.

25

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

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

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

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

DO NOT REPRINT**© FORTINET**

How Does NGFW Policy-Based Filtering Work?

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



© Fortinet Inc. All Rights Reserved.

26

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

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

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

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

DO NOT REPRINT

© FORTINET

Configuring App Control in Policy-Based Mode

The screenshot illustrates the configuration of application control in Policy-Based Mode. On the left, the 'Policy & Objects > Security Policy' interface shows a new policy named 'Full_Access' with 'port2' as the incoming interface and 'port1' as the outgoing interface. The source is set to 'LOCAL_SUBNET' and the destination is 'all'. The schedule is 'always', and the service is 'App Default'. In the 'Application' section, 'YouTube' is selected. The action is set to 'ACCEPT'. On the right, a 'Select Entries' dialog is open, showing a list of applications including 'youtube', 'YouTube_Messenger', 'YouTube_Downloader.YTD', 'YouTube_Comment.Posting', 'YouTube_HD.Streaming', 'YouTube_Search.Safety.Mode.Off', 'YouTube_SearchVideo', and 'YouTube_Video.Embedded'. A red box highlights the 'Group' tab in the 'Select Entries' dialog, and a red arrow points from the 'Group' tab to a 'New Application Group' dialog on the right. This dialog shows a group named 'High Bandwidth' with 'Type' set to 'Application' and members 'Dailymotion' and 'YouTube'. A red box highlights the 'Category' tab in the 'Select Entries' dialog, and another red arrow points from the 'Category' tab to the 'New Application Group' dialog.

Configuring application control in NGFW policy-based mode is simple. You can create a new security policy or edit an existing security policy. In the **Application** section, select the applications, categories, or groups that you want to allow or deny, and change the security policy **Action** accordingly. On applications that you selected to allow, you can further enhance network security by enabling antivirus scanning and IPS control. You can also enable the logging of **Security Events** or **All Sessions** to ensure that all application control events are logged.

DO NOT REPRINT

© FORTINET

Policy-Based Central SNAT Policy

Policy & Objects > Central SNAT

Edit Policy		
Incoming Interface	<input checked="" type="checkbox"/> port2 +	✖
Outgoing Interface	<input checked="" type="checkbox"/> port1 +	✖
Source Address	<input checked="" type="checkbox"/> all +	✖
Destination Address	<input checked="" type="checkbox"/> all +	✖

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Protocol any TCP UDP SCTP Specify 0

Policy & Objects > SSL Inspection & Authentication

Edit Policy		
Name	Default	✖
Incoming Interface	<input type="checkbox"/> any	▼
Outgoing Interface	<input type="checkbox"/> any	▼
Source	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> b all	+ ✖
Destination	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> b all	+ ✖
Service	<input checked="" type="checkbox"/> ALL	+ ✖

Firewall / Network Options

Central NAT is enabled so NAT settings from matching [Central SNAT policies](#) will be applied.

Security Profiles

SSL Inspection certificate-inspection

© Fortinet Inc. All Rights Reserved. 28

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

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

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

DO NOT REPRINT

© FORTINET

NGFW Policy Matching

- Based on the configuration shown in the screenshot:
 - Facebook, Flickr, Instagram, and Pinterest application traffic will be blocked by policy ID 2
 - All other Social.Media (for example, LinkedIn) application traffic will be allowed by policy ID 3
 - All applications that belong to the P2P application category will be blocked by policy ID 4
 - All other traffic and applications will be allowed by policy ID 5

Policy & Objects > Security Policy										
ID	Name	Source	Destination	Schedule	Service	Applications	URL Category	Action	Security Profiles	Log
1	port1 → port1									
2	Blocking apps	all	all	always	App Default	Facebook Flickr Instagram Pinterest		DENY	All	0
3	Allow social media	all	all	always	App Default	Social.Media		ACCEPT	All	0
4	Blocking P2P Apps	all	all	always	App Default	P2P		DENY	Disabled	0
5	Allow all	all	all	always	App Default			ACCEPT	default	UTM

FORTINET

© Fortinet Inc. All Rights Reserved.

29

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

DO NOT REPRINT**© FORTINET**

Application Control Traffic Shaping

- Granular control of bandwidth usage
- Some traffic can't be distinguished by port number/IP
 - Example: YouTube video URLs—don't say whether it is a text comment or a video
<https://www.youtube.com/watch?v=eO2vyJDoP3M>
- Only traffic that matches the signature is shaped
 - Won't interfere with other apps on same port/protocol
 - Useful for managing bandwidth-intensive apps

Total: 1,536 Kbps

**FORTINET**

© Fortinet Inc. All Rights Reserved.

30

If an application is necessary, but you need to prevent it from impacting bandwidth, then instead of blocking it entirely, you can apply a rate limit to the application. For example, you can rate limit applications used for storage or backup leaving enough bandwidth for more sensitive streaming applications, such as video conferencing.

Applying traffic shaping to applications is very useful when you're trying to limit traffic that uses the same TCP or UDP port numbers as mission-critical applications. Some high-traffic web sites, such as YouTube, can be throttled in this way.

Examine the details of how throttling works. Not all URL requests to www.youtube.com are for video. Your browser makes several HTTPS requests for:

- The web page itself
- Images
- Scripts and style sheets
- Video

All of these items have separate URLs. If you analyze a site like YouTube, the web pages themselves don't use much bandwidth; it is the video content that uses the most bandwidth. But, since all content is transported using the same protocol (HTTPS), and the URLs contain dynamically generated alphanumeric strings, traditional firewall policies can't block or throttle the traffic by port number or protocol because they are the same. Using application control, you can rate limit only videos. Doing this prevents users from saturating your network bandwidth, while still allowing them to access the other content on the site, such as for comments or sharing links.

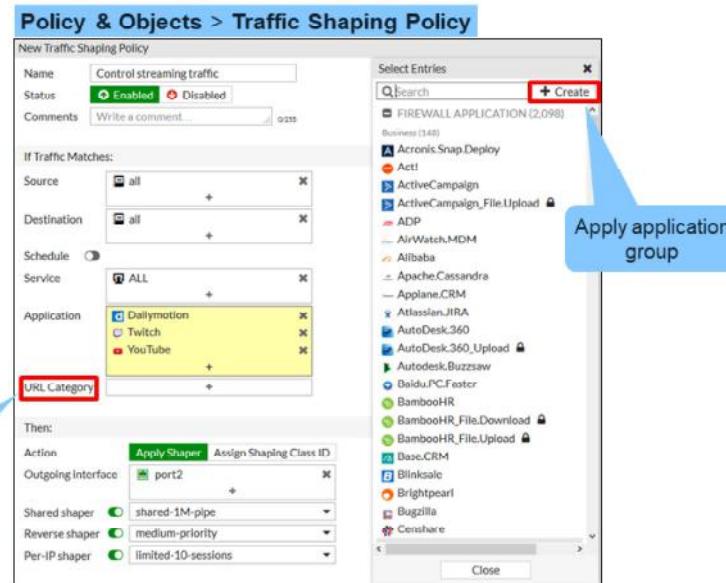
DO NOT REPRINT

© FORTINET

Configuring the Traffic Shaping Policy

- Must ensure matching criteria aligns with the settings in your firewall policy
 - Firewall policy must allow the traffic that you wish to control bandwidth of
- Can shape traffic for application control based on:
 - Application category
 - Application
 - Application group

Used for web filtering



FORTINET

© Fortinet Inc. All Rights Reserved.

31

You can limit the bandwidth of an application category or specific application by configuring a traffic shaping policy. You can also apply traffic shaping to FortiGuard web filter categories and to the application group.

You must ensure that the matching criteria aligns with the firewall policy or policies to which you want to apply shaping. It does not have to match outright. For example, if the source in the firewall policy is set to **all** (0.0.0.0/0.0.0.0), the source in the traffic shaping policy can be set to any source that is included in **all**, for example, **LOCAL_SUBNET** (10.0.1.0/24).

If the traffic shaping policy is not visible in the GUI, you can enable it on the **Feature Visibility** page.

There are two types of shapers that can be configured on the **Traffic Shaping Policy** page, and you can apply them in the traffic shaping policy:

- **Shared shaper**: Applies a total bandwidth to all traffic using that shaper. The scope can be per policy or for all policies referencing that shaper.
- **Per-IP shaper**: Applies traffic shaping to all source IP addresses in the security policy. Bandwidth is equally divided among the group.

Note that the outgoing interface is usually the egress interface (WAN). The **Shared shaper** setting is applied to ingress-to-egress traffic, which is useful for restricting bandwidth for uploading. The **Reverse Shaper** setting is also a shared shaper, but it is applied to traffic in the reverse direction (egress-to-ingress traffic). This is useful for restricting bandwidth for downloading or streaming, because it limits the bandwidth from the external interface to the internal interface.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which statement about application control in NGFW policy-based configuration is true?
 A. Applications are applied directly to the security policies.
 B. The application control profile must be applied to firewall policies.

2. Which statement about the HTTP block page for application control is true?
 A. It can be used only for web applications.
 B. It works for all types of applications.

DO NOT REPRINT

© FORTINET

Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control



Best Practices and Troubleshooting

Good job! You now understand application control operation modes.

Now, you will learn about logging and monitoring application control events.

DO NOT REPRINT

© FORTINET

Logging and Monitoring Application Control

Objectives

- Enable application control logging events
- Monitor application control events
- Use FortiView to see a detailed view of application control logs

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

By demonstrating competence in application control configuration, including reviewing application control logs, you will be able to effectively use and monitor application control events.

DO NOT REPRINT

© FORTINET

Enabling Application Control Logging

- Example of NGFW policy-based mode firewall policies

ID	Name	Source	Destination	Schedule	Service	Applications	UTM Category	Action	Security Profiles	Log	Hit Count
1	port1 → port1 ①										
2	Blocking apps	all	all	always	App Default	Facebook Flickr Instagram Pinterest		DENY	All		0
3	Allow social media	all	all	always	App Default	Social.Media		ACCEPT	default	All	0
4	Blocking P2P Apps	all	all	always	App Default	P2P		DENY		Disabled	0
5	Allow all	all	all	always	App Default			ACCEPT	default	UTM	0

FORTINET

© Fortinet Inc. All Rights Reserved.

35

Regardless of which operation mode application control is configured in, logging must be enabled on the security or firewall policy. When you enable the logging of security events or all session on a security or firewall policy, application control events are also logged. You must apply application control to the security or firewall policy to enable application control event logging.

When the **Deny** action is selected on a security or firewall policy, the **Log Violations** option must be enabled to generate application control events for blocked traffic.

DO NOT REPRINT**© FORTINET**

Logging Application Control Events

- All application control events are logged on the **Application Control** pane on the **Log & Report** page

Log & Report > Application Control

Date/Time	Source	Destination	Application Name	Action
2020/02/21 15:07:18	192.168.10.201	208.91.114.104 (firestore.firebaseio.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:18	192.168.10.201	208.91.114.104 (firestore.firebaseio.com)	HTTPS.BROWSER_Firefox	pass
2020/02/21 15:07:18	192.168.10.201	195.8.215.136 (dailymotion.com)	Dailymotion	block
2020/02/21 15:07:18	192.168.10.201	66.35.172.43 (www.fortiguard.com)	HTTPS.BROWSER_Firefox	pass
2020/02/21 15:07:18	192.168.10.201	195.8.215.136 (dailymotion.com)	Dailymotion	block
2020/02/21 15:07:05	192.168.10.201	69.147.82.60 (beap-bc.yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:04	192.168.10.201	69.147.82.60 (beap-bc.yahoo.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:05	192.168.10.201	66.218.87.15 (gec@yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:05	192.168.10.201	66.218.87.15 (gec@yahoo.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:05	192.168.10.201	192.229.211.35 (o.aecdn.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:05	192.168.10.201	192.229.211.35 (o.aecdn.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:04	192.168.10.201	152.199.24.48 (opus.analytics.yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:04	192.168.10.201	152.199.24.48 (opus.analytics.yahoo.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:04	192.168.10.201	66.218.84.43 (udc@yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:04	192.168.10.201	66.218.84.43 (udc@yahoo.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:04	192.168.10.201	54.173.199.3 (guce.yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:04	192.168.10.201	54.173.199.3 (guce.yahoo.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:01	192.168.10.201	69.147.82.61 (beap-bc.yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:01	192.168.10.201	69.147.82.61 (beap-bc.yahoo.com)	HTTPS.BROWSER	pass
2020/02/21 15:07:01	192.168.10.201	69.147.82.61 (beap-bc.yahoo.com)	Yahoo.Services	pass
2020/02/21 15:07:01	192.168.10.201	69.147.82.61 (beap-bc.yahoo.com)	HTTPS.BROWSER	pass

FORTINET

© Fortinet Inc. All Rights Reserved.

36

All application control events are logged on the **Application Control** pane on the **Log & Report** page. You can view details about individual logs by clicking on the log entry.

In the example shown on this slide, access to **Dailymotion** is blocked using the default application control profile. This information is available in the **Log Details** section, as well as information about the log source, destination, application, and action.

Note that this log message was generated by application control using a profile-based configuration. In an NGFW policy-based configuration, you will not find information such as application sensor name, because it does not apply. The remainder of the information and structure of the log message is the same for each log, regardless of which inspection mode FortiGate is operating in.

You can also view the details on the **Forward Traffic** logs pane. This pane is where firewall policies record activity. You'll also find a summary of the traffic to which FortiGate applied application control. Again, this is because application control is applied by a firewall policy. To find out which policy applied application control, you can review either the **Policy ID** or the **Policy UUID** fields of the log message.

DO NOT REPRINT**© FORTINET**

Application Control Events in Dashboard View

- Application control events are saved in a standalone dashboard on the **Top Applications** dashboard
 - Requires disk logging

Dashboard > Top Applications

Top Applications by Bytes					
Application	Category	Risk	Bytes	Sessions	Bandwidth
SSL	Network.Service	Low	12.29 MB	33	1.11 Mbps
YouTube_HD.Streaming	Video/Audio	Medium	3.94 MB	1	2.47 Mbps
YouTube_Video.Access	Video/Audio	Medium	2.32 MB	1	13.48 kbps
HTTPBROWSER_Firefox	Web.Client	Low	2.15 MB	7	3.64 kbps
Vimeo_Video.Play	Video/Audio	Medium	1.95 MB	2	872.04 kbps
YouTube_Video.Play	Video/Audio	Medium	1.07 MB	3	1.92 Mbps
Vimeo	Video/Audio	Medium	173.10 kB	5	46.79 kbps
LinkedIn	Social.Media	Low	75.13 kB	6	37.69 kbps
Dailymotion	Video/Audio	Low	70.19 kB	1	13.13 kbps
Google.Services	General.Interest	Low	33.66 kB	2	3.67 kbps
Vimeo_Video.Access	Video/Audio	Medium	19.31 kB	1	1.18 kbps
OCSP	Network.Service	Low	7.10 kB	4	1.66 kbps
NTP	Network.Service	Low	152 B	1	16 bps

FORTINET

© Fortinet Inc. All Rights Reserved.

37

On the **Dashboard** menu, the **Top Applications** standalone page provides details about each application, such as the application name, category, and bandwidth. You can drill down further to see more granular details by double-clicking an individual log entry. The detailed view provides information about the source, destination, policies, or sessions for the selected application.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Where do you enable logging of application control events?
 A. Application control logs are enabled in the firewall policy configuration.
 B. Application control logs are enabled on the **FortiView Applications** page of FortiGate.

2. Which piece of information is not included in the application event log when using NGFW policy-based mode?
 A. Application control profile name
 B. Application name



© Fortinet Inc. All Rights Reserved.

38

DO NOT REPRINT

© FORTINET

Lesson Progress



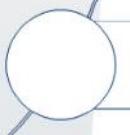
Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

Good job! You now understand application control logging and monitoring.

Now, you will learn about application control best practices and troubleshooting.

DO NOT REPRINT

© FORTINET

Best Practices and Troubleshooting

Objectives

- Recognize best practices for application control configuration
- Understand how to troubleshoot application control update issues

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

By demonstrating competence in application control best practices and troubleshooting, you will be able to configure and maintain an effective application control solution.

DO NOT REPRINT**© FORTINET**

Best Practices for Application Control

- Apply application control to only the traffic that requires it
 - Specify subnets (source, destination, or both) within the firewall policy, whenever possible
 - Don't apply application control to internal-to-internal traffic
- If using load balancing or failover internet connections, apply identical application control on all load balancing or redundant firewall policies
- Select **Deep-Inspection** instead of **Certificate-based** inspection as the SSL/SSH inspection method
- Use a FortiCloud account to save and view application control events in FortiView
 - FortiGate devices that don't have an internal disk for logging require FortiCloud logging to use FortiView
- Use hardware acceleration for application signature matching



© Fortinet Inc. All Rights Reserved.

41

This slide lists some best practices to keep in mind when implementing application control on FortiGate.

Not all traffic requires an application control scan. Don't apply application control to internal-only traffic.

To minimize resource use on FortiGate, be as specific as possible when creating firewall policies. This will not only reduce resource use, it will also help you build a more secure firewall configuration.

Create identical firewall policies for all redundant internet connections, to ensure that the same inspection is performed on failover traffic. Select **Deep-Inspection** instead of **Certificate-based** inspection for the SSL/SSH inspection mode, to ensure content inspection is performed on encryption protocols.

FortiGate models that feature specialized chips, such as network processors and content processors, can offload and accelerate application signature matching for enhanced performance.

You can use a FortiCloud account to save and view application control logs in FortiView, on FortiGate devices that do not have a log disk.

DO NOT REPRINT**© FORTINET**

Application Control Troubleshooting

- If FortiGuard has update issues, make sure that:
 - FortiGate has a stable connection to the Internet
 - FortiGate is able to resolve DNS (update.fortiguard.net)
 - TCP port 443 is open
- Force FortiGate to check for new application control updates:
`execute update-now`
- Verify that the application control signatures database version is up-to-date with the FortiGuard website

System > FortiGuard

FortiGuard Distribution Network	
License Information	
Entitlement	Status
FortiCare Support	Registered -
Enhanced Support	8x5 support - expires on 2020/05/06
Virtual Machine	Valid - expires on 2020/05/06
Allocated vCPUs	100% 1/1



© Fortinet Inc. All Rights Reserved.

42

If you are experiencing issues with a FortiGuard application control update, start troubleshooting the issue with the most basic steps:

- Make sure that FortiGate has a stable connection to the internet or FortiManager (if FortiGate is configured to receive updates from a FortiManager)
- If the internet connection is stable, check DNS resolution on FortiGate
- If FortiGate is installed behind a network firewall, make sure that port 443 is being allowed from FortiGate

You can check the FortiGuard website for the latest version of the application control database. If your locally installed database is out-of-date, try forcing FortiGate to check for the latest updates by running the `execute update-now` command.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which protocol does FortiGate use with FortiGuard to receive updates for application control?
 A. UDP
 B. TCP

2. Which SSL/SSH inspection method is recommended for use with application control scanning to improve application detection?
 A. Certificate-based inspection profile
 B. Deep-inspection profile



© Fortinet Inc. All Rights Reserved.

43

DO NOT REPRINT**© FORTINET**

Lesson Progress



Application Control Basics



Application Control Configuration



Logging and Monitoring Application Control Events



Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

Now, you'll review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Understand application control
- ✓ Detect types of applications
- ✓ Understand FortiGuard application control services
- ✓ Use application control signatures
- ✓ Configure application control in profile mode
- ✓ Configure application control in NGFW policy mode
- ✓ Use the application control traffic shaping policy
- ✓ Enable application control logging events
- ✓ Monitor application control events
- ✓ Use the dashboard to see a detailed view of application control logs
- ✓ Recognize best practices for application control configuration
- ✓ Understand how to troubleshoot application control update issues

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

By mastering the objectives covered in this lesson, you learned how to use methods beyond simply blocking protocols, port numbers, or IP addresses, to monitor and control both standard and non-standard network applications.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

Antivirus

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified 29 May 2020

In this lesson, you will learn how to use FortiGate to protect your network against viruses.

DO NOT REPRINT

© FORTINET

Lesson Overview



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

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

DO NOT REPRINT

© FORTINET

Antivirus Basics

Objectives

- Use antivirus signatures
- Review antivirus scanning techniques
- Enable FortiSandbox with antivirus
- Differentiate between available FortiGuard signature databases

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

By demonstrating competence in antivirus basics, you will be able to understand and apply antivirus on FortiGate.

DO NOT REPRINT

© FORTINET

What is Antivirus and How Does It Work?

- Antivirus is a database of virus signatures that is used to identify malicious code
- Virus names: <vector>/<pattern>
 - Example: W32/Kryptik.EMT!tr
 - <vector> for a virus will always be the same, but vendors assign different IDs for <pattern>
- To detect a virus, the antivirus engine must match file with pattern <signature>
- Each vendor uses different detection engines and signatures, such as:
 - MD5
 - CRC
 - Combinations of file attributes
 - Binary values in some areas
 - Encryption keys
 - Parts of code



© Fortinet Inc. All Rights Reserved.

4

An antivirus is a database of virus signatures that is used to identify infections. During an antivirus scan, in order to be detected as a virus, the virus must match a defined pattern called a *signature*.

Different vendors assign different names to the same virus. All vendors use the attack vector designation in the virus name. The vector comes at the beginning of the virus name. Some examples include:

- W32, which represents 32-bit Windows
- W64, which represents 64-bit Windows
- JS, which represents JavaScript (which is cross-platform)

Some vendors also use a pattern as part of the virus name. Some patterns detect only one virus per pattern. Other patterns are more flexible and can detect multiple viruses per pattern. The pattern that the vendor uses depends on the vendor's engine.

Host-based antivirus software, such as FortiClient, can help at the host level; however, host-based antivirus software cannot be installed on routers. Also, guest Wi-Fi networks and ISP customers might not have antivirus software installed.

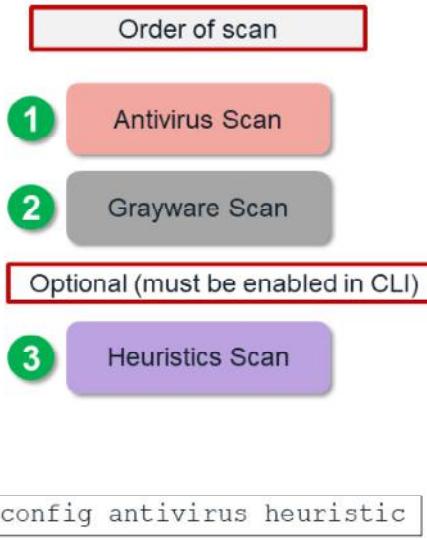
So, how can you protect guest networks, ISP customers, and your own network from malware threats?

DO NOT REPRINT

© FORTINET

Antivirus Scanning Techniques

- Antivirus scan:
 - Detects and eliminates malware in real time
 - Stops threats from spreading
 - Preserves the client reputation of your public IP
- Grayware scan:
 - Uses grayware signatures
 - Detects and blocks unsolicited programs
 - Antivirus actions apply
- Heuristics scan:
 - Looks for virus-like code
 - Example: Modifies registry to restart itself after reboot
 - Counts virus-like attributes
 - If greater than a threshold, file is suspicious
 - False positives possible
 - CLI command to enable
 - Two modes: pass detected file, block detected file



FORTINET

© Fortinet Inc. All Rights Reserved.

5

Like viruses, which use many methods to avoid detection, FortiGate uses many techniques to detect viruses. These detection techniques include:

- Antivirus scan: This is the first, fastest, simplest way to detect malware. It detects viruses that are an exact match for a signature in the antivirus database.
- Grayware scan: This scan detects unsolicited programs, known as grayware, that have been installed without the user's knowledge or consent. Grayware is not technically a virus. It is often bundled with innocuous software, but does have unwanted side effects, so it is categorized as malware. Often, grayware can be detected with a simple FortiGuard grayware signature.
- Heuristics scan: These scans are based on probability, so they increase the possibility of false positives, but they also detect zero-day viruses. Zero-day viruses are viruses that are new, unknown, and, therefore, have no existing associated signature. If your network is a frequent target, enabling a heuristics scan may be worth the performance cost because it can help you to detect a virus before the outbreak begins. By default, when the heuristic engine detects a virus-like characteristic, it logs the file as `Suspicious` but does not block it. You can choose whether to block or allow suspicious files.

The heuristics scan is an optional feature that must be enabled in the CLI. You can configure the action for the heuristic scan to `pass`, `block`, `disable` using the CLI command and by setting the modes to:

- `pass`: Detected files will be passed by FortiGate and will record an event log.
- `block`: Detected files will be blocked by FortiGate and will record an event log.

If all antivirus features are enabled, FortiGate applies the following scanning order: antivirus scan > grayware scan > heuristics scan.

DO NOT REPRINT

© FORTINET

Sandboxing

- FortiSandbox detects zero-day attacks with high certainty:
 - FortiGate uploads files to FortiSandbox Cloud or FortiSandbox Appliance

Note: You must activate a FortiCloud account to use FortiSandbox cloud
 - Uploaded files are executed in an isolated environment (VMs)
 - FortiSandbox examines the effects of the software to detect new malware
- You can configure FortiGate to receive a signature database from FortiSandbox Cloud or FortiSandbox Appliance to supplement the FortiGuard database

FortiSandbox Settings	
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Type	On-Premise
Server	10.0.1.201
Notifier email	admin@fortinet.com



© Fortinet Inc. All Rights Reserved.

6

What if heuristics scans are too uncertain? What if you need a more sophisticated, more certain way to detect malware and find zero-day viruses?

You can integrate your antivirus scans with FortiSandbox. For environments that require more certainty, FortiSandbox executes the file within a protected environment (VMs), then examines the effects of the software to see if it is dangerous.

For example, let's say you have two files. Both alter the system registry and are, therefore, suspicious. One is a driver installation—its behavior is normal—but the second file installs a virus that connects to a botnet command and control server. Sandboxing would reveal the difference.

FortiGate can be configured to receive a supplementary signature database from FortiSandbox based on the sandboxed results.

DO NOT REPRINT

© FORTINET

Sandboxing (Contd)

- Administrators must configure the antivirus profile to send files to FortiSandbox for inspection:
 - You can send all files, or *only files deemed suspicious* to FortiSandbox
 - Characteristics that are used to determine if a file is suspicious are updated by FortiGuard, based on the current threat climate

Security Profile > AntiVirus

Edit AntiVirus Profile
APT Protection Options

Treat Windows Executables in Email Attachments as Viruses

Send Files to FortiSandbox Appliance for Inspection

None	Suspicious Files Only	All Supported Files
<input style="width: 100%; height: 30px; margin-bottom: 5px;" type="button" value="+"/> <input style="width: 100%; height: 30px;" type="button" value="+"/>		

Do not submit files matching types
Do not submit files matching file name patterns

Use FortiSandbox database Allows FortiGate to use FortiSandbox signatures to supplement the FortiGuard antivirus database

Include Mobile Malware Protection

FORTINET

© Fortinet Inc. All Rights Reserved.

FortiOS is smart when it comes to determining what files are sent to FortiSandbox. FortiGuard provides FortiGate with information, based on the current threat climate, that is used to determine if a file should be deemed suspicious or not. FortiGate provides the administrator with granular control when it comes to determining what type of files are sent to FortiSandbox for further investigation. Administrators also have the option to use the FortiSandbox database in conjunction with the FortiGuard AV database to enhance their network security.

DO NOT REPRINT

© FORTINET

Antivirus Signature Database

- Requires a subscription to FortiGuard AntiVirus

System > FortiGuard

System > FortiGuard

AntiVirus	Licensed - expires on 2020/05/06
AV Definitions	Version 1.00000
AV Engine	Version 6.00132
Mobile Malware	Version 0.00000

Upgrade Database

- The antivirus scanning engine relies on the antivirus signature database
- The Mobile Malware subscription is part of the FortiGuard Antivirus license now
- Verify signatures versions on GUI or CLI commands

```
# diagnose autoupdate status
# diagnose autoupdate versions
```

FORTINET

© Fortinet Inc. All Rights Reserved.

8

You can update the antivirus database using the push method, schedule method, or both methods. Scheduled updates allow you to configure scheduled updates at regular intervals, such as hourly, daily, or weekly. You can also enable **Accept push updates**, which allows you to add new definitions as soon as they are released by FortiGuard. This is useful for high-security environments, because FortiGate will receive urgent security updates as soon as they are released.

Regardless of which method you select, you *must* enable virus scanning in at least one firewall policy. Otherwise, FortiGate will not download any updates. Alternatively, you can download packages from the Fortinet customer service and support website (requires subscription), and then manually upload them to your FortiGate. You can verify the update status and signature versions from the **FortiGuard** page on the GUI or using the CLI console.

DO NOT REPRINT**© FORTINET**

Antivirus Signature Database (Contd)

- FortiGuard antivirus databases:
 - Extended: Includes common and additional recent non-active viruses
 - Available on all models
 - The default antivirus database setting
 - Extreme: Includes extended plus additional dormant viruses
 - Extreme is only available on select FortiGate models
- Choosing an antivirus signature database (CLI only)

```
config antivirus settings
    set use-extreme-db {enable | disable}
end
```

**FORTINET**

© Fortinet Inc. All Rights Reserved.

9

Multiple FortiGuard antivirus databases exist, which you can configure using CLI commands. Support for each database type varies by FortiGate model.

All FortiGate devices include the extended database. The extended database contains signatures for viruses that have been detected in recent months, as identified by the FortiGuard Global Security Research Team. The extended database also detects viruses that are no longer active.

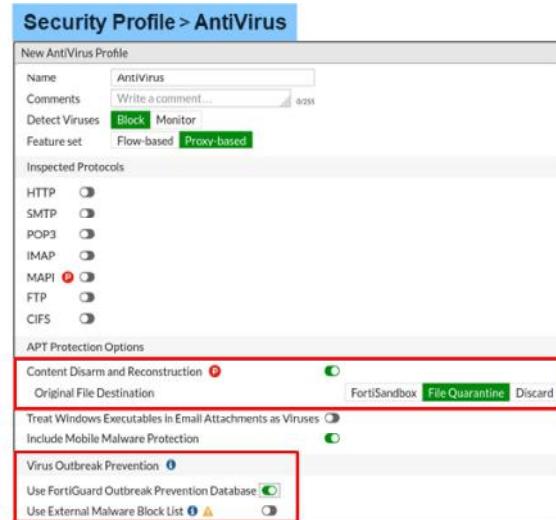
The extreme database is intended for use in high-security environments. The extreme database detects all known viruses, including viruses targeted at legacy operating systems that are no longer widely used. Most FortiGate models support the extreme database.

DO NOT REPRINT

© FORTINET

FortiGuard Protection Services

- Content disarm and reconstruction
 - CDR removes exploitable content and replaces it with content that's known to be safe
- Virus outbreak prevention
 - Additional layer of protection that keeps your network safe from newly emerging malware
 - Quick virus outbreaks can infect a network before signatures can be developed to stop them
 - Outbreak protection stops these virus outbreaks until signatures become available in FortiGuard
- Malware block list
 - Manual external malware signatures to support antivirus database
 - The block list can be in the form of MD5, SHA1, and SHA256 hashes
 - Defined as a Security Fabric connector



FORTINET

© Fortinet Inc. All Rights Reserved.

10

Content disarm and reconstruction (CDR): The CDR removes exploitable content and replaces it with content that's known to be safe. As files are processed through an enabled antivirus profile, content that's found to be malicious or unsafe is replaced with content that allows the traffic to continue, but doesn't put the recipient at risk. Content that can be scanned includes PDF and Microsoft Office files leaving the network on CDR-supported protocols (such as HTTP, SMTP, IMAP, and POP3—MAPI isn't supported). When the client tries to download the file, FortiGate removes all exploitable content in real-time, then the original file is sent to FortiSandbox for inspection. The client can download the original file by logging in to the FortiSandbox.

Virus outbreak prevention: An additional layer of protection that keeps your network safe from newly emerging malware. Quick virus outbreaks can infect a network before signatures can be developed to stop them. Outbreak protection stops these virus outbreaks until signatures become available in FortiGuard. FortiGate must have a Zero-Hour Virus Outbreak (ZHO) license. FortiGate adds hash-based virus detection for new threats that are not yet detected by the antivirus signatures. When the file is sent to the scanunit deamon, buffers are hashed and a request is sent to the urlfilter deamon. After checking against its request cache for known signatures, the urlfilter deamon sends an antivirus request to FortiGuard with the remaining signatures. FortiGuard returns a rating that is used to determine if the scanunit deamon should report the file as harmful or not. Jobs remain suspended in the scanunit deamon until the client receives a response, or the request times out.

Malware block list: FortiGate can enhance the antivirus database by linking a dynamic external malware block list to FortiGate. The list is hosted on a web server and is available through HTTP/HTTPS URL defined within the Security Fabric malware hash list. The list can be in the forms of MD5, SHA1, and SHA256 hashes, and are written on separate lines on a plaintext file. The malware block list can be defined as a Security Fabric connector and configured to pull the list dynamically by setting the refresh rate.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. If antivirus, grayware, and heuristic scans are enabled, in what order are they performed?
 - A. Heuristic scan, followed by grayware scan, followed by antivirus scan
 - B. Antivirus scan, followed by grayware scan, followed by heuristic scan

2. Which databases can be manually selected for use in antivirus scanning?
 - A. Extended and Extreme
 - B. Quick, Normal, and Extreme



© Fortinet Inc. All Rights Reserved.

11

DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand the basics of antivirus functionality.

Now, you will learn about antivirus scanning modes.

DO NOT REPRINT

© FORTINET

Antivirus Scanning Modes

Objectives

- Apply the antivirus profile in flow-based inspection mode
- Apply the antivirus profile proxy inspection mode
- Compare all available scanning modes

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

By demonstrating competence in all antivirus scanning modes available in FortiOS, you will be able to use the antivirus profile in an effective manner.

DO NOT REPRINT

© FORTINET

Flow-Based Inspection Mode

- Uses the extended antivirus database by default
 - Extreme database on certain FortiGate models—depending on the CLI settings
- Optimized performance compared to proxy-based scan
 - Uses a hybrid of advanced scan modes available only in proxy-based profiles
 - Proxy-based offers two scanning modes: default scanning and legacy scanning
 - Flow-based is designed to use a hybrid of proxy-based scanning modes
- FortiGate buffers the whole file, but transmits to the client simultaneously
 - When the *last* packet arrives, the AV engine starts the scan
 - Files bigger than buffer size are not scanned—can enable logging of these files
 - Packets are not delayed by scan—*except last packet*
 - Lower perceived latency—data loads faster
- If a virus is detected, the last packet is dropped and the connection is reset
- If an identical request is made, the block replacement page is inserted immediately



© Fortinet Inc. All Rights Reserved.

14

AV can operate in flow-based or proxy-based inspection mode, both of which use the full AV database (extended or extreme—depending on the CLI settings) and the IPS engine to examine network traffic.

Flow-based inspection mode uses a hybrid of the scanning modes available in proxy-based inspection: the default scanning mode and the legacy scanning mode. The default mode enhances the scanning of nested archive files without buffering the container archive file. The legacy mode buffers the full container, and then scans it.

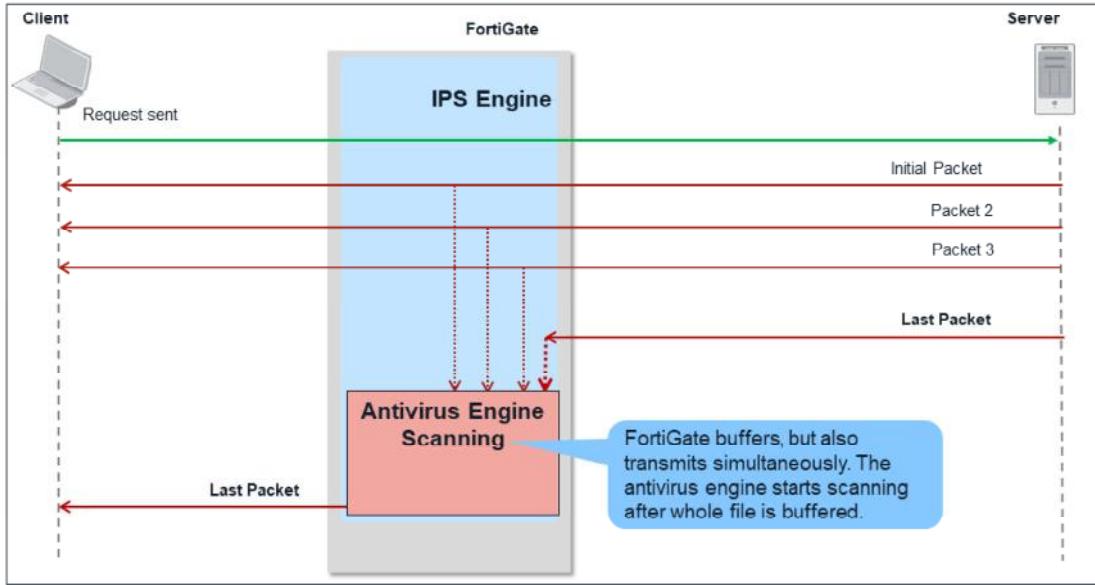
In flow-based inspection mode, the IPS engine reads the payload of each packet, caches a local copy, and forwards the packet to the receiver at the same time. Because the file is transmitted simultaneously, flow-based mode consumes more CPU cycles than proxy-based. However, depending on the FortiGate model, some operations can be offloaded to SPUs to improve performance. When FortiGate receives the last packet of the file, it puts the packet on hold and sends a copy to the IPS engine. The IPS engine extracts the payload and assembles the whole file, and then sends the whole file to the AV engine for scanning.

Two possible scenarios can occur when a virus is detected:

- When a virus is detected on a TCP session where some packets have been already forwarded to the receiver, FortiGate resets the connection and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a second attempt to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
- If the virus is detected at the start of the connection, the IPS engine sends the block replacement message immediately.

DO NOT REPRINT**© FORTINET**

Flow-Based Inspection Mode Packet Flow

**FORTINET**

© Fortinet Inc. All Rights Reserved.

15

As you can see on this slide, the client sends a request and starts receiving packets immediately, but FortiGate also caches those packets at the same time. When the last packet arrives, FortiGate caches it and puts it on hold. Then, the IPS engine extracts the payload of the last packet, assembles the whole file, and sends it to the antivirus engine for scanning. If the antivirus scan does not detect any viruses, and the result comes back clean, the last cached packet is regenerated and delivered to the client. However, if a virus is found, the last packet is dropped. Even if the client has received most of the file, the file will be truncated and the client will be not able to open a truncated file.

Regardless of which mode you use, the scan techniques give similar detection rates. How can you choose between the scan engines? If performance is your top priority, then flow inspection mode is more appropriate. If security is your priority, proxy inspection mode—with client comforting disabled—is more appropriate.

DO NOT REPRINT**© FORTINET**

Flow-Based Inspection Mode

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Detect Viruses: **Block** Monitor

Feature set: **Flow-based** Proxy-based

Inspected Protocols:

- HTTP
- SMTP
- POP3
- IMAP
- FTP
- CIFS

APT Protection Options

- Treat Windows Executables in Email Attachments as Viruses
- Include Mobile Malware Protection
- Virus Outbreak Prevention
- Use FortiGuard Outbreak Prevention Database
- Use External Malware Block List ⚠

© Fortinet Inc. All Rights Reserved.

16

This slide shows an example of the **AntiVirus Profile** operating in flow-based inspection mode. By default, **Feature set** is set to **Flow-based**.

DO NOT REPRINT**© FORTINET**

Proxy Inspection Mode

- Uses extended or extreme antivirus database
- Buffers the whole file
 - Antivirus engine starts scanning after the end of the file is detected
 - Files bigger than buffer size are not scanned—can configure to pass or block
 - Packets sent to the client after scan finishes—*client must wait*
 - Highest perceived latency
- Provides granularity over performance
- Weighted towards being more thorough and easily configurable
- Displays block message immediately if virus is detected



© Fortinet Inc. All Rights Reserved.

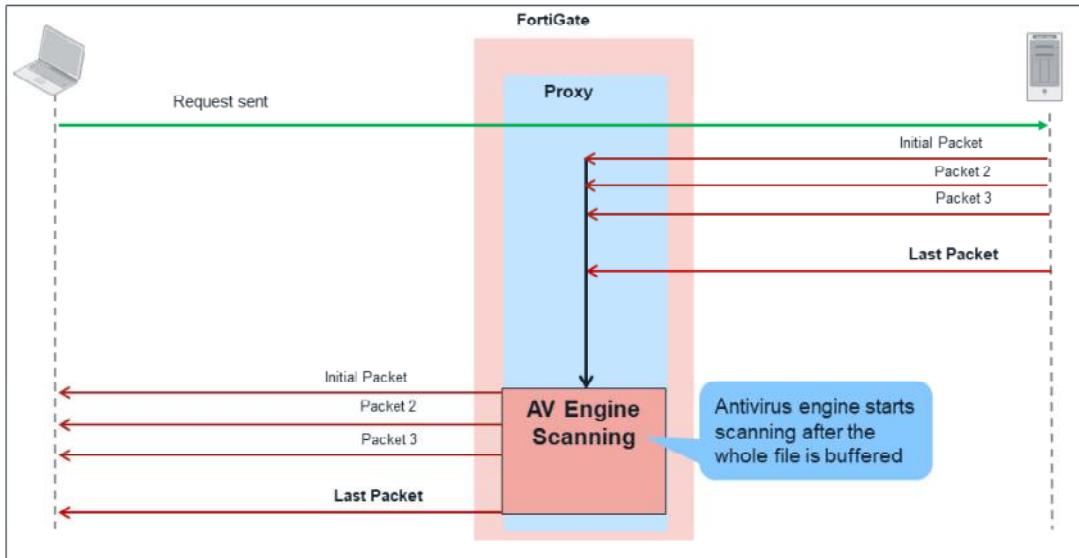
17

Each protocol's proxy picks up a connection and buffers the entire file first (or waits until the oversize limit is reached) before scanning. The client must wait for the scanning to finish. If the virus is detected, the block replacement page is displayed immediately. Because FortiGate has to buffer the whole file and then do the scanning, it takes a long time to scan. Also, from the client point of view, it has to wait for the scanning to finish and might terminate the connection due to lack of data.

You can configure client comforting for HTTP and FTP from the `config firewall profile-protocol-options` command tree. This allows the proxy to slowly transmit some data until it can complete the buffer and finish the scan. This prevents a connection or session timeout. No block replacement message appears in the first attempt, as FortiGate is transmitting the packets to the end client.

DO NOT REPRINT**© FORTINET**

Proxy Inspection Mode Packet Flow

**FORTINET**

© Fortinet Inc. All Rights Reserved.

18

With a proxy inspection mode scan, the client sends a request and FortiGate starts buffering the whole file, then sends it to the antivirus engine for scanning. If the file is clean (without any viruses), FortiGate starts transmitting the file to the end client. If a virus is found, no packets are delivered to the end client and the proxy sends the replacement block message to the end client.

DO NOT REPRINT

© FORTINET

Proxy Inspection Mode Enabled

- Configure the antivirus profile
 - Feature set is Proxy-based**
- Provides additional antivirus support
 - MAPI protocol inspection
 - Content disarm and reconstruction (CDR)

Policy & Objects > Firewall Policy

Inspection Mode Flow-based **Proxy-based**

- Proxy-based antivirus profiles
 - Only available if inspection mode is proxy-based
 - Can use flow-based antivirus profiles

Security Profiles > AntiVirus

New AntiVirus Profile	
Name	AV Proxy
Comments	Write a comment... 0/255
Detect Viruses	<input checked="" type="radio"/> Block <input type="radio"/> Monitor
Feature set	<input type="radio"/> Flow-based <input checked="" type="radio"/> Proxy-based
Inspected Protocols	
HTTP	<input type="radio"/>
SMTP	<input type="radio"/>
POP3	<input type="radio"/>
IMAP	<input type="radio"/>
MAPI	<input checked="" type="radio"/>
FTP	<input type="radio"/>
CIFS	<input type="radio"/>
APT Protection Options	
Content Disarm and Reconstruction	<input type="radio"/>
Treat Windows Executables In Email Attachments as Viruses	<input type="radio"/>
Include Mobile Malware Protection	<input checked="" type="radio"/>
Virus Outbreak Prevention	<input type="radio"/>
Use FortiGuard Outbreak Prevention Database	<input type="radio"/>
Use External Malware Block List	<input type="radio"/>

FORTINET

© Fortinet Inc. All Rights Reserved.

19

Applying a proxy-based antivirus profile requires two sections in FortiGate configuration to use non-default settings:

1. Antivirus profile
2. Firewall policy

Antivirus profile provides the option to select a proxy-based approach as the inspection mode within the profile. This allows the profile to inspect MAPI protocol traffic, as well as to sanitize Microsoft documents and PDF files using the content disarm and reconstruction (CDR) feature.

If the inspection mode on the antivirus profile is set as **Proxy-based**, it is only available when the firewall policy inspection mode is set to **Proxy-based**.

DO NOT REPRINT**© FORTINET**

Antivirus Scanning Modes Comparison

	Flow-based (hybrid)	Proxy-based
Catching Rate	Highest	Highest
Sandbox Support	Yes	Yes
Advanced Heuristic	Yes	Yes
Memory	High	High
Perceived Latency	High	Highest
MAPI, NNTP Scanning	No	Yes
SMB Scanning	Yes	No
HTTP, FTP, IMAP, POP3, SMTP Scanning	Yes	Yes
Use FortiSandbox Database	Yes	Yes
Use Mobile Malware Protection Service	Yes	Yes



© Fortinet Inc. All Rights Reserved.

20

This slide provides comparison of the different antivirus scanning modes.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What two additional features of an antivirus profile are available in proxy-based inspection mode?
 A. MAPI inspection and CDR
 B. Full and quick

2. What antivirus database is limited to specific FortiGate models?
 A. Extended
 B. Extreme



© Fortinet Inc. All Rights Reserved.

21

DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand antivirus scanning modes.

Now, you will learn about antivirus configuration.

DO NOT REPRINT

© FORTINET

Configuring Antivirus

Objectives

- Configure antivirus profiles
- Configure protocol options
- Review virus statistics
- Log and monitor antivirus events

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

By demonstrating competence in antivirus configuration, including reviewing antivirus logs, you will be able to use the antivirus profile in an effective manner.

DO NOT REPRINT

© FORTINET

Configuring Antivirus Profiles

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default
Comments: Scan files and block viruses. 29/255

Detect Viruses: Block Monitor

Feature set: Flow-based Proxy-based

Default inspection mode is flow. Inspection mode is now per policy.

Inspected Protocols:

- HTTP:
- SMTP:
- POP3:
- IMAP:
- FTP:
- CIFS:

APT Protection Options:

- Treat Windows Executables in Email Attachments as Viruses:
- Send Files to FortiSandbox Appliance for Inspection:
 - Do not submit files matching types:
 - Do not submit files matching file name patterns:
- Use FortiSandbox database:
- Include Mobile Malware Protection:
- Virus Outbreak Prevention:
- Use FortiGuard Outbreak Prevention Database:
- Use External Malware Block List:

config firewall policy
edit <policy_id>
set inspection-mode [proxy | flow]
end

FortiSandbox-related options are available only if FortiGate is configured to use FortiSandbox Cloud or Appliance under Security Fabric.

External Malware Block List can be enabled if an external threat feed security fabric is configured.

- Configure all required antivirus profile options

FORTINET

© Fortinet Inc. All Rights Reserved.

24

The antivirus profile can be configured on the **AntiVirus** page. Since the default inspection mode on a firewall policy is flow-based, **Feature set** is required to be set to **Flow-based**. If the inspection mode of the firewall policy is proxy-based, **Feature set** can be set to **Proxy-based**, which allows specific functions that are only available using proxy-based inspection mode firewall policy such as MAPI protocol and CDR.

Both feature sets provide the following options:

APT (Advanced Persistent Threats) Protection Options:

- Treat Windows Executables in Email Attachment as Viruses:** By default, this option is enabled and files (including compressed files) identified as Windows executables can be treated as viruses.
- Send Files to FortiSandbox Appliance for Inspection:** If FortiSandbox Cloud or Appliance is configured, you can configure the antivirus profile to send malicious files to FortiSandbox for behaviour analysis. If tagged as malicious, any future files matching the same behavior will be blocked if **Use FortiSandbox Database** is enabled.

Virus Outbreak Prevention:

- Use FortiGuard Virus Outbreak Prevention Database:** FortiGuard virus outbreak prevention is an additional layer of protection that keeps your network safe from newly emerging malware. Quick virus outbreaks can infect a network before signatures can be developed to stop them. Outbreak protection stops these virus outbreaks until signatures become available on FortiGuard.
- Use External Malware Block List:** FortiGate can enhance the antivirus database by linking a dynamic external malware block list to FortiGate. Malware block list can be defined as a Security Fabric connector and configured to pull the list dynamically by setting the refresh rate.

In the antivirus profile, you can define what FortiGate should do if it detects an infected file. After you configure an antivirus profile, you must apply it in the firewall policy.

DO NOT REPRINT

© FORTINET

Configuring Protocol Options

- More granular control
- Allows configuration of:
 - Protocol port mappings
 - Common options
 - Web and email options
- Configure for both proxy-based and flow-based firewall policies
 - From the GUI, on the **Protocol Options** page
 - From the CLI, using the `config firewall profile-protocol-options` command

```
config firewall profile-protocol-options
edit <profile_name>
config <protocol_name>
```

Policy & Objects > Protocol Options

Edit Protocol Options		
Name	protocol_profile	
Comments	All default services. 25/255	
Log oversized files	<input type="checkbox"/>	
RPC over HTTP	<input type="checkbox"/>	
Feature set	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based	
Protocol Port Mapping		
HTTP	any	Specify 80
SMTP	any	Specify 25
POP3	any	Specify 110
IMAP	any	Specify 143
FTP	any	Specify 21,222,23
NNTP	any	Specify 119
MAPI	135	
DNS	53	
CIFS	445	
Common Options		
Comfort Clients	<input type="checkbox"/>	
Block oversized file/email	<input type="checkbox"/>	
Web Options		
Chunked Bypass	<input type="checkbox"/>	
Email Options		
Allow Fragmented Messages	<input checked="" type="checkbox"/>	
Append Signature (SMTP)	<input type="checkbox"/>	

You can specify more than one port number (separated by comma)

© Fortinet Inc. All Rights Reserved.

25

FORTINET

Protocol options provide more granular control than antivirus profiles. You can configure protocol port mappings, common options, web options, and email options, to name a few.

By default, **Feature set** is set to **Flow-based**. It can be set to **Proxy-based**, which allows a function to add a Fortinet bar for the purpose of presenting the countdown for FortiGuard quotas, and is only available on firewall policy using proxy-based inspection mode.

You can configure protocol options on the **Proxy Options** page on the GUI or from the CLI. Protocol options are used by antivirus and other security profiles, such as web filtering, DNS filtering, and data loss prevention (DLP), to name a few.

Once protocol options are configured, they are applied in the firewall policy.

DO NOT REPRINT**© FORTINET**

Protocol Options—Large Files

- By default, FortiOS allows files that are too big for the buffer size
 - Files that are bigger than oversize limit are bypassed from scanning
- You can modify this behavior for all protocols

```
config firewall profile-protocol-options
edit <profile name>
config <protocol name>
set options oversize
set oversize-limit <integer>
end
end
```

HTTP, FTP, and so on
Default value is 10 MB.
Maximum value is hardware dependant.

- You can enable logging of oversize files using CLI

```
config firewall profile-protocol-options
edit <profile_name>
set oversize-log {enable|disable}
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

26

So what is the recommended buffer limit? It varies by model and configuration. You can adjust the oversize-limit for your network for optimal performance. A smaller buffer minimizes proxy latency (for both scanning modes) and RAM usage, but that may allow viruses to pass through undetected. When a buffer is too large, clients may notice transmission timeouts. You need to balance the two.

If you aren't sure about the value to set oversize-limit to, you can temporarily enable oversize-log to see if your FortiGate is scanning large files frequently. You can then adjust the value accordingly.

Files that are bigger than the oversize limit are bypassed from scanning. You can enable logging of oversize files by enabling the oversize-log option from the CLI.

DO NOT REPRINT**© FORTINET**

Protocol Options—Compressed Files

- Often, compression algorithms can be identified using header only
- Archives are unpacked and files and archives within are scanned separately
 - Nested archives are supported (default is 12 layers)
 - Supported formats: zip, tar, gzip, rar, lzh, cab, arj, msc, bzip, bzip2, 7z, egg, xz, cpio, ar, ace, iso, daa, crx, and chm
 - Decompressed files have a separate oversize limit
 - Limit can be configured for each protocol separately

```
config firewall profile-protocol-options
edit <profile_name>
config <protocol_name>
set uncompressed-oversize-limit [1-<model_limit>]
set uncompressed-nest-limit [1-<model_limit>]
end
end
```

HTTP, FTP, and so on

- Password-protected archives cannot be decompressed
- Increasing the size will increase memory usage!

FORTINET

© Fortinet Inc. All Rights Reserved.

27

Large files are often compressed. When compressed files go through scanning, the compression acts like encryption: the signatures won't match. So, FortiGate must decompress the file in order to scan it.

Before decompressing a file, FortiGate must first identify the compression algorithm. Some archive types can be correctly identified using only the header. Also, FortiGate must check whether the file is password protected. If the archive is protected with a password, FortiGate can't decompress it, and, therefore, can't scan it.

FortiGate decompresses files into RAM. Just like other large files, the RAM buffer has a maximum size. Increasing this limit may decrease performance, but it allows you to scan larger compressed files.

If an archive is nested—for example, if an attacker is trying to circumvent your scans by putting a zip file inside the zip file—FortiGate will try to undo all layers of compression. By default, FortiGate will attempt to decompress and scan up to 12 layers deep, but you can configure it to scan up to the maximum number supported by your device (usually 100). Often, you shouldn't increase this setting because it increases RAM usage.

DO NOT REPRINT**© FORTINET**

Detection Rate and File Size

- Most malware is small
- Very large files require more RAM to scan completely
- Often, scanning only small files is an acceptable risk
 - Default: 10 MB threshold for oversize
 - Maximum size varies by model

Malware Type	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB	∞
Exploit	99.83%	99.95%	99.97%	99.97%	99.98%	99.98%	99.99%	100%	100%	100%	100%
Mass-mailer	99.62%	99.87%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Phish	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Spyware	95.08%	97.97%	98.88%	99.47%	99.76%	99.83%	99.89%	99.91%	99.94%	99.95%	100%
Trojan	97.52%	99.24%	99.62%	99.80%	99.88%	99.93%	99.95%	99.97%	99.98%	99.98%	100%
Virus	98.27%	99.37%	99.63%	99.80%	99.88%	99.93%	99.95%	99.97%	99.98%	99.99%	100%
worm	99.08%	99.65%	99.74%	99.86%	99.89%	99.92%	99.94%	99.94%	99.95%	99.96%	100%

FORTINET

© Fortinet Inc. All Rights Reserved.

28

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold.

Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM—something that no device has in the real world.

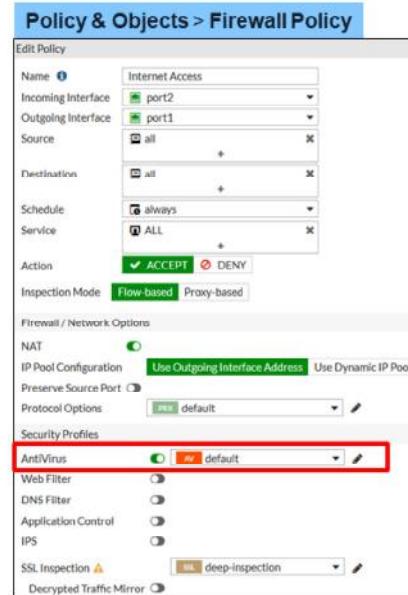
Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

DO NOT REPRINT

© FORTINET

Applying the Antivirus Profile

- Apply the antivirus profile and protocol options on the firewall policy, to scan traffic
- Ensure that **deep-inspection** is selected for the **SSL/SSH Inspection** setting—required to scan encrypted protocols



FORTINET

© Fortinet Inc. All Rights Reserved.

29

Before FortiGate devices can start scanning traffic for malware, you need to apply the antivirus profile, the protocol options, and SSL/SSH inspection profiles on the firewall policy.

In full SSL inspection level, FortiGate terminates the SSL/TLS handshake at its own interface, before it reaches the server. When certificates and private keys are exchanged, it is with FortiGate and not the server. Next, FortiGate starts a second connection with the server.

Because traffic is unencrypted while passing between its interfaces, FortiGate can inspect the contents and look for matches with the antivirus signature database, before it re-encrypts the packet and forwards it.

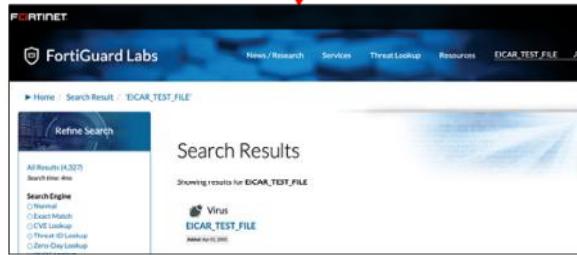
For these reasons, full SSL inspection level is the only choice that allows antivirus to be effective.

DO NOT REPRINT

© FORTINET

Antivirus Block Page

- Antivirus block page contains:
 - File name
 - Virus name
 - Website host and URL
 - Use name and group (if authentication is enabled)
 - Link to FortiGuard Encyclopedia



FORTINET

© Fortinet Inc. All Rights Reserved.

30

For antivirus scanning in proxy-based inspection mode (with client comforting disabled), the block replacement page is displayed *immediately* when a virus is detected.

For flow-based inspection mode scanning, if a virus is detected at the start of the stream, the block replacement page is displayed at the *first attempt*. If a virus is detected after a few packets have been transmitted, the block replacement page is *not* displayed. However, FortiGate caches the URL and can display the replacement page immediately, on the second attempt.

Note that if deep inspection is enabled, all HTTPS-based applications also display the block replacement message.

The block page includes the following:

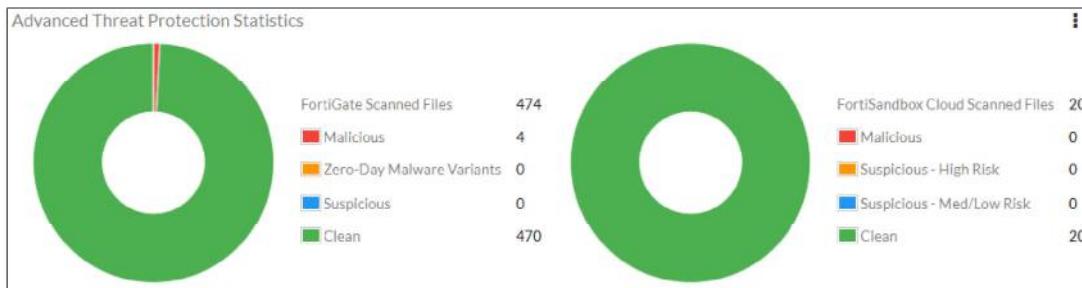
- File name
- Virus name
- Website host and URL
- User name and group (if authentication is enabled)
- Link to FortiGuard Encyclopedia—which provides analysis, recommended actions (if any), and detection availability

You can go directly to the FortiGuard website to view information about other malware, and scan, submit, or do both, with a sample of a suspected malware.

DO NOT REPRINT**© FORTINET**

Advanced Threat Protection Statistics

- The **Advanced Threat Protection Statistics** widget provides real-time statistics related to antivirus scans
- Shows statistics for:
 - Virus scan
 - FortiSandbox



© Fortinet Inc. All Rights Reserved.

31

You can find virus scanning statistics on the **Advanced Threat Protection Statistics** widget on the dashboard.

If your FortiGate is submitting files for sandboxing, it keeps statistics about the number of files submitted and the results of those scans. These statistics are separate from files that are scanned locally on FortiGate.

DO NOT REPRINT

© FORTINET

Antivirus Logs

Log & Report > AntiVirus

Date/Time	%	Service	Source	File Name	Virus/Botnet	User	Details	Action
2020/03/03 10:58:29		HTTPS	192.168.10.201	eicar.com	EICAR_TEST.FILE		URL: https://secure.eicar.org/eicar.com	blocked
2020/03/03 10:58:32		HTTPS	192.168.10.201	eicar.com.zip	EICAR_TEST.FILE		URL: https://secure.eicar.org/eicar.com.zip	blocked
2020/03/03 10:58:32		HTTPS	192.168.10.201	eicar.com.zip	EICAR_TEST.FILE		URL: https://secure.eicar.org/eicar.com.zip	blocked
2020/03/03 10:58:24		HTTPS	192.168.10.201	eicar.com.txt	EICAR_TEST.FILE		URL: https://secure.eicar.org/eicar.com.txt	blocked
2020/03/03 10:58:16		HTTPS	192.168.10.201	eicar.com	EICAR_TEST.FILE		URL: https://secure.eicar.org/eicar.com	blocked
2020/03/03 18:38:09		HTTP	192.168.10.201	eicarcom2.zip	EICAR_TEST.FILE		URL: http://205.8.eicar.org/download/eicarcom2.zip	blocked
2020/03/03 18:38:06		HTTP	192.168.10.201	eicar.com.zip	EICAR_TEST.FILE		URL: http://205.8.eicar.org/download/eicar.com.zip	blocked
2020/03/03 18:38:03		HTTP	192.168.10.201	eicar.com.txt	EICAR_TEST.FILE		URL: http://205.8.eicar.org/download/eicar.com.txt	blocked
2020/03/02 18:23:53		HTTP	192.168.10.201	eicar.com	EICAR_TEST.FILE		URL: http://205.8.eicar.org/download/eicar.com	blocked

Log & Report > Forward Traffic

Date/Time	Source	Destination	Security Events	Result	Policy
2020/03/03 11:17:11	192.168.10.201	194.124.10.114 [internetport.gprod.mozilla.net]	✓ 1.07 kB / 1.17 kB	Internet Access (I)	
2020/03/03 11:17:11	192.168.10.201	194.124.10.114 [internetport.gprod.mozilla.net]	✓ 1.40 kB / 1.47 kB	Internet Access (I)	
2020/03/03 11:16:17	192.168.10.201	35.160.101.217 [httpwww.services.mozilla.com]	✓ 2.86 kB / 4.80 kB	Internet Access (I)	
2020/03/03 11:19:47	192.168.10.201	184.8.84.243.40 [http://prod-f8-pump.apple.com.akadns.net]	✓ 429 B / 1.34 kB	Internet Access (I)	
2020/03/03 11:19:47	192.168.10.201	184.8.84.242.215 [http://prod-f8-pump.apple.com.akadns.net]	✓ 429 B / 1.34 kB	Internet Access (I)	
2020/03/03 11:19:47	192.168.10.201	184.8.84.243.40 [http://prod-f8-pump.apple.com.akadns.net]	✓ 429 B / 1.34 kB	Internet Access (I)	
2020/03/03 11:05:58	192.168.10.201	52.89.36.130 [services.mozilla.net.mozilla.org]	✓ 1.47 kB / 1.47 kB	Internet Access (I)	
2020/03/03 11:05:58	192.168.10.201	99.88.36.130 [http://settings.services.mozilla.com]	✓ 2.47 kB / 14.79 kB	Internet Access (I)	
2020/03/03 11:05:58	192.168.10.201	52.89.36.130 [services.mozilla.net.mozilla.org]	✓ 1.44 kB / 1.44 kB	Internet Access (I)	
2020/03/03 11:01:33	192.168.10.201	52.25.6.89 [queryingentity.mozilla.org]	Deny UTM Blocked	Internet Access (I)	
2020/03/03 11:01:33	192.168.10.201	213.211.19.89 [secure.eicar.org]	Drop UTM Blocked	Internet Access (I)	
2020/03/03 11:01:33	192.168.10.201	69.147.82.61 [http://pypg.tyshooters.net]	UTM Allowed	Internet Access (I)	

Log Details

IP: 192.168.10.201
Source Port: 54385
Source Interface: port2
User:

Destination

IP: 213.211.19.89
Port: 443
Destination Interface: port1
URL: https://secure.eicar.org/eicar.com

Application Control

Data

File Name: eicar.com

Action

Action: blocked
Threat: 2
Policy: 1

Security

Level: Critical
Threat Level: Critical
Threat Score: 50

Cellular

AntiVirus

Profile Name: default
Virus/Botnet: EICAR_TEST_FILE
Virus ID: 2172
Reference: http://www.fortinet.com/v?vn=EICAR_TE
Detection: Virus
Type: Virus
Direction: incoming
Quarantine: Skip
FortiSandbox: 275a02100fb6489e54d471899f7d9916c
Checksum:
Submitted to FortiSandbox: false

FORTINET

© Fortinet Inc. All Rights Reserved.

32

If you enable logging, you can find details on the **AntiVirus** log page.

When the antivirus scan detects a virus, by default, it creates a log about what virus was detected, as well as the action, policy ID, antivirus profile name, and detection type. It also provides a link to more information on the FortiGuard website.

You can also view log details on the **Forward Traffic** log page, where firewall policies record traffic activity. You'll also find a summary of the traffic on which FortiGate applied an antivirus action.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the default scanning behavior for files over 10 MB?

- A. Allow the file without scanning
- B. Block all large files that exceed the buffer threshold



© Fortinet Inc. All Rights Reserved.

33

DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand antivirus configuration.

Now, you will learn about some antivirus best practices.

DO NOT REPRINT

© FORTINET

Best Practices

Objectives

- Recognize recommended antivirus configuration practices
- Log antivirus events
- Monitor antivirus and FortiSandbox events
- Use hardware acceleration with antivirus scans

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

By demonstrating competence in antivirus best practices, you will be able to configure an effective antivirus solution.

DO NOT REPRINT**© FORTINET**

Recommended Configuration Practices

- Perform antivirus scan on all internet traffic
 - If using load balancing or redundant internet connections, ensure all internal to external firewall policies have antivirus profiles applied on them
- Use *deep-inspection* instead of *certificate-based* inspection, to ensure that full content inspection is performed
- Use FortiSandbox Cloud or a FortiSandbox device to enable sandboxing support
 - Configure the antivirus profile to use the FortiSandbox database
- Do not increase the maximum file size to be scanned, unless it is required
 - Viruses usually travel in small files
 - More scanning means more memory utilization



© Fortinet Inc. All Rights Reserved.

36

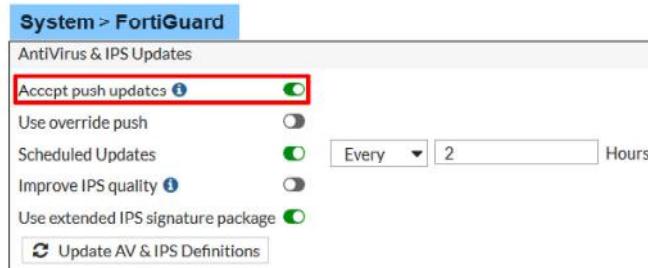
The following are some best practices to follow when configuring antivirus scanning for use on FortiOS:

- Enable antivirus scanning on all internet traffic.
This includes internal to external firewall policies, and any VIP firewall policies.
- Use *deep-inspection* instead of *certificate-based* inspection, to ensure that full content inspection is performed.
- Use FortiSandbox for protection against new viruses.
- Do not increase the maximum file size to be scanned, unless there is good reason, or you need to do so in order to meet a network requirement.

DO NOT REPRINT**© FORTINET**

Recommended Configuration Practices

- Enable FortiGuard push updates to ensure FortiGate receives antivirus updates as soon as they are available



- Make sure FortiGate has a stable connection to FortiGuard servers

FORTINET

© Fortinet Inc. All Rights Reserved.

37

Additional best practices to follow when configuring antivirus scanning include the following:

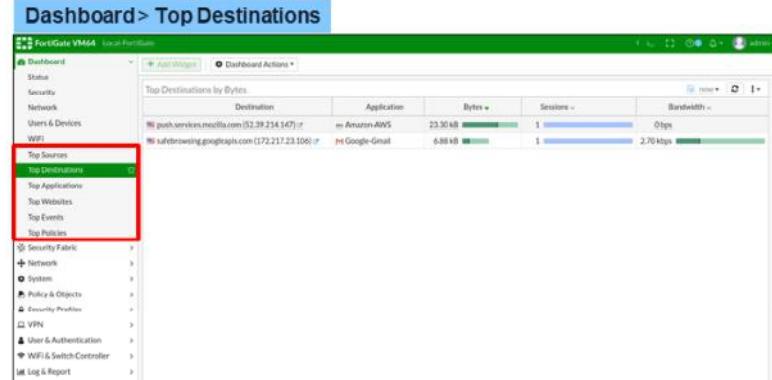
- Enable FortiGuard push updates to ensure that FortiGate receives antivirus updates as soon as they are available.
This will help keep the FortiGate database up-to-date and offer protection against new viruses.
- Ensure that FortiGate has a stable connection to FortiGuard servers.

DO NOT REPRINT

© FORTINET

Log Antivirus Events

- Enable logging of oversized files
 - This will ensure that files that are not scanned are *logged*
- Ensure that firewall policies with antivirus applied have security events logging enabled
- Use standalone dashboard to monitor threats to your network
 - Dashboard organizes threats based on network segments on the device



FORTINET

© Fortinet Inc. All Rights Reserved.

38

Logging is an important part of managing a secure network. Enable logging for oversized files so that if there are files that are not scanned, you can be aware of it. Also, ensure that security events logging is enabled on all firewall policies using security profiles. Use the standalone dashboards to view relevant information regarding threats to your network. The standalone dashboard organizes information into network segments and breaks it down into various categories.

DO NOT REPRINT**© FORTINET**

Hardware Acceleration for Antivirus Scanning

- Accelerates flow-based antivirus only
- FortiGate models that feature NTurbo (NP6 or NP7) can accelerate antivirus processing to enhance performance
 - SoC4 models also support NTurbo
- Creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface

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

Enable NTurbo acceleration

- Proxy inspection mode
 - Proxy-based inspection cannot be offloaded for acceleration



© Fortinet Inc. All Rights Reserved.

39

The FortiGate main CPU is responsible for performing UTM/NGFW inspection on the network traffic. FortiGate models that have specialized chips can offload inspection tasks to enhance performance while providing the same level of protection. FortiGate devices that support the NTurbo feature can offload UTM/NGFW sessions to network processors. NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface. This can improve performance by accelerating antivirus inspection, without sacrificing security.

DO NOT REPRINT**© FORTINET**

Hardware Acceleration for Antivirus Scanning (Contd)

- FortiGate models with content processors (CP8 or CP9) support offloading of flow-based pattern matching
- Flow-based pattern databases are compiled and downloaded to the content processors from the IPS engine and IPS database
 - Accelerates pattern matching while reducing the load on FortiGate CPU

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

Enable AV scan offloading to CP

- Proxy inspection mode
 - Proxy-based antivirus scanning cannot be offloaded for acceleration



© Fortinet Inc. All Rights Reserved.

40

FortiGate models that have CP8 or CP9 content processors can offload flow-based pattern matching to CP8 or CP9 processors. When CP acceleration is enabled, flow-based pattern databases are compiled and downloaded to the content processors from the IPS engine and IPS database. This reduces load on the FortiGate CPU because flow-based pattern matching requests are redirected to the CP hardware. Before flow-based inspection is applied to the traffic, the IPS engine uses a series of decoders to determine the appropriate security modules that can be used, depending on the protocol of the packet and policy settings. In addition, if SSL inspection is configured, the IPS engine also decrypts SSL packets. SSL decryption is also offloaded and accelerated by CP8 or CP9 processors.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which type of inspection mode can be offloaded using NTurbo hardware acceleration?
 - A. Proxy-based
 - B. Flow-based

2. What does the logging of oversized files option do?
 - A. Enables logging of all files that cannot be scanned because of oversize limit
 - B. Logs all files that are over 5 MB



© Fortinet Inc. All Rights Reserved.

41

DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Good job! You now understand antivirus best practices.

Now, you will learn about antivirus troubleshooting.

DO NOT REPRINT

© FORTINET

Troubleshooting

Objectives

- Troubleshoot common antivirus issues

After completing this section, you should be able to troubleshoot common issues with antivirus.

By demonstrating competence in troubleshooting common antivirus issues, you will be able to configure and maintain an effective antivirus solution.

DO NOT REPRINT**© FORTINET**

Troubleshooting Common Antivirus Issues

- Valid contract but antivirus database is out-of-date?
 - Check FortiGuard website for latest antivirus database version
 - <https://fortiguard.com/updates/antivirus>
 - Make sure the antivirus profile is applied on at least one firewall policy
- Run the real-time update debug to isolate update-related issues

```
# diagnose debug application update -1  
# diagnose debug enable  
# execute update-av
```



© Fortinet Inc. All Rights Reserved.

44

What if FortiGate shows a valid license but the antivirus database is out-of-date?

Check the current database version installed on your FortiGate and compare the version number with the current release on the FortiGuard website. FortiGate may not update the antivirus database if it is not being used (applied on a firewall policy). Make sure the antivirus profile is applied on at least one firewall policy. If you continue to see issues with the update, run the real-time debug command to identify the problem.

DO NOT REPRINT

© FORTINET

Troubleshooting Common Antivirus Issues (Contd)

- FortiGuard update issues? Make sure that:
 - FortiGate has a stable connection to the internet
 - FortiGate is able to resolve DNS (update.fortiguard.net)
 - TCP port 443 is open
- Force FortiGate to check for new antivirus updates


```
# execute update-av
```
- Verify that the FortiGuard antivirus license is valid

System > FortiGuard	
AntiVirus	Licensed - expires on 2021/02/19
AV Definitions	<input checked="" type="radio"/> Version 1.00000
AV Engine	<input checked="" type="radio"/> Version 6.00132
Mobile Malware	<input checked="" type="radio"/> Version 0.00000
	<input type="button" value="Upgrade Database"/>

FORTINET

© Fortinet Inc. All Rights Reserved.

45

If you are having issues with the antivirus license or FortiGuard updates, start troubleshooting with basic connectivity tests. Most of the time, issues related to updates are caused by connectivity problems with FortiGuard servers.

- Make sure that FortiGate has a stable internet connection and can resolve DNS (update.fortinet.com).
- If there is another firewall between FortiGate and the internet, make sure TCP port 443 is open and traffic is allowed from and to the FortiGate device.
- Force FortiGate to check for new virus updates using the CLI command: `execute update-av`.
- Verify that the FortiGate device is registered and has a valid antivirus service contract.

DO NOT REPRINT**© FORTINET**

Troubleshooting Common Antivirus Issues (Contd)

- Unable to catch viruses even with a valid contract?
 - Check all internal to external firewall policies for configuration errors
 - Ensure that the proper antivirus profile, along with the correct protocol options and SSL/SSH inspection profiles are applied
 - Make sure the same antivirus profile and SSH/SSL inspection are applied on all redundant internet connection firewall policies
 - Check the **Advanced Threat Protection Statistics Widget** for virus statistics
- Some useful antivirus commands are:

```
# get system performance status
# diagnose antivirus database-info
# diagnose autoupdate versions
# diagnose antivirus test "get scantime"
# execute update-av
```

Displays virus statistics for the last one minute

Displays current antivirus database information

Displays current antivirus engine and signature versions

Displays scan times for infected files

Forces FortiGate to check for antivirus updates from FortiGuard server

FORTINET

© Fortinet Inc. All Rights Reserved.

46

What if you have a valid contract and updated database, and you are still having issues catching viruses? Start troubleshooting for basic configuration errors. Most of the time, issues are caused by misconfiguration on the device.

- Make sure that the correct antivirus profile is applied on the right firewall policy.
- Make sure that you are using the same antivirus profile and SSL/SSH inspection on all internet connection firewall policies.
- Add and use advanced the threat protection statistics widget to get the latest virus statistics from the unit.

These are some of the commands that can be used to retrieve information and troubleshoot antivirus issues:

- **get system performance status:** Displays statistics for the last one minute.
- **diagnose antivirus database-info:** Displays current antivirus database information.
- **diagnose autoupdate versions:** Displays current antivirus engine and signature versions.
- **diagnose antivirus test "get scantime":** Displays scan times for infected files.
- **execute update-av:** Forces FortiGate to check for antivirus updates from the FortiGuard server.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What command do you use to force FortiGate to check for new antivirus updates?
 A. execute update antivirus
 B. execute update-av



© Fortinet Inc. All Rights Reserved.

47

DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Basics



Antivirus Scanning Modes



Antivirus Configuration



Best Practices



Troubleshooting

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Use antivirus signatures
- ✓ Review antivirus scanning techniques
- ✓ Enable FortiSandbox with antivirus
- ✓ Differentiate between available FortiGuard signature databases
- ✓ Apply the antivirus profile in flow-based and proxy-based inspection modes
- ✓ Compare all available scanning modes
- ✓ Configure antivirus profiles and protocol options
- ✓ Review virus statistics
- ✓ Log and monitor antivirus events
- ✓ Recognize recommended antivirus configuration practices
- ✓ Log and monitor antivirus and FortiSandbox events
- ✓ Use hardware acceleration with antivirus scans
- ✓ Troubleshoot common antivirus issues

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

By mastering the objectives covered in this lesson, you learned how to use FortiGate features and functions to protect your network against viruses.

DO NOT REPRINT**© FORTINET****FORTINET**

FortiGate Security

Intrusion Prevention and Denial of Service

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.Last Modified: 29 May 2020

In this lesson, you will learn how to use FortiGate to protect your network against intrusions and denial of service (DoS) attacks.

DO NOT REPRINT**© FORTINET**

Lesson Overview



Intrusion Prevention System

Denial of Service

Web Application Firewall

Best Practices

Troubleshooting

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

DO NOT REPRINT

© FORTINET

Intrusion Prevention System (IPS)

Objectives

- Differentiate between exploits and anomalies
- Identify the different components of an IPS package
- Manage FortiGuard IPS updates
- Select an appropriate IPS signature database
- Configure an IPS sensor
- Identify the IPS sensor inspection sequence
- Apply IPS to network traffic

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

By demonstrating competence in IPS, you should be able to implement an effective IPS solution to protect your network from intrusion.

DO NOT REPRINT

© FORTINET

Why use IPS?

- Increased volume and sophistication of attacks on organizations
 - Driven by previously successful high-profile hacks and a highly profitable black-market demand for stolen data
 - More attacks against client and cloud applications
 - Attacks are no longer targeted only at servers and server-based applications
 - BYOD and remote workers increase risk of exposure



See attacks happening in real time around the world on the FortiGuard Labs live threat map.

FORTINET

© Fortinet Inc. All Rights Reserved.

4

Organizations are under continuous attacks. Cybercriminals, motivated by previously successful high-profile hacks and a highly profitable black market for stolen data, continue to increase both the volume and sophistication of their attacks on organizations. Many organizations encourage BYOD and flexible working environments, which has led to the explosion of anytime, anywhere data consumption. This consumption increases the risk that sensitive data will be exposed to unauthorized access outside corporate boundaries.

Today's threat landscape requires IPS to block a wider range of threats, while minimizing false positives.

DO NOT REPRINT**© FORTINET**

Exploits and Anomalies

Exploit

- A known, confirmed attack
- Detected when a file or traffic matches a signature pattern:
 - IPS signatures
 - WAF signatures
 - Antivirus signatures
- Example:
 - Exploit of known application vulnerabilities

Anomaly

- Can be zero-day or denial of service attacks (DoS)
- Detected by behavioral analysis:
 - Rate-based IPS signatures
 - DoS policies
 - Protocol constraints inspection
- Example:
 - Abnormally high rate of traffic (DoS/flood)



© Fortinet Inc. All Rights Reserved.

5

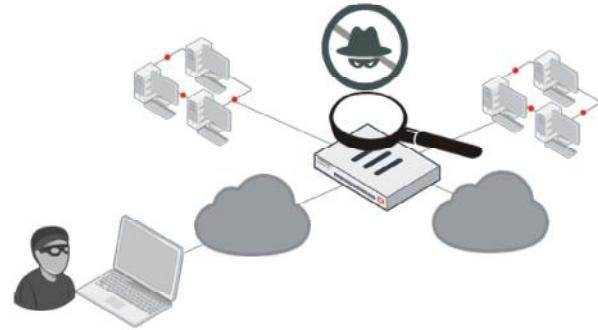
It's important to understand the difference between an anomaly and an exploit. It's also important to know which FortiGate features offer protection against each of these types of threats.

Exploits are known attacks, with known patterns that can be matched by IPS, WAF, or antivirus signatures.

Anomalies are unusual behaviors in the network, such as higher-than-usual CPU usage or network traffic. Anomalies must be detected and monitored (and, in some cases, blocked or mitigated) because they can be the symptoms of a new, never-seen-before attack. Anomalies are usually better detected by behavioral analysis, such as rate-based IPS signatures, DoS policies, and protocol constraints inspection.

DO NOT REPRINT**© FORTINET****IPS**

- Flow-based detection and blocking
 - Known exploits that match signatures
 - Network errors and protocol anomalies
- IPS components
 - IPS signature databases
 - Protocol decoders
 - IPS engine
 - Application control
 - Antivirus (flow based)
 - Web filter (flow based)
 - Email filter (flow based)
 - Data leak prevention (DLP) (flow-based in one-arm sniffer mode)

**FORTINET**

© Fortinet Inc. All Rights Reserved.

6

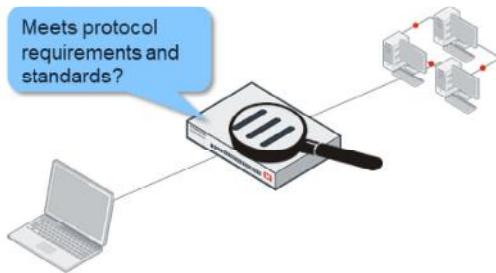
IPS on FortiGate uses signature databases to detect known attacks. Protocol decoders can also detect network errors and protocol anomalies.

The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, email filtering, and flow-based DLP in one-arm sniffer mode.

DO NOT REPRINT**© FORTINET**

What Are Protocol Decoders?

- Decoders parse protocols
- IPS signatures find parts of a protocol that don't conform
 - For example, too many HTTP headers, or a buffer overflow attempt
- Unlike proxy-based scans, IPS often does not require IANA standard ports
 - Automatically selects decoder for protocol at each OSI layer

**FORTINET**

© Fortinet Inc. All Rights Reserved.

7

How does the IPS engine determine if a packet contains an attack or anomaly?

Protocol decoders parse each packet according to the protocol specifications. Some protocol decoders require a port number specification (configured in the CLI), but usually, the protocol is automatically detected. If the traffic doesn't conform to the specification—if, for example, it sends malformed or invalid commands to your servers—then the protocol decoder detects the error.

DO NOT REPRINT**© FORTINET**

FortiGuard IPS Updates

- IPS packages are updated by FortiGuard
 - IPS signature databases
 - Protocol decoders
 - IPS engine
- Regular updates are required to ensure IPS remains effective
- Enable push updates to receive updates as they become available
- The Botnet IPs and Botnet Domains subscription is part of a FortiGuard IPS license

System > FortiGuard	
License Information	
Entitlement	Status
Intrusion Prevention	Licensed - expires on 2020/05/06 Version 15.00789
IPS Definitions	Version 6.00007
IPS Engine	Version 2.00574
Malicious URLs	Version 2.00574
Botnet IPs	Version 1.00000
Botnet Domains	Version 0.00000

System > FortiGuard	
AntiVirus & IPS Updates	
Accept push updates	<input checked="" type="checkbox"/>
Use override push	<input type="checkbox"/>
Scheduled Updates	<input checked="" type="checkbox"/> Every <input type="text" value="2"/> Hours
Improve IPS quality	<input type="checkbox"/>
Use extended IPS signature package	<input checked="" type="checkbox"/>
<input type="button" value="Update AV & IPS Definitions"/>	

FORTINET

© Fortinet Inc. All Rights Reserved.

8

By default, an initial set of IPS signatures is included in each FortiGate firmware release. FortiGuard updates the IPS signature database with new signatures. That way, IPS remains effective against new exploits. Unless a protocol specification or RFC changes (which doesn't happen very often), protocol decoders are rarely updated. The IPS engine itself changes more frequently, but still not often.

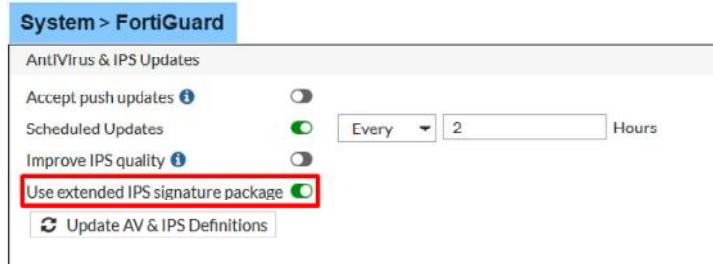
FortiGuard IPS service updates the IPS signatures most often. The FortiGuard research team identifies and builds new signatures, just like antivirus signatures. So, if your FortiGuard Services contract expires, you can still use IPS. However, just like antivirus scans, IPS scans will become increasingly ineffective the longer your signatures go without being updated—old signatures won't defend against new attacks.

IPS is a FortiGuard subscription, and includes Botnet IPs and Domains databases.

DO NOT REPRINT**© FORTINET**

Choosing the Signature Database

- Regular
 - Common attacks with fast, certain identification (default action is block)
- Extended
 - Performance-intensive

**FORTINET**

© Fortinet Inc. All Rights Reserved.

9

The IPS signature database is divided into the regular and extended databases. The regular signature database contains signatures for common attacks whose signatures cause rare or no false positives. It's a smaller database, and its default action is to block the detected attack.

The extended signature database contains additional signatures for attacks that cause a significant performance impact, or don't support blocking because of their nature. In fact, because of its size, the extended database is not available for FortiGate models with a smaller disk or RAM. But, for high-security networks, you might be required to enable the extended signatures database.

DO NOT REPRINT

© FORTINET

List of IPS Signatures

The screenshot shows the FortiGate management interface under 'Security Profiles > Intrusion Prevention'. On the left, there's a configuration panel for an 'IPS Sensor' named 'default' with comments 'Prevent critical attacks.' and a checked 'Block malicious URLs' option. Below it is a table for 'IPS Signatures and Filters' with three rows labeled 'sv1', 'sv2', and 'sv3', each with severity levels from High (red) to Information (green). A large blue callout bubble points to this table with the text 'Active signature database'.

In the center, there's a summary section titled 'FortiGate' with three donut charts: 'IPS Signatures' (with a 'View IPS Signatures' link highlighted by a red box), 'Severity' (High, Critical, Medium, Low, Information), and 'Target' (Server, Client). Below these is a table titled 'IPS Signature (7010)' listing four entries:

Name	Severity	Target	OS	Action	CVE-ID
3Com.3CDaemon.FTPServer.Buffer.Overflow	High	Server	Windows	<input checked="" type="radio"/> Block	CVE-2005-0277
3Com.3CDaemon.FTPServer.Information.Disclosure	Medium	Client	Windows	<input checked="" type="radio"/> Block	CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure	High	Server	Windows	<input checked="" type="radio"/> Block	
3Com.OfficeConnect. ADSL.Wireless.Firewall.Router.DoS	Low		Linux	<input checked="" type="radio"/> Block	

A blue callout bubble points to the 'Action' column of the last three rows with the text 'Default action'. The bottom right corner of the interface shows '© Fortinet Inc. All Rights Reserved.' and the number '10'.

After FortiGate downloads a FortiGuard IPS package, new signatures appear in the signature list. When configuring FortiGate, you can change the **Action** setting for each sensor that uses a signature.

The default action setting is often correct, except in the following cases:

- Your software vendor releases a security patch. Continuing to scan for exploits will waste FortiGate resources.
- Your network has a custom application with traffic that inadvertently triggers an IPS signature. You can disable the setting until you notify Fortinet so that the FortiGuard team can modify the signature to avoid false positives.

DO NOT REPRINT**© FORTINET**

Configuring IPS Sensors

- Add individual signatures
- Add groups of signatures using filters

Security Profiles > Intrusion Prevention

New IPS Sensor

Name: IPS profile

Comments: Write a comment... 0/255

Block malicious URLs:

IPS Signatures and Filters

+ Create New Edit Delete

Details	Exempt IPs	Action	Packet Logging
No results			

Add Signatures

Type: Signature

Action: Default

Packet logging: Enable Disable

Status: Enable Disable Default

Filter: Server Client HTTP Windows

IPS Signatures

Type: Signature

Action: Default

Packet logging: Enable Disable

Status: Enable Disable Default

Rate-based settings: Default Specify

Exempt IPs: Edit IP Exemptions

+ Add All Results Add Selected Search Selected Add

Name	Severity	Target	OS	Action	CVE ID
7ACMS.Config.Controller.RemoteCode.Execution	High	Server	Windows	Block	CVE-2019-10684
VE-2018-6546	Medium	Client	Windows	Block	VE-2018-6546
VE-2018-7264	Medium	Client	Windows	Block	VE-2018-7264
VE-2018-4335	Medium	Client	Windows	Block	VE-2018-4335
VE-2018-4895	Medium	Client	Windows	Block	VE-2018-4895
VE-2018-16014	Medium	Client	Windows	Block	VE-2018-16014
VE-2019-1499	Medium	Client	Windows	Block	VE-2019-1499
VE-2009-9865	Medium	Client	Windows	Block	VE-2009-9865

FORTINET

© Fortinet Inc. All Rights Reserved.

11

There are two ways to add predefined signatures to an IPS sensor. One way is to select the signatures individually. After you select a signature in the list, the signature is added to the sensor with its default action. Then, you can right-click the signature and change the action.

The second way to add a signature to a sensor is using filters. FortiGate will add all the signatures that match the filters.

DO NOT REPRINT**© FORTINET**

Configuring IPS Sensors

- Add rate-based signatures to block traffic when the threshold is exceeded during a time period
 - Track the traffic based on source or destination IP address

Name	Severity	Target	OS	Action	CVE-ID
Apache.httpd.mod_cache_socache.DoS	High	Server	Windows, Linux	Block	CVE-2018-1303
FTPLLogin.Brute.Force	High	Server	All	Pass	
IMAP.Login.Brute.Force	High	Server	All	Pass	
MS.Active.Directory.LDAP.Packet.Han...	High	Server	Windows, Client	Block	CVE-2013-3868
MS.RDP.Connection.Brute.Force	High	Server	Windows	Pass	

© Fortinet Inc. All Rights Reserved.

12

You can also add rate-based signatures to block specific traffic when the threshold is exceeded during the configured time period. You should apply rate-based signatures only to protocols you actually use. Then, configure **Duration** to block malicious clients for extended periods. This saves system resources and can discourage a repeat attack. FortiGate does not track statistics for that client while it is temporarily blocklisted.

DO NOT REPRINT**© FORTINET**

IPS Sensor Inspection Sequence

The screenshot shows the 'Security Profiles > Intrusion Prevention' section of the FortiGate management interface. A new IPS sensor named 'server ips' is being configured. The 'IPS Signatures and Filters' table lists two entries:

Details	Exempt IPs	Action	Packet Logging
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow TGT Server SEV [yellow/red] SEV [yellow/red] SFV [red] OS Windows	0	<input checked="" type="radio"/> Monitor <input type="radio"/> Disabled	<input checked="" type="radio"/> Default <input type="radio"/> Disabled

A blue callout bubble points to the 'Create New' button with the text: 'New entries will be placed at the bottom of the list'. Another blue callout bubble points to the table with the text: 'IPS signatures and filters are processed in sequence'.

FORTINET

© Fortinet Inc. All Rights Reserved.

13

When the IPS engine compares traffic with the signatures in each filter, order matters. The rules are similar to firewall policy matching: the engine evaluates the filters and signatures at the top of the list first, and applies the first match. The engine skips subsequent filters.

So, position the most likely matching filters, or signatures, at the top of the list. Avoid making too many filters, because this increases evaluations and CPU usage. Also, avoid making very large signature groups in each filter, which increase RAM usage.

In the event of a false-positive outbreak, you can add the triggered signature as an individual signature and set the action to **Monitor**. This will allow you to monitor the signature events using IPS logs, while investigating the false-positive issue.

DO NOT REPRINT**© FORTINET**

Configuring IP Exemptions

- Exempt specific source or destination IP addresses from specific signatures
- Only configurable under individual IPS signatures

The screenshot shows two windows from the Fortinet Security Fabric interface. The top window is titled "Security Profiles > Intrusion Prevention" and displays a table of IPS Signatures and Filters. One row is selected, showing details for "3Com.3CDaemon.FTP.Server.Information.Disclosure". The "Exempt IPs" column contains the number "1", which is highlighted with a red box and has a red arrow pointing down to the "Edit IP Exemptions" window below. The "Edit IP Exemptions" window has a table with two columns: "Source IP/Netmask" and "Destination IP/Netmask". The "Source IP/Netmask" field contains "10.0.1.10/32" and the "Destination IP/Netmask" field contains "0.0.0.0/0".

FORTINET

© Fortinet Inc. All Rights Reserved.

14

Sometimes it is necessary to exempt specific source or destination IP addresses from specific signatures. This feature is useful during false-positive outbreaks. You can temporarily bypass affected endpoints until you investigate and correct the false-positive issue.

You can configure IP exemptions on individual signatures only. Each signature can have multiple exemptions.

DO NOT REPRINT**© FORTINET**

IPS Actions

- Choose what action to take when a signature is triggered

The screenshot shows the FortiGate configuration interface for adding signatures. The 'Action' dropdown menu is open, displaying five options: Allow (selected), Monitor, Block, Reset, and Default. A red box highlights the 'Allow' option. Below the menu, there is a table listing four IPS signatures, each with columns for Severity, Target, OS, Action, and CVE-ID.

IPS Signature	Severity	Target	OS	Action	CVE-ID
3Com.3CDaemon.FTP.Server.Buffer.Overflow	██████	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure	██████	Client	Windows	Block	CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure	██████	Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	██████	Server	Linux	Block	

FORTINET

© Fortinet Inc. All Rights Reserved.

15

When you create a new entry to add signatures or filters, you can select the action by clicking **Action**.

Select **Allow** to allow traffic to continue to its destination. Select **Monitor** to allow traffic to continue to its destination and log the activity. Select **Block** to silently drop traffic matching any of the signatures included in the entry. Select **Reset** to generate a TCP RST packet whenever the signature is triggered. Select **Default** to use the default action of the signatures.

Quarantine allows you to quarantine the attacker's IP address for a set duration. You can set the quarantine duration to any number of days, hours, or minutes.

If you enable **Packet logging**, FortiGate saves a copy of the packet that matches the signature.

DO NOT REPRINT**© FORTINET**

Enabling Botnet Protection

- The botnet database:
 - Part of the IPS contract
 - Should be used with the IPS profile to maximize the protection of internal endpoints
- Can be enabled only on the IPS profile
- Administrators can set the action to **Block** or **Monitor**
- IPS logs are generated

Details	Exempt IPs	Action	Packet Logging
SEV [Yellow]		<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Disabled
SEV [Orange]		<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Disabled
SEV [Red]		<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Disabled
SEV [Grey]		<input checked="" type="checkbox"/> Default	<input checked="" type="checkbox"/> Disabled

FORTINET

© Fortinet Inc. All Rights Reserved.

16

Since the botnet database is part of the FortiGuard IPS contract, administrators can enable scanning of botnet connections to maximize their internal security. You enable botnet scanning on the IPS profile that you applied the firewall policy on. You can also enable scanning of botnet connections using the CLI.

There are three possible actions for botnet and C&C:

- **Disable:** Do not scan connections to botnet servers
- **Block:** Block connections to botnet servers
- **Monitor:** Log connections to botnet servers

DO NOT REPRINT**© FORTINET**

Applying IPS Inspection

Add IPS sensors as security profiles to firewall policies

Policy & Objects > Firewall Policy

Security Profiles

- AntiVirus
- Web Filter
- DNS Filter
- Application Control

- IPS IPS protect_client

- SSL Inspection ⚠ SSL deep-inspection

- Decrypted Traffic Mirror

Logging Options

- Log Allowed Traffic Security Events All Sessions
- Generate Logs when Session Starts
- Capture Packets

Enable this option to log all sessions including blocked and allowed traffic

FORTINET

© Fortinet Inc. All Rights Reserved.

17

To apply an IPS sensor, you must enable **IPS** and then select the sensor in a firewall policy. By default, FortiGate logs all security events. This means you can see any traffic that is being blocked by IPS.

If you think some traffic should be blocked but is passing through the policy, you should change the **Log Allowed Traffic** method to **All Sessions**. This will log all traffic processed by that firewall policy, and not just the traffic that is blocked by the security profiles. This can help you in identifying false negative events.

DO NOT REPRINT**© FORTINET**

IPS Logging

Log & Report > Intrusion Prevention

Date/Time	%	Severity	Source	Protocol	User	Action	Count	Attack Name
2020/03/11 08:09:46	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:07:11	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:06:14	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:04:49	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:04:48	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:04:36	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:04:28	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:04:20	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:04:14	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:03:42	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/11 08:03:13	[REDACTED]	[REDACTED]	192.168.10.201	6		dropped		Dorifel.Botnet
2020/03/10 16:02:36	[REDACTED]	[REDACTED] user (1.1.1.1)	6	[REDACTED] user		detected		test_botnet
2020/03/10 16:02:36	[REDACTED]	[REDACTED] user (1.1.1.1)	6	[REDACTED] user		detected		test_attack



If you enabled security events logging in the firewall policies that apply IPS, you can view IPS events by clicking **Log & Report > Intrusion Prevention**. The **Intrusion Prevention** log menu appears only if FortiGate has matched attack attempts with IPS signatures.

You should review IPS logs frequently. The logs are an invaluable source of information about the kinds of attacks that are being targeted at your network. This will help you develop action plans and focus on specific events, for example, patching a critical vulnerability.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which one of the following IPS actions allows traffic and logs the activity?
 - A. Allow
 - B. Monitor

2. Which IPS component is updated most frequently?
 - A. Protocol decoders
 - B. IPS signature database



© Fortinet Inc. All Rights Reserved.

19

DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Web Application Firewall



Best Practices



Troubleshooting

Good job! You now understand the IPS on FortiGate.

Now, you will learn about denial of service.

DO NOT REPRINT

© FORTINET

Denial of Service (DoS)

Objectives

- Identify a DoS attack
- Configure a DoS policy

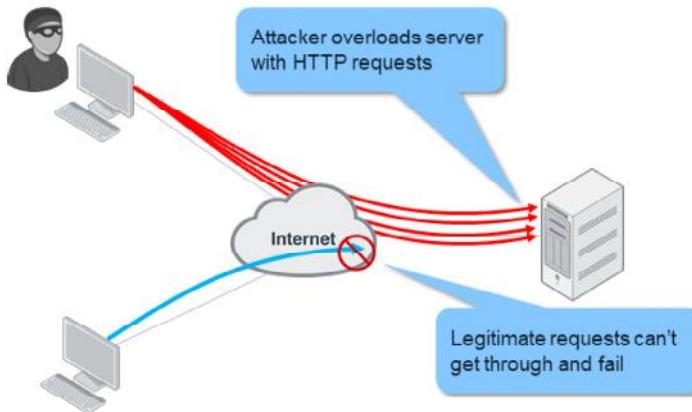
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in DoS, you should be able to protect your network from common DoS attacks.

DO NOT REPRINT**© FORTINET**

DoS Attacks

- Attacker's sessions consume all resources—RAM, CPU, port numbers
- Slows down or disables the target until it can't serve legitimate requests

**FORTINET**

© Fortinet Inc. All Rights Reserved.

22

So far, you've learned about signatures that match illegal commands and invalid protocol implementations. Those are easy to confirm as attacks.

What about attacks that function by exploiting asymmetric processing or bandwidth between clients and servers?

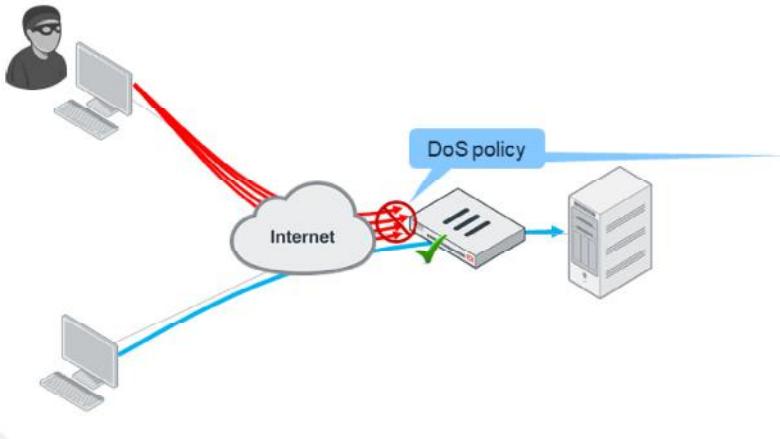
The goal of a DoS attack is to overwhelm the target—to consume resources until the target can't respond to legitimate traffic. There are many ways to accomplish this. High-bandwidth usage is only one type of DoS attack. Many sophisticated DoS attacks, such as Slowloris, don't require high bandwidth.

DO NOT REPRINT

© FORTINET

DoS Policy

- DoS policies apply the action when the configured threshold is exceeded
 - Half-open connections, source address, destination address, ports, and so on
 - Multiple sensors can detect different anomalies



Policy & Objects > IPv4 DoS Policy					
New Policy					
Incoming Interface	<input checked="" type="checkbox"/> port1 <input checked="" type="checkbox"/> all				
Source Address	<input checked="" type="checkbox"/> all +				
Destination Address	<input checked="" type="checkbox"/> all +				
Service	<input checked="" type="checkbox"/> All +				
L3 Anomalies					
Name	Logging	Action	Disable	Block	Monitor
ip_src_session	<input checked="" type="checkbox"/>	Disable	Block	Monitor	5000
ip_dst_session	<input checked="" type="checkbox"/>	Disable	Block	Monitor	5000
L4 Anomalies					
Name	Logging	Action	Disable	Block	Monitor
tcp_syn_flood	<input checked="" type="checkbox"/>	Disable	Block	Monitor	2000
tcp_port_scan	<input checked="" type="checkbox"/>	Disable	Block	Monitor	1000
tcp_src_session	<input checked="" type="checkbox"/>	Disable	Block	Monitor	5000
tcp_dst_session	<input checked="" type="checkbox"/>	Disable	Block	Monitor	5000
udp_flood	<input checked="" type="checkbox"/>	Disable	Block	Monitor	2000
udp_scan	<input checked="" type="checkbox"/>	Disable	Block	Monitor	2000
ulp_src_session	<input checked="" type="checkbox"/>	Disable	Block	Monitor	5000
ulp_dst_session	<input checked="" type="checkbox"/>	Disable	Block	Monitor	5000

© Fortinet Inc. All Rights Reserved.

23

To block DoS attacks, apply a DoS policy on a FortiGate device that is located between attackers and all the resources that you want to protect.

DoS filtering is done early in the packet handling process, which is handled by the kernel.

DO NOT REPRINT**© FORTINET**

Types of DoS Attacks

- TCP SYN flood
 - Attacker floods victim with incomplete TCP/IP connection requests
 - The victim's connection table becomes full, so legitimate clients can't connect
- ICMP sweep
 - Attackers sends ICMP traffic to find targets
 - Attacker then attacks hosts that reply
- TCP port scan
 - Attacker probes a victim by sending TCP/IP connection requests to varying destination ports
 - Based on replies, attacker can map out which services are running on the victim system
 - Attacker then targets those destination ports to exploit the system



© Fortinet Inc. All Rights Reserved.

24

In TCP, the client sends a SYN packet to initiate a connection. The server must respond with a SYN/ACK packet, and save the connection information in RAM while it waits for the client to acknowledge with an ACK packet. Normal clients will ACK quickly and begin to transmit data. But malicious clients continue to send more SYN packets, half-opening more connections, until the server's connection table becomes full. Once the server's table is full, it can't accept more connections and begins to ignore all new clients.

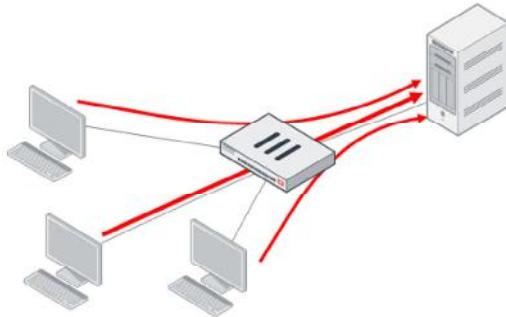
ICMP is used during troubleshooting: devices respond with success or error messages. However attackers can use ICMP to probe a network for valid routes and responsive hosts. By doing an ICMP sweep, the attacker can gain information about your network before crafting more serious exploits.

Attackers use port scanning to determine which ports are active on a system. The attacker sends TCP SYN requests to varying destination ports. Based on the replies, the attacker can map out which services are running on the system, and then proceed to exploit those services.

DO NOT REPRINT**© FORTINET**

Types of DoS Attacks

- Distributed DoS
 - Many of the same characteristics of an individual DoS attack
 - However, attack originates from multiple sources

**FORTINET**

© Fortinet Inc. All Rights Reserved.

25

An individual DoS attack is a flood of traffic coming from a single address. It can originate from the internet, or even from your internal network. Typically, a single device makes many connections or sessions, and possibly uses much bandwidth to connect to a single location. A variation of this is the distributed denial of service attack or DDoS. It has many of the same characteristics as an individual DoS attack, but the main difference is that multiple devices are all attacking one destination at the same time.

DO NOT REPRINT**© FORTINET**

DoS Policy Configuration

- Can apply multiple DoS policies to any physical or logical interface
- Types
 - Flood
 - Detects a large volume of the same type of traffic
 - Sweep/scan
 - Detects probing attempts
 - Source (SRC)
 - Detects a large volume of traffic from an individual IP
 - Destination (DST)
 - Detects a large volume of traffic destined for an individual IP

Policy & Objects > IPv4 DoS Policy

New Policy					
Incoming Interface	port1	Source Address	all	Destination Address	all
	+		+		+
Service	ALL				
	+				
L3 Anomalies					
Name	Logging	Action	Disable	Block	Monitor
ip_src_session					5000
ip_dst_session					5000
L4 Anomalies					
Name	Logging	Action	Disable	Block	Monitor
tcp_syn_flood					2000
tcp_port_scan					1000
tcp_src_session					5000
tcp_dst_session					5000
udp_flood					2000
udp_scan					2000
udp_src_session					5000
udp_dst_session					5000

© Fortinet Inc. All Rights Reserved.

26

FORTINET

You can apply DoS protection to four protocols: TCP, UDP, ICMP, and SCTP. And, you can apply four different types of anomaly detection protocol:

- A flood sensor detects a high volume of that specific protocol, or signal in the protocol
- A sweep/scan detects probing attempts to map which of the host's ports respond and, therefore, might be vulnerable
- Source signatures look for large volumes of traffic originating from a single IP
- Destination signatures look for large volumes of traffic destined for a single IP

When you implement DoS for the first time, if you don't have an accurate baseline for your network, be careful not to completely block network services. To prevent this from happening, configure the DoS policy initially to log, but not block. Using the logs, you can analyze and identify normal and peak levels for each protocol. Then, adjust the thresholds to allow normal peaks, while applying appropriate filtering.

The threshold for flood, sweep, and scan sensors are defined as the maximum number of sessions or packets per second. The threshold for source and destination sensors are defined as concurrent sessions. Thresholds that are too high can exhaust your resources before the DoS policies trigger. Thresholds that are too low will cause FortiGate to drop normal traffic.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which one of the following behaviors is a characteristic of a DoS attack?
 - A. Attempts to exploit a known application vulnerability
 - B. Attempts to overload a server with TCP SYN packets

2. Which DoS anomaly sensor can be used to detect and block a port scanner's probing attempts?
 - A. `tcp_syn_flood`
 - B. `tcp_port_scan`



DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Web Application Firewall



Best Practices



Troubleshooting

Good job! You now understand how to protect your network from DoS attacks on FortiGate.

Now, you will learn about web application firewall.

DO NOT REPRINT

© FORTINET

Web Application Firewall (WAF)

Objectives

- Identify the purpose of WAF on FortiGate
- Identify common web attacks
- Configure a WAF profile

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

By demonstrating competence in WAF, you should be able to apply the correct WAF inspection to protect the servers in your network.

DO NOT REPRINT

© FORTINET

WAF

- Websites are attractive targets for hackers
- FortiGuard web filtering is for clients, not servers
- WAF provides protection for web services

System > Feature Visibility



FORTINET

Available only in proxy inspection mode.

Policy & Objects > Firewall Policy

The screenshot shows a 'New Policy' configuration. Under 'Inspection Mode', the 'Proxy-based' tab is selected. In the 'Security Profiles' section, the 'WAF' profile is selected, indicated by a red box. Other profiles listed include AntiVirus, Web Filter, DNS Filter, Application Control, and IPS.

© Fortinet Inc. All Rights Reserved.

30

What is a WAF and why do you need it?

Some FortiGate features are meant to protect clients, not servers. For example, FortiGuard web filtering blocks requests based on the category of the server's web pages. Antivirus prevents clients from accidentally downloading spyware and worms. Neither protects a server (which doesn't send requests—it receives them) from malicious scripts or SQL injections. Protecting web servers requires a different approach because they are subject to other kinds of attacks. This is where WAF applies.

The WAF feature is available only in proxy inspection mode.

DO NOT REPRINT**© FORTINET**

Example of a Web Attack—Cross-Site Scripting

1. An attacker inputs JavaScript in an HTML form/parameter
2. The web app does not reject illegal input
3. Usually, the web app saves the input to a database
4. An innocent client requests a page that is retrieved from the database. The page:
 - Now includes malicious script
 - Can cause client's browser to transmit to third-party, malicious server
- The variety of attacks based on cross-site scripting (XSS) is limitless, but they commonly include transmitting private data like authentication cookies or other session information to the attacker



© Fortinet Inc. All Rights Reserved.

31

Let's look at some examples of attacks that target web applications specifically.

One type of attack is called cross-site scripting (XSS). If a web application doesn't sanitize its inputs and reject JavaScript, it ends up storing the XSS attack in its database. Then, when other clients request the page that reuses that data, the JavaScript is now embedded in the page.

JavaScript can do many things with a page, including rewriting the whole page and making its own requests. This is the basic mechanism of asynchronous JavaScript and XML (AJAX) apps. In this case, XSS causes innocent clients to transmit to a different server that is controlled by the attacker. This could, for example, transmit credit card information or passwords from an HTTP form to the attacker.

DO NOT REPRINT**© FORTINET**

Example of a Web Attack–SQL Injection

- SQL statements are inserted into entry fields of a web application
- The web application doesn't reject illegal input
- When the web application connects to the database to add input, it can:
 - Download sensitive data from the database (`select * from USERS`)
 - Modify database (insert/update/delete)
 - Perform administrative operations (close management interface)



© Fortinet Inc. All Rights Reserved.

32

Another very common web attack is a SQL injection. Just like an XSS attack, the root cause of a SQL injection is that the web application doesn't sanitize input. If the attacker enters a SQL query into an input such as an HTML form, the web app simply accepts it, and passes it along to the database engine, which accidentally runs the query.

The SQL language can do anything to the data. It can, for example, download the table of users so that the attacker can run a password cracker. A query could add new entries for new administrator log in attempts, or modify log in attempts, blocking administrators from logging in.

DO NOT REPRINT

© FORTINET

WAF Configuration

The screenshot displays two main configuration panels for a WAF profile.

Left Panel: Security Profiles > Web Application Firewall

- Signatures:**

Status	Signature	Action	Severity
Disable	Cross Site Scripting	Monitor	Low
Disable	Cross Site Everything (Extended)	Allow	Low
Enable	SQL Injection	Block	Medium
Disable	SQL Injection (Extended)	Allow	Low
Enable	Generic Attacks	Block	Medium
Disable	Generic Attacks (Extended)	Allow	Low
Enable	Trojans	Block	Medium
Enable	Information Disclosure	Allow	Low
Enable	Known Exploits	Block	Medium
- Constraints:**

Status	Constraint	Limit	Action	Severity
Disable	Illegal Host Name		Block	Low
Disable	Illegal HTTP Version		Monitor	Low
Disable	Illegal HTTP Request Method		Block	Low
Enable	Content Length	67,100,864	Monitor	Low
Enable	Header Length	8,192	Monitor	Low
Enable	Header Line Length	1,024	Monitor	Low
Enable	Number of Header Lines in Request	32	Monitor	Low
Enable	Total URL and Body Parameters Length	8,192	Monitor	Low
Enable	Total URL Parameters Length	8,192	Monitor	Low

Right Panel: Policy & Objects > Firewall Policy

A new policy named "default" is being configured:

- Configuration:**
 - Inbound Access: port1, port2
 - Source: all
 - Destination: webserver01
 - Schedule: always
 - Service: ALL
 - Action: ACCEPT (selected)
- Inspection Mode:** Flow-based (selected)
- Firewall / Network Options:**
 - NAT: Enabled
 - IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool
 - Preserve Source Port: Enabled
 - Protocol Options: default
- Security Profiles:**
 - AntiVirus: Off
 - Web Filter: Off
 - DNS Filter: Off
 - Application Control: Off
 - IPS: Off
 - Web Application Firewall: Web (selected)
- SSL Inspection:** certificate-inspection

© Fortinet Inc. All Rights Reserved. 33

One component of a WAF profile is WAF signatures. WAF signatures work in the same way as IPS signatures. FortiGate can act on the traffic that matches any of them. Some WAF signatures are categorized as extended. They are more likely to cause false positives, but are sometimes required in high-security environments.

HTTP constraints can monitor and control the number, type, and length of many HTTP headers, which are also inputs. This prevents unexpected inputs that a malicious client could craft to compromise your server. The limits can vary by your server's software, but also by its hardware. If a server has limited RAM, for example, then it is potentially easier to overload or crash with an excessive number of headers, because parsing the headers and storing them in buffers requires RAM.

After you configure a WAF profile, it is assigned to one or more firewall policies.

DO NOT REPRINT**© FORTINET**

FortiWeb

- Provides more specialized web server protection
- More complete protocol understanding
- HTTP state attack protection
- HTTP vulnerability scans/penetration tests
- HTTP rewriting and application delivery (basic ADC)
- Better performance for high HTTP traffic

**FORTINET**

© Fortinet Inc. All Rights Reserved.

34

FortiWeb is a specialized WAF device. For environments where the protection of web services is critical, you can complement FortiGate with a FortiWeb device.

FortiWeb offers a more complete HTTP protocol understanding and state attack protection. It can perform vulnerability scans and penetration tests. It can also rewrite the HTTP packets, and route traffic based on the HTTP content.

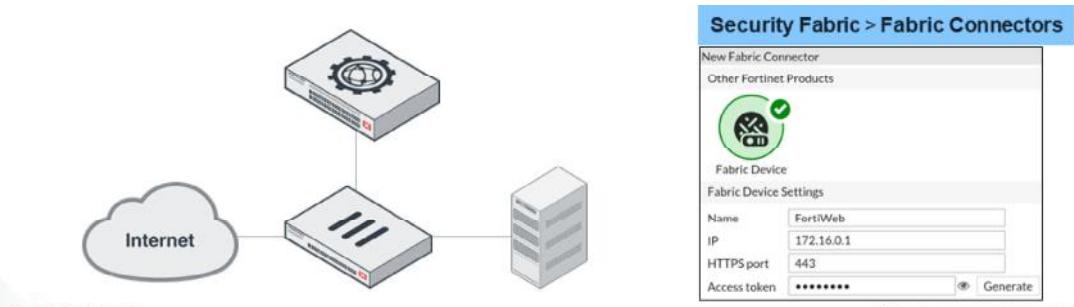
DO NOT REPRINT**© FORTINET**

FortiGate-FortiWeb Integration

- FortiWeb installed standalone (online or offline), usually behind FortiGate



- FortiGate configured to forward HTTP traffic to FortiWeb for inspection



In most cases, FortiWeb is installed as a standalone device, usually located between FortiGate and the protected web servers. FortiWeb can be installed online (web traffic crossing the device) or offline (device is connected as a one-arm sniffer).

Alternatively, you can configure FortiGate to forward web traffic to an external FortiWeb, where the WAF inspection happens. This is useful, for example, when you need to protect servers located in multiple sites with one single FortiWeb. With this setup, FortiGate will forward all web traffic to the FortiWeb if the traffic matches a firewall policy configured with a WAF profile enabled for external inspection.

For detailed information on FortiWeb, see the NSE 6 FortiWeb training material.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. WAF protocol constraints protect against what type of attacks?
 A. Buffer overflow
 B. ICMP Sweep

2. To use the WAF feature, which inspection mode should be used in the firewall policy?
 A. Flow
 B. Proxy



© Fortinet Inc. All Rights Reserved.

36

DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Web Application Firewall



Best Practices



Troubleshooting

Good job! You now understand how to protect your servers using WAF on FortiGate.

Now, you will learn about IPS best practices.

DO NOT REPRINT**© FORTINET**

Best Practices

Objectives

- Identify the IPS implementation methodology
- Enable full SSL inspection for IPS-inspected traffic
- Identify hardware acceleration components for IPS

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

By demonstrating competence in identifying IPS implementation best practices, you should be able to deploy an IPS solution on FortiGate that will be efficient and effective. You should also be able to apply full SSL inspection for IPS inspected traffic, as well as identify hardware acceleration components for IPS.

DO NOT REPRINT**© FORTINET**

IPS Implementation

- Analyze requirements
 - Not all policies require IPS
 - Start with the most business-critical services
 - Avoid enabling IPS on internal-to-internal policies
- Evaluate applicable threats
 - Create IPS sensors specifically for the resources you want to protect
- Maintain IPS continuously
 - Monitor logs for anomalous traffic patterns
 - Tune IPS profiles based on observations



© Fortinet Inc. All Rights Reserved.

39

Before you implement IPS, you must analyze the needs of your network. Enabling the default profiles across all policies will quickly cause issues, the least of which are false positives. Performing unnecessary inspections on all network traffic can cause high resource utilization which can hamper the FortiGate ability to process regular traffic.

You must also evaluate applicable threats. If your organization runs only Windows, there is no need to scan for Mac OS vulnerabilities. It is also important to consider the direction of the traffic. There are many IPS signatures that apply only to clients, and many signatures that apply only to servers. Create IPS sensors specific to the resources you want to protect. This will make sure that FortiGate is not scanning traffic with irrelevant signatures.

Lastly, IPS is not a *set-and-forget* implementation. You must monitor logs regularly for anomalous traffic patterns, and adjust your IPS profile configuration based on your observations. You should also audit your internal resources regularly to identify if certain vulnerabilities are still applicable to your organization.

DO NOT REPRINT

© FORTINET

Full SSL Inspection

- Enable a full SSL inspection profile to ensure you're inspecting encrypted traffic

The screenshot displays two configuration pages from the FortiGate management interface:

- Security Profiles > SSL/SSH Inspection**: A form for creating a new SSL inspection profile named "webserver_ssl". It includes fields for comments, SSL inspection options (protecting the server), and protocol port mapping (HTTPS port 443).
- Policy & Objects > Firewall Policy**: A policy configuration page where the "SSL inspection" field is set to "webserver_ssl". A red arrow points from the "SSL inspection" dropdown in the policy page to the "SSL inspection profile" dropdown in the security profile page.

Both pages include standard firewall policy settings like source, destination, schedule, and service. The policy page also shows NAT and WAF configurations.

Certain vulnerabilities apply only to encrypted connections. In some of these cases, FortiGate can't identify the threat reliably if it can't parse the payload. For this reason, you must use an SSL inspection profile if you want to get the maximum benefit from your IPS and WAF features.

The example on this slide shows an SSL inspection profile configured to protect a server. This policy, when applied to inbound traffic, will be able to apply IPS and WAF inspection on encrypted traffic reliably, because FortiGate will be able to decrypt encrypted sessions and inspect all parts of the packet.

It's important to note that DoS policies do not have the ability to assign SSL inspection profiles. This is because DoS does not require SSL inspection to maximize its detection ability, because it does not inspect packet payload. DoS inspects only specific session types and their associated volume.

DO NOT REPRINT**© FORTINET**

Hardware Acceleration

- FortiGate models with NP6, NP7, and SoC4 can benefit from NTurbo acceleration (np-accel-mode).
- FortiGate models that have a CP8 or CP9, support offloading of IPS pattern matching to the content processor (cp-accel-mode).

```
fgt # get hardware status
Model name: FortiGate 300D
ASIC version: CP8
ASIC SRAM: 64M
CPU: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
Number of CPUs: 4
RAM: 7996 MB
Compact Flash: 15331 MB /dev/sda
Hard disk: 114473 MB /dev/sdb
USB Flash: not available
Network Card chipset: Intel(R) Gigabit Ethernet
Network Driver (rev. 0003)
Network Card chipset: FortiASIC NP6 Adapter (rev.)
```

```
# config ips global
# set np-accel-mode [ basic | none ]
# set cp-accel-mode [ basic | advanced | none ]
# end
```

np-accel-mode

- basic: offloads IPS processing to NP

cp-accel-mode

- basic: offloads basic IPS pattern matching to CP8 or CP9
- advanced: offloads more types of IPS pattern matching
 - Only available in units with two or more CP8s or one or more CP9s

© Fortinet Inc. All Rights Reserved.

41

Usually, traffic requiring inspection, such as antivirus or IPS, is handled by the CPU on FortiGate. However, there are specialized chips on specific FortiGate models that can offload these inspection tasks. This frees up CPU cycles to manage other tasks, and also accelerates sessions requiring security inspection.

FortiGate models that support a feature called NTurbo can offload IPS processing to NP6, NP7, or SoC4 processors. If the command `np-accel-mode` is available under `config system global`, then the FortiGate model supports NTurbo.

Some FortiGate models also support offloading IPS pattern matching to CP8 or CP9 content processors. If the command `cp-accel-mode` is available under `config ips global`, then the FortiGate model supports IPS pattern matching acceleration to its CP8 or CP9 processor.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which chipset uses NTurbo to accelerate IPS sessions?
A. CP9
 B. SoC3

2. Which of the following features requires full SSL inspection to maximize its detection capability?
 A. WAF
B. DoS



DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Web Application Firewall



Best Practices



Troubleshooting

Good job! You now understand some best practices for IPS implementation on FortiGate.

Now, you will learn about IPS troubleshooting.

DO NOT REPRINT**© FORTINET**

Troubleshooting

Objectives

- Troubleshoot FortiGuard IPS updates
- Troubleshoot IPS high-CPU usage
- Manage IPS fail-open events
- Investigate false-positive detection

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

By demonstrating competence in troubleshooting, you should be able to identify, investigate, and manage some common issues with IPS deployments on FortiGate.

DO NOT REPRINT**© FORTINET**

FortiGuard IPS Troubleshooting

- All IPS update requests are sent to update.fortiguard.net on TCP port 443
 - Can be configured to connect through a web proxy (CLI only):
 - config system autoupdate tunneling
- Verify update status in GUI

The screenshot shows the 'System > FortiGuard' page. On the left, there's a sidebar with links: 'Intrusion Prevention', 'IPS Definitions', 'IPS Engine', 'Malicious URLs', 'Botnet IPs', and 'Botnet Domains'. The main area has a title 'Licensed - expires on 2021/02/19' with a green checkmark. Below it, there are two columns of items, each with a radio button and a 'View List' button:

Category	Item	Action
IPS Definitions	Version 15.00790	<input type="radio"/> View List
IPS Definitions	Version 6.00007	<input type="radio"/> View List
IPS Engine	Version 2.00577	<input type="radio"/> View List
IPS Engine	Version 1.00000	<input type="radio"/> View List
Malicious URLs	Version 0.00000	<input type="radio"/> View List
Botnet IPs	Version 0.00000	<input type="radio"/> View List
Botnet Domains	Version 0.00000	<input type="radio"/> View List

- Enable real-time debug in CLI

```
# diagnose debug application update -l
# diagnose debug enable
# execute update-now
```

After enabling real-time debugging, force a manual update of all FortiGuard packages.

© Fortinet Inc. All Rights Reserved.

45

FortiGate IPS update requests are sent to update.fortiguard.net on TCP port 443. You can also configure FortiGate to connect through a web proxy for updates.

You should check the last update timestamp regularly. You can verify it in the GUI. If there is any indication that the IPS definitions are not updating, you should investigate. Always make sure FortiGate has proper DNS resolution for update.fortiguard.net. If, by chance, there are any intermediary devices between the FortiGate and the internet, make sure the correct firewall rules are in place to allow traffic on port 443. Any intermediary devices performing SSL inspection on this traffic can also cause issues with updates.

Finally, you can use the FortiGuard update debug to monitor update events in real time.

DO NOT REPRINT**© FORTINET**

IPS and High-CPU Use

```
# diagnose test application ipsmonitor ?  
  
1: Display IPS engine information  
2: Toggle IPS engine enable/disable status  
3: Display restart log  
4: Clear restart log  
5: Toggle bypass status  
6: Submit attack characteristics now  
10: IPS queue length  
11: Clear IPS queue length  
12: IPS L7 socket statistics  
13: IPS session list  
14: IPS NTurbo statistics  
15: IPSA statistics  
97: Start all IPS engines  
98: Stop all IPS engines  
99: Restart all IPS engines and monitor
```

Shuts down IPS engine completely

IPS engine remains active, but does not inspect traffic

FORTINET

© Fortinet Inc. All Rights Reserved.

46

Short spikes in CPU usage by IPS processes could be caused by firewall policy or profile changes. These spikes are usually normal. Spikes might happen when FortiGate has hundreds of policies and profiles, or many virtual domains. Continuous high-CPU use by the IPS engines is not normal, and you should investigate it. The command shown here, along with displayed options, can be used to troubleshoot these issues.

If there are high-CPU use problems caused by the IPS, you can use the `diagnose test application ipsmonitor` command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

If the CPU use remains high after enabling IPS bypass mode, it usually indicates a problem in the IPS engine, that you must report to Fortinet's support team. You can disable the IPS engine completely using option 2. If you wish to restore IPS inspection of traffic after you finish troubleshooting, use option 5 again.

Another recommendation to keep in mind: if you need to restart the IPS, use option 99, as shown on this slide. This guarantees that all the IPS-related processes restart properly.

DO NOT REPRINT**© FORTINET**

IPS Fail Open

- Fail open is triggered when the IPS socket buffer is full and new packets can't be added for inspection

```
config ips global  
  set fail-open <enable|disable>  
  ...  
end
```

- IPS fail open entry log:

```
date=2017-09-21 time=09:07:59 logid=0100022700 type=event subtype=system  
level=critical vd="root" logdesc="IPS session scan paused" action="drop"  
msg="IPS session scan, enter fail open mode"
```

- When troubleshooting IPS fail open events, try to identify a pattern
 - Has the traffic volume increased recently?
 - Does fail open trigger at specific times during the day?
- Create IPS profiles specifically for the traffic type
 - An IPS sensor configured to protect Windows servers doesn't need Linux signatures
 - Disable IPS on internal-to-internal policies

Packets dropped!

FORTINET

© Fortinet Inc. All Rights Reserved.

47

IPS goes into fail open mode when there is not enough available memory in the IPS socket buffer for new packets. What happens during that state depends on the IPS configuration. If the `fail-open` setting is enabled, some new packets (depending on the system load) will pass through without being inspected. If it is disabled, new packets will be dropped.

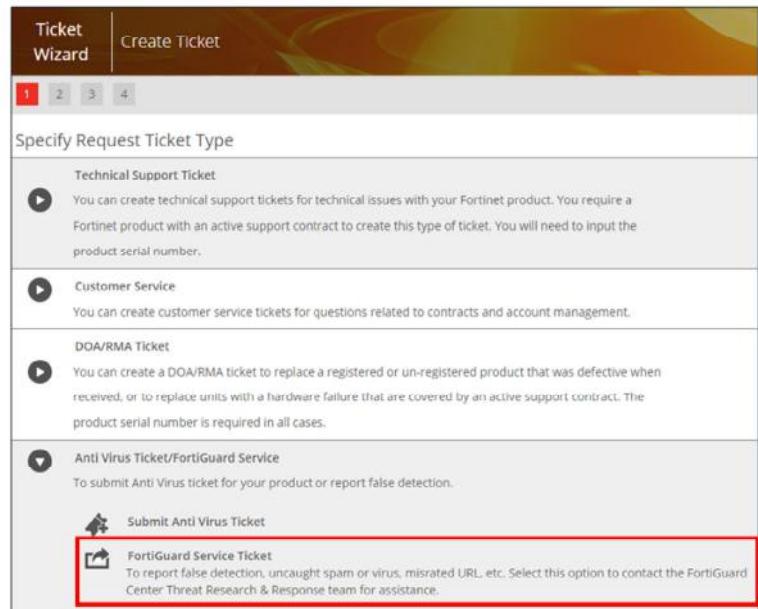
Frequent IPS fail open events usually indicate that the IPS is not able to keep up with the traffic demands. So, try to identify patterns. Has the traffic volume increased recently? Have throughput demands increased? Does fail open trigger at specific times during the day?

Tune and optimize your IPS configuration. Create IPS profiles specific to the type of traffic being inspected, and disable IPS profiles on policies that don't need them.

DO NOT REPRINT**© FORTINET**

False-Positive Detection

- Check the logs to determine which signature is triggering the false-positive
- Use IP exemptions on the signature as a temporary bypass for the affected endpoints
- Collect samples of the traffic:
 - Use the **Packet Logging** action
- Provide the traffic samples and the IPS logs to the FortiGuard team for further investigation



FORTINET

© Fortinet Inc. All Rights Reserved.

48

In the event of a false-positive detection, first determine which signature is generating them. You should also verify that the traffic is hitting the correct policy and IPS sensor. After you have verified these factors, you should gather samples of the traffic. Use the **Packet Logging** action on the signature. Provide the traffic samples and the matching IPS logs to the FortiGuard team for further investigation.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which FQDN does FortiGate use to obtain IPS updates?
 A. update.fortiguard.net
 B. service.fortiguard.com

2. When IPS fail open is triggered, what is the expected behavior, if the IPS fail open option is set to enabled?
 A. New packets will pass through without inspection
 B. New packets will be dropped



© Fortinet Inc. All Rights Reserved.

49

DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Web Application Firewall



Best Practices



Troubleshooting

Congratulations! You have completed this lesson.

Now you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Manage FortiGuard IPS updates
- ✓ Configure an IPS sensor
- ✓ Apply IPS to network traffic
- ✓ Identify a DoS attack
- ✓ Configure a DoS policy
- ✓ Identify common web attacks
- ✓ Configure a WAF profile
- ✓ Identify IPS implementation methodology
- ✓ Troubleshoot common IPS issues

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

By mastering the objectives covered in this lesson, you have gained the skills and knowledge that you need to configure, maintain, and troubleshoot your FortiGate IPS solution.

DO NOT REPRINT

© FORTINET



FORTINET

FortiGate Security

SSL-VPN

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

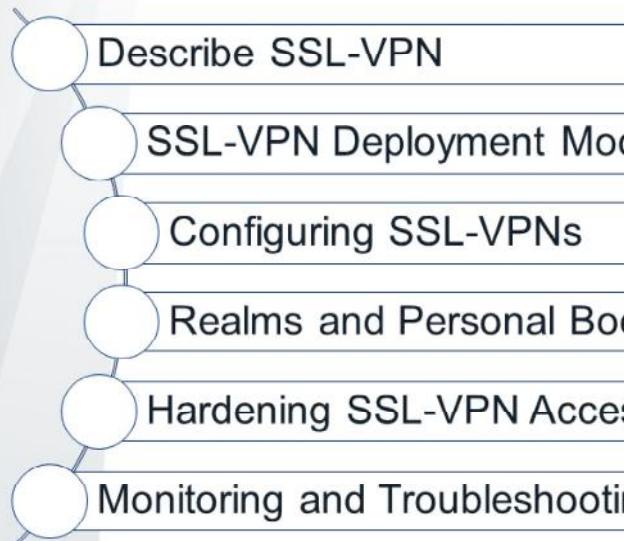
Last Modified: 29 May 2020

In this lesson, you will learn how to configure and use SSL-VPNs. SSL-VPNs are an easy way to give remote users access to your private network.

DO NOT REPRINT

© FORTINET

Lesson Overview



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

DO NOT REPRINT

© FORTINET

Describe SSL-VPN

Objectives

- Define a virtual private network (VPN)
- Describe the differences between SSL-VPN and IPsec VPN

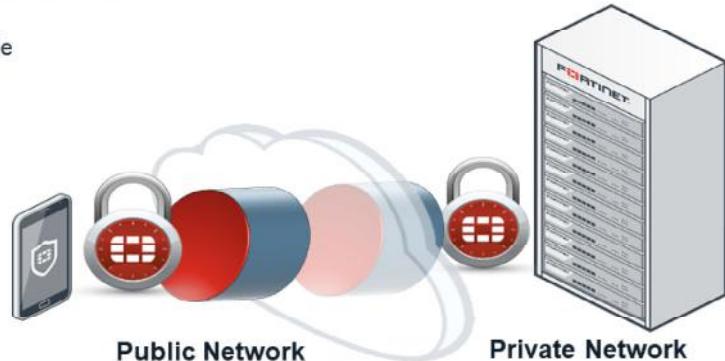
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding VPN concepts, you will be able to more effectively understand how FortiGate manages SSL-VPN methods.

DO NOT REPRINT**© FORTINET**

What Are VPNs?

- A VPN extends a private network across a public network
- Securely connect remote LANs and devices
 - Employees who travel
 - Branch offices to servers at a central office
- Safely transmit private data across the internet
 - Tamper-proof
 - Attackers can't change a message or file
 - Encrypt
 - Unauthorized users can't eavesdrop
 - Authenticate
 - Only known users can access the private network

**FORTINET**

© Fortinet Inc. All Rights Reserved.

4

A VPN creates a tunnel that gives users or remote LANs secure access to your private network, as if they were connected to your LAN.

A VPN is often used when LANs are separated by an untrusted public network, such as the Internet. As well as providing users with secure access to private networks while they are traveling, a VPN can also interconnect branch office networks located across the internet, and even on the other side of the world.

User data inside a VPN tunnel is encrypted for privacy. It cannot be read, even if it is intercepted by unauthorized users. VPNs also use security methods to ensure that only authorized users can establish a VPN and access the private network's resources. They typically also provide tamper proofing.

Most VPNs are SSL or IPsec VPNs. FortiOS supports both, as well as less common, weaker VPNs such as PPTP. In this lesson, we will focus on SSL-VPNs.

DO NOT REPRINT

© FORTINET

Comparing SSL-VPN and IPsec VPN

	SSL-VPN	IPsec VPN
Tunnel type:	<ul style="list-style-type: none"> HTTPS tunnel <ul style="list-style-type: none"> SSL/TLS layer 	<ul style="list-style-type: none"> IPsec tunnel <ul style="list-style-type: none"> ESP layer
Can be between:	<ul style="list-style-type: none"> Browser and FortiGate FortiClient and FortiGate 	<ul style="list-style-type: none"> FortiClient and FortiGate FortiGate and FortiGate FortiGate and compatible third-party IPsec VPN gateway FortiGate and compatible third-party IPsec VPN clients
Log in through:	<ul style="list-style-type: none"> HTTPS web page on FortiGate FortiClient <ul style="list-style-type: none"> fortissl virtual adapter 	<ul style="list-style-type: none"> IPsec client <ul style="list-style-type: none"> Site-to-site doesn't require IPsec client



FORTINET

© Fortinet Inc. All Rights Reserved.

5

How are SSL-VPNs different from IPsec VPNs?

The protocols are different. SSL and TLS are commonly used to encapsulate and secure e-commerce and online banking on the Internet (HTTP). SSL-VPNs use a similar technique, but often with non-HTTP protocols encapsulated. SSL resides higher up on the network stack than IP and, therefore, it usually requires more bits—more bandwidth—for SSL-VPN headers. In comparison, IPsec uses some special protocols. The primary protocol is ESP, which encapsulates and encrypts UDP, RDP, HTTP, or other protocols that are inside in the IPsec tunnel.

Also, IPsec VPN is a standard. It can interoperate with multiple vendors, and supports peers that are devices and gateways—not just user clients with FortiGate only, like SSL-VPN does.

The client software is also different. In an SSL-VPN, your web browser might be the only client software you need. You can go to FortiGate's SSL-VPN portal (an HTTPS web page), and then log in. Alternatively, you can install a FortiClient. This increases the number of protocols that can be sent through the VPN tunnel.

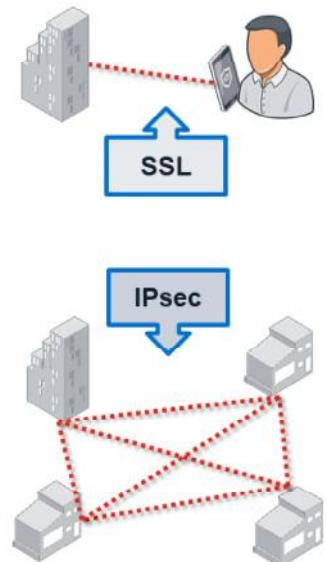
In comparison, to use IPsec VPN, you're usually required to install special client software, or have a local gateway, such as a desktop model FortiGate, in order to connect to the remote gateway. You might also need to configure firewalls between VPN peers to allow IPsec protocols. However, IPsec is a standard protocol supported by most vendors, so a VPN session can be established not only between two FortiGate devices, but also between different vendors' devices, and between a gateway and clients. It's highly extensible and configurable. By comparison, SSL-VPN can only be established between a computer and a vendor-specific gateway, such as FortiGate.

DO NOT REPRINT

© FORTINET

Comparing SSL-VPN and IPsec VPN (Contd)

	SSL-VPN	IPsec VPN
Category:	<ul style="list-style-type: none"> Vendor specific 	<ul style="list-style-type: none"> Industry standard
Set up:	<ul style="list-style-type: none"> Does not require installation Simpler setup <ul style="list-style-type: none"> Only client-to-FortiGate No user-configured settings Technical support less requested 	<ul style="list-style-type: none"> Requires installation Flexible setup <ul style="list-style-type: none"> Mesh and star topologies For clients or peer gateways Performance based: IPsec cryptography is faster in FortiOS
Better for:	<ul style="list-style-type: none"> Better for users, internet cafés, libraries, and so on 	<ul style="list-style-type: none"> Office-to-office traffic Data centers



FORTINET

© Fortinet Inc. All Rights Reserved.

6

After you've logged in, the SSL-VPN connects your computer to your private network. No user-configured settings are required, and firewalls are typically configured to allow outgoing HTTP, so technical support calls are less likely. Simplicity makes SSL-VPN ideal for non-technical users, or users who connect from public computers, such as those found in public libraries and Internet cafés.

In general, IPsec VPN is preferred when tunnels must be up continuously and interoperate with many types of devices, while SSL-VPN is preferred when people travel and need to connect to the office.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What does a VPN do?

- A. Extends a private network across a public network
- B. Protects a network from external attacks

2. Which statement about IPsec and SSL VPNs is true?

- A. Either an SSL-VPN or an IPsec VPN can be established between two FortiGate devices.
- B. Either an SSL-VPN or an IPsec VPN can be established between an end-user workstation and a FortiGate device.



© Fortinet Inc. All Rights Reserved.

7

DO NOT REPRINT

© FORTINET

Lesson Progress



Describe SSL-VPN



SSL-VPN Deployment Modes



Configuring SSL-VPNs



Realms and Personal Bookmarks



Hardening SSL-VPN Access



Monitoring and Troubleshooting

Good job! You now understand basic concepts related to the function of SSL-VPNs and how SSL-VPN is different from IPsec.

Now, you will learn about the SSL-VPN deployment modes supported by FortiGate.

DO NOT REPRINT

© FORTINET

SSL-VPN Deployment Modes

Objectives

- Describe the differences between SSL-VPN modes

After completing this section, you should be able to describe the differences between SSL-VPN modes. By demonstrating competence in understanding the different ways FortiGate allows SSL-VPN connections, you will be better able to design the configuration of your SSL-VPN.

DO NOT REPRINT**© FORTINET**

SSL-VPN Deployment Modes

- Tunnel mode
 - Accessed through a FortiClient
 - Requires a virtual adapter on the client's host

- Web mode
 - Requires only a web browser
 - Supports a limited number of protocols:
 - FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, Telnet, VNC, and Ping

VPN > SSL-VPN Portals

Edit SSL-VPN Portal

Name

Limit Users to One SSL-VPN Connection at a Time

Tunnel Mode

Enable Web Mode

OK **Cancel**

```
config vpn ssl web portal
  edit <portal-name>
    set tunnel-mode [enable|disable]
    set web-mode [enable|disable]
  end
```

© Fortinet Inc. All Rights Reserved.

10

There are two modes you can use to access an SSL-VPN. Both can build an SSL-VPN connection, but they don't support the same features.

Which should you choose?

It depends on which applications you need to send through the VPN, the technical knowledge of your users, and whether or not you have administrative permissions on their computers.

Tunnel mode supports the most protocols, but requires the installation of a VPN client, or more specifically, a virtual network adapter. To tunnel traffic using the virtual adapter, you must use FortiClient remote access feature or FortiClient VPN-only client.

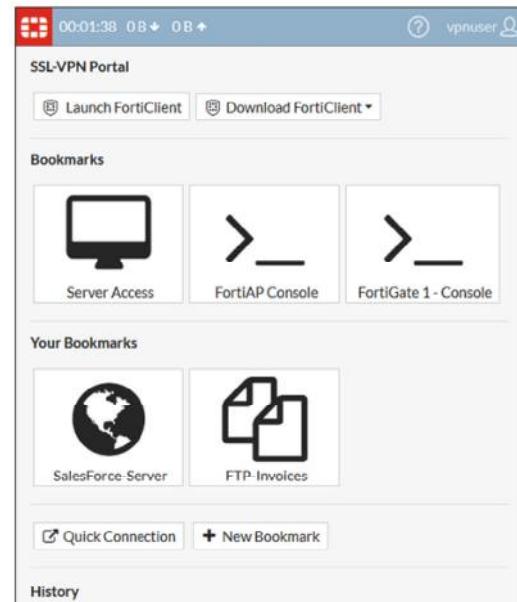
Web mode requires only a web browser, but supports a limited number of protocols.

DO NOT REPRINT

© FORTINET

Web Mode

- Connect to the FortiGate SSL-VPN portal from any browser
 - The web portal displays the status of SSL-VPN
 - The SSL-VPN stays up only while the SSL-VPN portal page is open
- Access internal network resources easily using:
 - Bookmarks
 - Quick connection
- Disadvantages:
 - Interaction with the internal network exclusively by browser
 - Through the SSL-VPN portal
 - External network applications cannot send data across the VPN
 - Limited number of protocols supported



FORTINET

© Fortinet Inc. All Rights Reserved.

11

Web access is the simplest SSL-VPN mode.

Like you would with any other HTTPS website, you simply log in to the SSL-VPN portal web page on FortiGate. It acts like a server-side reverse proxy, or a simple secure HTTP/HTTPS gateway, that connects you with the applications on the private network.

The **Bookmarks** section on the **SSL-VPN Portal** page contains links to all or some of the resources available for the user to access. The **Quick Connection** widget allows users to type the URL or IP address of the server they want to reach. A web SSL-VPN user makes use of these two widgets to access the internal network. The main advantage of web mode is that it does not usually require you to install extra software.

Web mode has two main disadvantages:

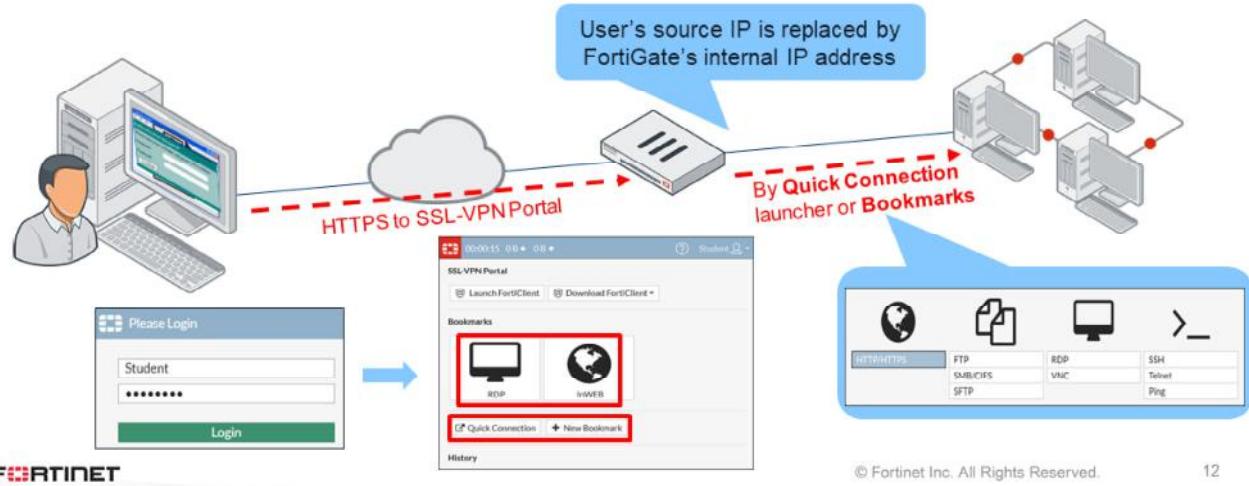
- All interaction with the internal network must be done using the browser exclusively (through the web portal). External network applications running on the user's PC cannot send data across the VPN.
- This a secure HTTP/HTTPS gateway mechanism that doesn't work for accessing everything, but just few popular protocols, such as HTTP, FTP, and Windows shares.

DO NOT REPRINT

© FORTINET

Web Mode (Contd)

1. Remote users connect to the SSL-VPN portal—HTTPS web page on FortiGate
2. Users authenticate.
3. Users access resources through the **Quick Connection** launcher or **Bookmarks**



© Fortinet Inc. All Rights Reserved.

12

How does web mode work?

1. Remote users establish a secure connection between the SSL security in the web browser and the FortiGate SSL-VPN portal, using HTTPS.
2. Once connected, users provide credentials in order to pass an authentication check.
3. Then, FortiGate displays the SSL-VPN portal that contains services and network resources for users to access.

Different users can have different portals with different resources and access permissions. Also notice the source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address.

DO NOT REPRINT

© FORTINET

Tunnel Mode

- Connect to FortiGate through FortiClient
 - Tunnel is up only while the SSL-VPN client is connected
 - FortiClient adds a virtual network adapter called `fortissl`
- FortiGate establishes the tunnel
 - Assigns a virtual IP address to the client from a pool of reserved addresses
 - All traffic is encapsulated with SSL/TLS
- Advantage:
 - Any IP network application on the client can send traffic through the tunnel
- Disadvantage:
 - Requires the installation of a VPN client

<http://www.forticlient.com/>



FORTINET

© Fortinet Inc. All Rights Reserved.

13

Tunnel mode is the second option FortiGate provides to access resources within an SSL-VPN.

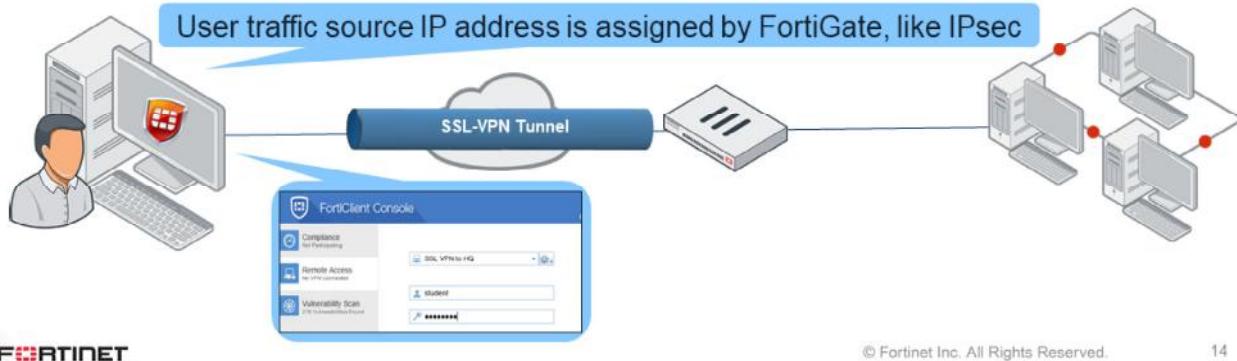
Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as `fortissl` to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated.

The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel. The main disadvantage is that tunnel mode requires the installation of a VPN software client, which requires administrative privileges.

DO NOT REPRINT**© FORTINET**

Tunnel Mode (Contd)

1. Remote users connect to the SSL-VPN gateway through the SSL-VPN client
2. Users authenticate
3. The virtual adapter creates the tunnel
4. Users access resources through an encrypted tunnel (SSL/TLS)



© Fortinet Inc. All Rights Reserved.

14

How does tunnel mode work?

1. Users connect to FortiGate through FortiClient.
2. Users provide credentials to successfully authenticate.
3. FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter (fortissl). This is the client's source IP address for the duration of the connection.
4. Then, users can access services and network resources through the encrypted tunnel.

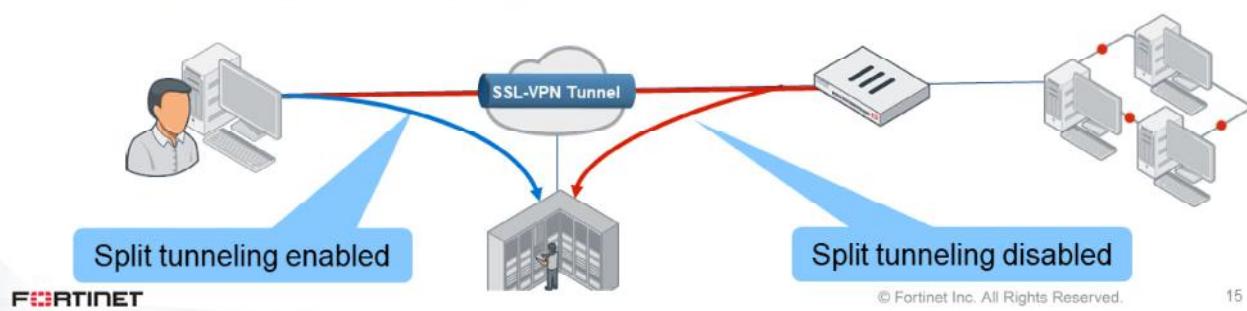
FortiClient encrypts all traffic from the remote computer and sends it over the SSL-VPN tunnel. FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

DO NOT REPRINT

© FORTINET

Tunnel Mode—Split Tunneling

- **Disabled:**
 - All traffic routes through an SSL-VPN tunnel to a remote FortiGate, then to the destination. This includes internet traffic
 - An egress firewall policy is required
 - Traffic inspection and security features can be applied
- **Enabled:**
 - Only traffic destined for the private network is routed through the remote FortiGate
 - Internet traffic uses the local gateway; unencrypted route
 - Conserves bandwidth and alleviates bottlenecks



FORTINET

© Fortinet Inc. All Rights Reserved.

15

Tunnel mode also supports split tunneling.

When split tunneling is disabled, all IP traffic generated by the client's computer—including Internet traffic—is routed across the SSL-VPN tunnel to FortiGate. This sets up FortiGate as the default gateway for the host. You can use this method in order to apply security features to the traffic on those remote clients, or to monitor or restrict internet access. This adds more latency and increases bandwidth usage.

When split tunneling is enabled, only traffic that is destined for the private network behind the remote FortiGate is routed through the tunnel. All other traffic is sent through the usual unencrypted route.

Split tunneling helps to conserve bandwidth and alleviates bottlenecks.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. A web-mode SSL-VPN user connects to a remote web server. What's the source IP address of the HTTP request the web server receives?
 - A. The remote user's IP address
 - B. The FortiGate device internal IP address
2. Which statement about tunnel-mode SSL-VPN is correct?
 - A. It supports split tunneling.
 - B. It requires a bookmarks.
3. A web-mode SSL-VPN user uses _____ to access internal network resources.
 - A. Bookmarks
 - B. FortiClient



© Fortinet Inc. All Rights Reserved.

16

DO NOT REPRINT

© FORTINET

Lesson Progress



Describe SSL-VPN



SSL-VPN Deployment Modes



Configuring SSL-VPNs



Realms and Personal Bookmarks



Hardening SSL-VPN Access



Monitoring and Troubleshooting

Good job! You now understand the SSL-VPN operation modes supported by FortiGate.

Now, you will learn about how to configure SSL-VPNs.

DO NOT REPRINT

© FORTINET

Configuring SSL-VPNs

Objectives

- Define authentication for SSL-VPN users
- Configure SSL-VPN portals
- Configure SSL-VPN settings
- Define firewall policies for SSL-VPNs

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

By demonstrating competence in configuring the SSL-VPN settings on FortiGate, you will be able to better design the architecture of your SSL-VPN tunnels.

DO NOT REPRINT**© FORTINET**

Configuring SSL-VPN

1. Set up user accounts and groups for remote SSL-VPN users
2. Configure SSL-VPN portals
3. Configure SSL-VPN settings
4. Create a firewall policy to and from the SSL-VPN interface
 - Accepts and decrypts packets
 - Allows traffic from SSL-VPN clients to the internal network and the reverse

Optionally:

5. Create a firewall policy to allow SSL-VPN traffic to the internet
 - Useful to allow all clients' traffic through FortiGate to Internet when split tunneling is disabled
 - FortiGate can be used to apply security profiles



FORTINET

© Fortinet Inc. All Rights Reserved.

19

To configure SSL-VPN, you must take these steps:

1. Configure user accounts and groups.
2. Configure the SSL-VPN portal.
3. Configure SSL-VPN settings.
4. Create a firewall policy to accept and decrypt packets. This policy is also used to provide access to internal networks.
5. Optionally, configure a firewall policy to allow traffic from the SSL-VPN client to the internet and apply security profiles. User traffic will go to the internet through FortiGate, where you can monitor or restrict client access to the internet.

Some steps can be configured in a different order than what is shown on this slide.

DO NOT REPRINT**© FORTINET**

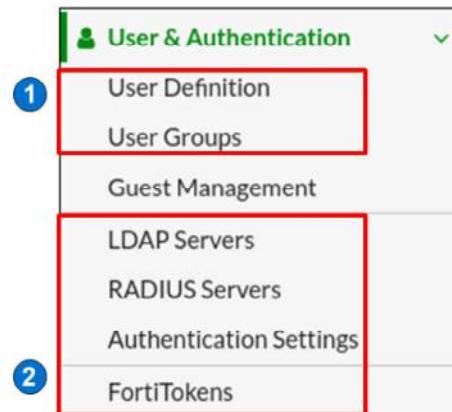
Step 1: Set Up User Accounts and Groups

1. Define user accounts and groups
2. Configure SSL-VPN authentication methods:
 - Local password authentication
 - Remote password authentication or server-based authentication such as LDAP, RADIUS, TACACS+
 - Two-factor authentication
 - Better security than just passwords



User name with password
(one factor)

Token code
(two factor)



FORTINET

© Fortinet Inc. All Rights Reserved.

20

The first step is to create the accounts and user groups for the SSL-VPN clients.

All FortiGate authentication methods, with the exception of remote password authentication using the Fortinet Single Sign-On (FSSO) protocol, can be used for SSL-VPN authentication. This includes local password authentication and remote password authentication (using the LDAP, RADIUS, and TACACS+ protocols).

FortiOS version 6.4 also support SSL-VPN authentication using certificate or both certificate and remote authentication (using the LDAP or RADIUS).

You can also configure two-factor authentication with FortiToken, for better security.

DO NOT REPRINT

© FORTINET

Step 2: Configure the SSL-VPN Portal

The screenshot shows the FortiGate SSL-VPN Portals configuration interface. On the left, there's a table listing three portals: full-access, tunnel-access, and web-access. The 'Tunnel Mode' column has green checkmarks for full-access and tunnel-access, while web-access has a red question mark. The 'Web Mode' column has green checkmarks for full-access and tunnel-access, while web-access has a green checkmark. A large blue arrow points from the table to a detailed configuration window for 'Tunnel Mode'. This window includes fields for 'Name' (full-access), 'Limit Users to One SSL-VPN Connection at a Time' (unchecked), 'Tunnel Mode' (selected), 'Enable Split Tunneling' (unchecked), 'Routing Address' (LOCAL_SUBNET selected), and 'Source IP Pools' (fortissl selected). Another blue arrow points from the 'Tunnel Mode' window to a 'Web Mode' configuration window. This window includes fields for 'Portal Message' (SSL-VPN Portal), 'Theme' (Blue selected), and various 'Show' options like Session Information, Connection Launcher, Login History, and User Bookmarks. A third blue arrow points from the 'Web Mode' window to an 'Admin-defined bookmarks' section. This section shows a table with one entry: 'Name' (FortiAP Console), 'Type' (TELNET selected), 'Host' (10.0.1.2), and 'Description' (Root AP / Mesh-1). At the bottom right of the configuration windows, it says '© Fortinet Inc. All Rights Reserved.' and '21'.

The second step is to configure the SSL-VPN portal(s). An SSL-VPN portal contains tools and resource links for the users to access.

In tunnel mode, when you enable split tunneling, you need to select a **Routing Address** setting, which usually specifies networks behind the FortiGate for the SSL-VPN users to access.

Also, for tunnel mode you need to select an IP pool for users to acquire an IP address when connecting. There is a default pool available within the address objects if you do not create your own.

If you enable web mode, you can customize the SSL-VPN portal and preconfigure bookmarks to appear for all users who log in to the SSL-VPN portal. Also, you can individually configure and link each portal to a specific user or user group, so they have access to only required resources.

DO NOT REPRINT

© FORTINET

Example: SSL-VPN Portal

- SSL-VPN portal page
 - Web mode only
- Widgets
 - **Bookmarks**, predefined by admin
 - **Your Bookmarks**, defined by user
 - **Quick Connection**, for users
- History
 - User logs
- **Download FortiClient**
 - SSL-VPN client for connections in tunnel mode

The screenshot shows the SSL-VPN Portal web interface at <https://<FortiGateIP>:<port>/remote/login>. The top navigation bar includes a clock (00:01:38), battery level (08+), signal strength (08+), and user info (vpnuser). The main content area is titled "SSL-VPN Portal". It features a "Bookmarks" section with three items: "Server Access" (monitor icon), "FortiAP Console" (greater-than icon), and "FortiGate 1 - Console" (greater-than icon). Below this is a "Your Bookmarks" section with two items: "SalesForce-Server" (globe icon) and "FTP-Invoices" (two documents icon). At the bottom of the portal are two buttons: "Quick Connection" (with a checked checkbox) and "+ New Bookmark". To the right of the portal is a sidebar with a "Download FortiClient" dropdown menu. The menu lists "Download FortiClient" with icons for iOS, Android, Windows, and Mac. Below the dropdown are sections for "Admin-defined bookmarks" (listing the same three items as the portal) and "User's bookmarks" (listing the same two items as the portal). At the very bottom of the sidebar is a "Protocols" section with icons for HTTP/HTTPS, FTP, SMB/CIFS, SFTP, RDP, VNC, SSH/Telnet, and Ping.

FORTINET

22

This slide shows an example of an SSL-VPN web mode portal page after the user logs in. It allows you to download a FortiClient VPN client from the **Download FortiClient** drop-down list. This FortiClient VPN client is used to connect to SSL-VPN in tunnel mode.

Also notice the SSL-VPN bookmarks provide links to network resources. The settings for web mode allow users to:

- Use the administrator-defined bookmarks in the **Bookmarks** section. Users cannot modify administrator-added bookmarks.
- Use the widget in the **Your Bookmarks** section to add personal bookmarks.
- Access network resources directly using the **Quick Connection** widget.

Now, you will learn more about the protocols and server applications available on the SSL-VPN portal (web mode) through the **Bookmarks** or **Quick Connection** widget.

DO NOT REPRINT

© FORTINET

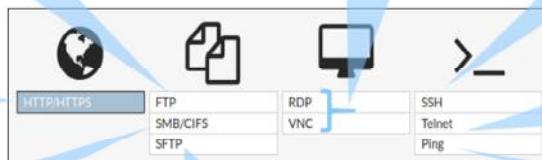
SSL-VPN Bookmarks

Allows you to transfer files between the SSL-VPN client and a remote host or server

Allows you to remotely control a computer

Allows the exchange of data between two hosts, using a secure channel

Access websites



Allows you to log in to a remote host using your computer as a virtual text-only terminal

Implements SMB protocol to support file sharing between SSL-VPN client and a remote host/server

Allows you to transfer files over SSH between the SSL-VPN client and a remote host or server

Allows you to ping IP address or host name to check reachability

FORTINET

© Fortinet Inc. All Rights Reserved.

23

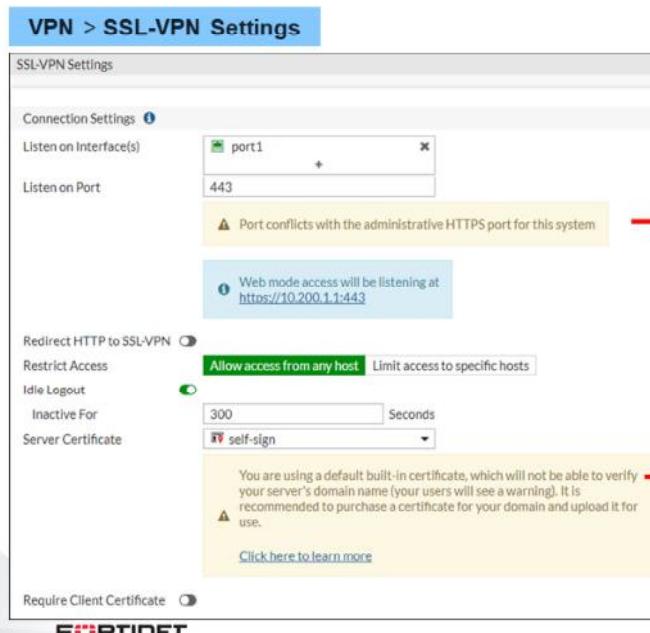
Depending on the web portal configuration, one or more of the following are available:

1. HTTP/HTTPS allows you to access private websites.
2. File Transfer Protocol (FTP), allows you to transfer files between the SSL-VPN client and hosts or servers located in the private network.
3. Virtual Network Computing (VNC), allows you to remotely control another computer within the private network.
4. Remote Desktop Protocol (RDP), similar to VNC, allows you to remotely control a computer running Microsoft Terminal Services.
5. Secure Shell (SSH), allows the exchange of data between two hosts using a secure channel.
6. Teletype Network Emulation (TELNET), enables a virtual, text-only terminal in the SSL-VPN to log in to a remote host.
7. Ping, allows you to ping an IP address or a host name to check reachability.
8. SSH File Transfer Protocol (SFTP), allows you to transfer files over SSH between the SSL-VPN client and hosts or servers located in the private network.
9. SMB/CIFS, implements the Server Message Block (SMC) protocol to support file sharing between the SSL-VPN client and a remote host or server in the private network. Windows file sharing through SMB/CIFS is supported through shared directories.

DO NOT REPRINT

© FORTINET

Step 3: Configure SSL-VPN Settings



- FortiGate interface for SSL-VPN portal:
 - Default port is 443
 - By default, admin GUI interface and SSL-VPN portal use same HTTPS port
 - Advised to use different interfaces for admin GUI access and SSL-VPN portal
 - If both services use the same interface and port, only the SSL-VPN portal appears
- Restrict access to known hosts.
- SSL-VPN time out:
 - Default idle: 300 sec (5 min)
- Digital server certificate:
 - Self-signed certificate used by default
 - To avoid browser security warnings, use a certificate issued by a public CA, or install the self-signed certificate on all clients

© Fortinet Inc. All Rights Reserved.

24

After you configure the SSL-VPN portal, the next step is to configure the SSL-VPN settings.

Let's start with the **Connection Settings** section. Here, you need to map a FortiGate interface to the SSL-VPN portal. The default port for the SSL-VPN portal is 443. This means users need to connect to the IP address of the FortiGate interface mapped to the SSL-VPN portal, using port 443-HTTPS. If you enable **Redirect HTTP to SSL-VPN**, users who connect using HTTP (TCP port 80) will be redirected to HTTPS.

Port 443 is the standard default port for administration of the HTTPS protocol. This is convenient because users do not need to specify the port in their browsers. For example, <https://www.example.com/> automatically uses port 443 in any browser. This is considered a valid setup on FortiGate because you usually don't access the SSL-VPN login through every interface. Likewise, you generally don't enable administrative access on every interface of your FortiGate. So, even though the ports may overlap, the interfaces that each one uses to access may not. However, if the SSL-VPN login portal and HTTPS admin access both use the same port, and are both enabled on the same interface, only the SSL-VPN login portal will appear. To have access to both portals on the same interface, you need to change the port number for one of the services. If you change the administrator access port, this will affect the port number for that service on all interfaces.

Also, an inactive SSL-VPN is disconnected after 300 seconds (5 minutes) of inactivity. You can change this timeout using the **Idle Logout** setting on the GUI.

Finally, like other HTTPS websites, the SSL-VPN portal presents a digital certificate when users connect. By default, the portal uses a self-signed certificate, which triggers the browser to show a certificate warning. To avoid the warning, you should use a digital certificate signed by a publicly known certificate authority (CA). Alternatively, you can load the FortiGate self-signed digital certificate into the browser as a trusted authority.

DO NOT REPRINT

© FORTINET

Step 3: Configure SSL-VPN Settings (Contd)

- Define the IP range for the SSL-VPN
 - IPs are assigned to clients' virtual adapters while joined to VPN
- Resolve names by DNS server
 - Use internal DNS if resolving internal domain names
 - Optionally, resolve names by WINS servers
- Specify authentication portal mapping
 - Specify portals for each user or group
 - Define portal for all other users or groups
 - It cannot be deleted

The screenshot shows the 'VPN > SSL-VPN Settings' page. Under 'Tunnel Mode Client Settings', there are two tabs: 'Automatically assign addresses' (selected) and 'Specify custom IP ranges'. A note states: 'Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210'. Under 'DNS Server', there are two tabs: 'Same as client system DNS' (selected) and 'Specify'. Under 'Specify WINS Servers', there is a 'Specify' button. In the 'Authentication/Portal Mapping' section, there is a table:

Users/Groups	Portal
Teachers	web-access
Accountants	full-access
All Other Users/Groups	tunnel-access

FORTINET

© Fortinet Inc. All Rights Reserved.

25

Define the tunnel-mode client settings and the authentication rules that map users to the appropriate portal.

When users connect, the tunnel is assigned an IP address. You can choose to use the default range or create your own range. The IP range determines how many users can connect simultaneously.

DNS server resolution is only effective when the DNS traffic is sent over the VPN tunnel. Generally, this will be the case only when split tunnel mode is disabled and all traffic is being sent from the user's computer across the tunnel.

Finally, you can allow different groups of users to access different portals. In the example shown on this slide, teachers have access only to the web portal. Accountants can use FortiClient to connect in tunnel mode.

DO NOT REPRINT

© FORTINET

Step 4: Firewall Policies To and From SSL-VPN Interface

- Listens for connections to the SSL-VPN portal
- **ssl.<vdom_name>** policy enables portal with user authentication
- The selected **Incoming Interface** is the SSL-VPN virtual interface
 - Example: **ssl.root** for root VDOM
- Passes decrypted traffic to the selected **Outgoing Interface**

Policy & Objects > Firewall Policy

Name	SSL VPN Access
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port3
Source	SSLVPN_TUNNEL_ADDR1 Accountants SSL_VPN_USERS Teachers
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	✓ ACCEPT ✘ DENY

FORTINET

© Fortinet Inc. All Rights Reserved.

26

The fourth, and last, mandatory step involves creating firewall policies for logging on.

SSL-VPN traffic on FortiGate uses a virtual interface called `ssl.<vdom_name>`. Each virtual domain (VDOM) contains a different virtual interface based on its name. By default, if VDOMs are not enabled, then the device operates with a single VDOM called `root`.

To activate and successfully log in to the SSL-VPN, there must be a firewall policy from the SSL-VPN interface to the interface to which you want to allow access for the SSL-VPN users, including all of the users and groups that can log in as the source. Without a policy like this, no login portal is presented to users.

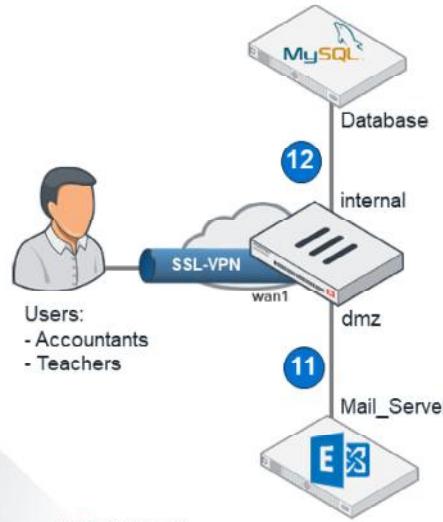
If there are resources behind other interfaces that users need access to, then you need to create additional policies that allow traffic from `ssl.root` to exit those interfaces.

DO NOT REPRINT

© FORTINET

Example: Access to Internal Resources

- All traffic generated by the user exits through the `ssl.<vdom_name>` interface
 - Applies to both web and tunnel mode



edit 11

```
set srcintf ssl.root
set dstintf dmz
set srcaddr all
set dstaddr Mail_Server
set action accept
set schedule always
set service ALL
set groups Accountants
next
```

edit 12

```
set srcintf ssl.root
set dstintf internal
set srcaddr all
set dstaddr Database
set action accept
set schedule always
set service ALL
set groups Teachers
next
```

© Fortinet Inc. All Rights Reserved.

27

Any traffic from SSL-VPN users, whether in web portal or tunnel mode, exits from the `ssl.<vdom_name>` interface.

This slide shows an example of firewall policies that are configured to allow access to resources behind other interfaces that users need access to when connected through SSL-VPN.

DO NOT REPRINT

© FORTINET

Step 5: Create a Firewall Policy to Access the Internet

- Create a firewall policy to allow internet access
 - From **ssl.root** to egress interface
- Useful when split tunneling is disabled
- Apply security profiles to restrict user access to the Internet

Policy & Objects > Firewall Policy

Name	Internet Access
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port1
Source	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> Accountants <input checked="" type="checkbox"/> SSL_VPN_USERS <input checked="" type="checkbox"/> Teachers
Destination	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> +
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY



© Fortinet Inc. All Rights Reserved.

28

Optionally, if split tunneling is disabled, you need to create an additional firewall policy from **ssl.root** to the egress interface to allow clients access to the internet.

You can also apply security profiles to this firewall policy to restrict user access to the internet.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following steps is necessary to configure SSL-VPN connections?
 A. Create firewall policy from SSL-VPN interface to internal interface
 B. Enable event logs for SSL-VPN traffic: users, VPN, and endpoints

2. What action may allow internet access in tunnel mode if the remote network does not allow internet access to SSL-VPN users?
 A. Enable split tunneling
 B. Configure the DNS server to use the same as the client's system DNS

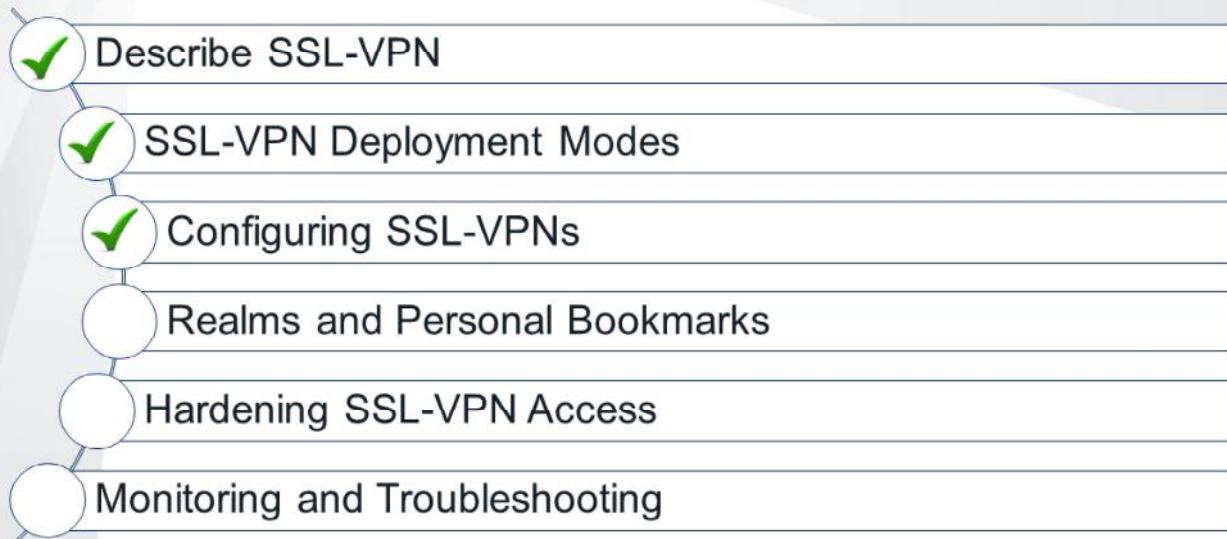


© Fortinet Inc. All Rights Reserved.

29

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand how to configure the FortiGate for SSL-VPN connections.

Now, you'll learn how to create multiple SSL-VPN login sites for different user groups, and manage user-added bookmarks.

DO NOT REPRINT

© FORTINET

Realms and Personal Bookmarks

Objectives

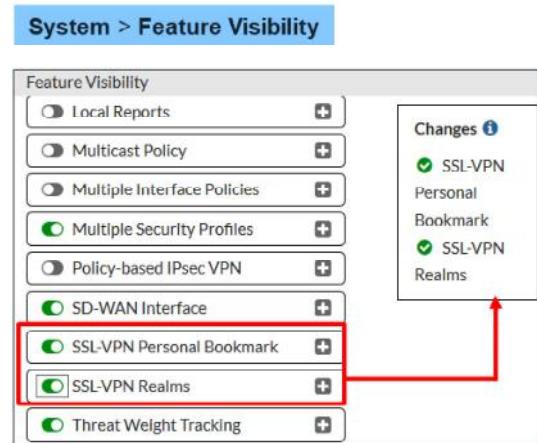
- Configure realms for the SSL-VPN portal
- Configure personal bookmarks for the SSL-VPN portal

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

By demonstrating competence in understanding these topics, you will be able to create multiple SSL-VPN login sites for different user groups and manage user-specific bookmarks.

DO NOT REPRINT**© FORTINET**

How to Find Realms and Personal Bookmarks Settings



- By default, all SSL-VPN users using the same portal will see the same bookmarks
- Enable features for customizing realms and user bookmarks:
 - **SSL-VPN Realms**
 - **SSL-VPN Personal Bookmark**
- By default, these features are hidden
 - To make the feature visible on the GUI, click **System > Feature Visibility**
 - Displayed on the **VPN** menu

FORTINET

© Fortinet Inc. All Rights Reserved.

32

By default, all SSL-VPN users will see the same bookmarks, configured by an administrator, and the same theme.

By default, the features for customizing SSL-VPN realms and SSL-VPN bookmarks are hidden on the FortiGate GUI.

DO NOT REPRINT

© FORTINET

Configure Realms

- By default, all users connect to the same login page for SSL-VPN portal
 - <https://10.0.1.254:10443>
- Customize URLs for specialized portals (realms)
 - <https://10.0.1.254:10443/Accountants>
 - <https://10.0.1.254:10443/Teachers>

```
config vpn ssl web realm
  edit Accountants
    set max-current-users 500
    set login page <HTML content>
  next
end
```

The screenshot shows the 'Edit SSL-VPN Realm' screen for the 'Accountants' realm. The 'URL Path' is set to '/Accountants'. The 'Limit Concurrent Users' is set to 500. The 'Customize Login Page' button is highlighted with a red box. An arrow points down to a detailed view of the 'SSL-VPN Login Page' HTML code, which includes fields for Name and Password, and a 'Login' button.

© Fortinet Inc. All Rights Reserved.

33

To add flexibility to your SSL-VPN deployment, you may consider configuring SSL-VPN realms.

The realms are custom login pages. They are usually for user groups, such as your accounting team and your sales team, but can be for individual users as well. With realms, users and user groups can access different portals based on the URL they enter.

With different portals, you can customize each login page separately, as well as limit concurrent user logins separately.

Example of realms on a FortiGate:

<https://192.168.1.1>
<https://192.168.1.1/Accounting>
<https://192.168.1.1/TechnicalSupport>
<https://192.168.1.1/Sales>

DO NOT REPRINT

© FORTINET

Apply Realms

- In **SSL-VPN Settings**, apply realms on the **Authentication/Portal Mapping** page
 - Customize portals for each user/group with realms.

The screenshot illustrates the process of applying realms in the SSL-VPN Settings. It consists of three main parts:

- SSL-VPN Settings > Authentication/Portal Mapping:** A table showing user groups and their corresponding realms and portals. A blue callout points to the 'Edit' button in the header bar, which is highlighted with a red box. The table rows are:

Users/Groups	Realm	Portal
Teachers	/Teachers	web-access
Accounts	/	full-access
All Other Users/Groups	/	tunnel-access
- Edit Authentication/Portal Mapping:** A dialog box where a new realm is being added. A red box highlights the 'Specify' button next to the 'Default realm'. The list of realms includes /Accounts and /Teachers, with /Accounts highlighted in green.
- Browser Login Screen:** A screenshot of a web browser showing a 'Please Login' page with fields for 'Username' and 'Password' and a 'Login' button. The URL in the address bar is https://10.200.1.1:10443/remote/login/realm=Accounts&lang=en, with the 'realm' parameter highlighted by a red box.

After realms are set up, you must apply them in the **SSL-VPN Settings** window.

Configure the authentication rules in order to map users to the appropriate realm. These settings allow different groups of users to access the defined portals by different realms.

In the example shown on this slide, teachers have access only to their own realms. If they need access to the root realm to see the global portal, you would need to add an additional authentication rule for them.

DO NOT REPRINT

© FORTINET

SSL-VPN Personal Bookmarks

VPN > SSL-VPN Portals

Edit SSL-VPN Portal	<input checked="" type="checkbox"/>
Enable Web Mode	<input checked="" type="checkbox"/>
Portal Message	
Theme	
Show Session Information	<input checked="" type="checkbox"/>
Show Connection Launcher	<input checked="" type="checkbox"/>
Show Login History	<input checked="" type="checkbox"/>
User Bookmarks	<input checked="" type="checkbox"/>

SSL-VPN Portal (Web Mode)



VPN > SSL-VPN Personal Bookmarks

User	User Group	Bookmarks
Accountant-1	Accounts	★ Finance-FTP
Accountant-2	Accounts	★ SalesForce-Server ★ FTP-Invoices
Student	SSL_VPN_USERS	
Teacher-1	Teachers	★ Training-Server

FORTINET

- Show user-added bookmarks through the SSL-VPN web portal
 - Enable option on **VPN > SSL-VPN Portal** page
 - These are not the administrator-defined bookmarks
- Administrators can:
 - GUI: View and delete user bookmarks
 - CLI: Create bookmarks for a specific user
- Supports SSO for any link that requires authentication

```
config vpn ssl web user-bookmark
edit Accountant-1#Accounts
  config bookmarks
    edit Finance-FTP
      set apptype ftp
      set folder ftp://finance@ftp.acme.com/Invoices
      set sso disable
next
```

© Fortinet Inc. All Rights Reserved.

35

When users log in to their individual portal, there is an option that allows them to create their own bookmarks. An administrator must enable the **User Bookmarks** option on the **SSL-VPN Portal** page to allow this.

Administrators can view and delete user-added bookmarks on the **SSL-VPN Personal Bookmarks** page. This allows administrators to monitor and remove any unwanted bookmarks that do not meet with corporate policy.

On the FortiGate CLI, you can create bookmarks for each user. These bookmarks will appear even if the user bookmark option is disabled in the portal, because that option only affects the user's ability to create and modify their own bookmarks—not administrator-defined bookmarks.

Depending on the type of bookmark you want to create, you may need to configure additional information that the application requires, such as URLs for websites and folders for FTP sites.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which statement about SSL-VPN realms is correct?
 A. SSL-VPN realms allow access to different SSL-VPN portals by user groups
 B. SSL-VPN realms allow unlimited concurrent SSL-VPN users

2. Which FortiGate interface allows administrators to create user-specific bookmarks?
 A. Command line interface (CLI)
 B. Graphical user interface (GUI)

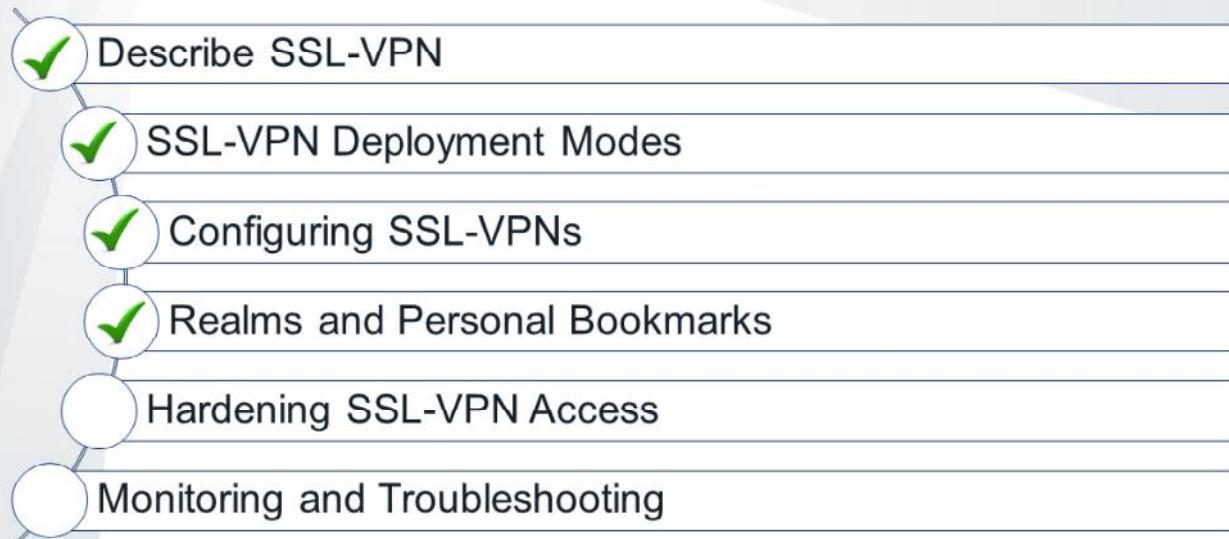


© Fortinet Inc. All Rights Reserved.

36

DO NOT REPRINT**© FORTINET**

Lesson Progress



Good job! You now understand how to configure SSL-VPN realms and review user-added bookmarks.

Now, you'll learn how to harden SSL-VPN access.

DO NOT REPRINT

© FORTINET

Hardening SSL-VPN Access

Objectives

- Configure client integrity checking
- Apply two-factor authentication using security certificates
- Restrict clients by IP and MAC address

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

By demonstrating competence in understanding how to strengthen security for SSL-VPN accesses, you will be able to restrict users, ensuring that your internal network is secure, and limiting the possibility of attacks and viruses entering the network from an outside source.

DO NOT REPRINT**© FORTINET**

Client Integrity Checking

- SSL-VPN gateway checks client integrity
 - Requires Microsoft Windows
- Detects client security applications recognized by the **Windows Security Center**
 - Antivirus and firewall software
 - Security attributes recorded on the client's computer
- Checks the status of applications through their globally unique identifier (GUID)
 - Custom host checks
- Determines the state of the applications
 - Active/inactive
 - Current version number
 - Signature updates



FORTINET

© Fortinet Inc. All Rights Reserved.

39

When a user connects to your network through an SSL-VPN, a portal is established between your network and the user PC. The VPN session is secured natively in two ways: the connection is encrypted and the user must log in with their credentials, such as a username and password. However, you can configure additional security checks to increase the security of the connection.

One method of increasing your security is through client integrity checking. Client integrity ensures that the connecting computer is secure by checking whether specific security software, such as antivirus or firewall software, is installed and running. This feature only supports Microsoft Windows clients, because it accesses the Windows Security Center to perform its checks. Alternatively, you can customize this feature to check the status of other applications using their GUID. The GUID is a unique ID in the Windows Configuration Registry that identifies each Windows application. Client integrity can also check the current software and signature versions for the antivirus and firewall applications.

Client integrity checking is applicable to both web mode and tunnel mode.

DO NOT REPRINT

© FORTINET

Configure Client Integrity Check

- External vendor software ensures client integrity
FortiClient, AVG, CA, F-Secure, Kaspersky, McAfee, Norton, Symantec, Panda, Sophos, Trend-Micro, Zone Alarm,...
- Check if software is installed on host client
 - Configure through CLI or GUI
 - Software needs to be updated and recognized by Windows Security Center
 - None – No host checking
 - av – Verify if there is any antivirus software
 - fw – Verify if there is any firewall software
 - av-fw – Verify if there is both antivirus and firewall software
 - Custom – Verify custom or proprietary software
 - If not, FortiGate rejects SSL-VPN connection attempt

```
config vpn ssl web host-check-software
show
```

VPN > SSL-VPN Portals > portal-name

<input checked="" type="radio"/> Host Check	Realtime AntiVirus	Firewall	Enable both
Type	Restrict to specific OS versions <input type="checkbox"/>		

```
config vpn ssl web portal
edit <portal_name>
  set host-check [none|av|fw|av-fw|custom]
  set host-check-interval <seconds>
end
```

Administrators should have in-depth knowledge of the Windows OS to use and maintain this feature

© Fortinet Inc. All Rights Reserved.

40

FORTINET

The client integrity check is performed while the VPN is still establishing, just after user authentication has finished. If the required software is not running on the client's PC, the VPN connection attempt is rejected, even with valid user credentials. Client integrity is enabled per web portal, and can be configured using CLI commands or the FortiGate GUI.

The list of recognized software, along with the associated registry key value, is available on the CLI only. Software is split into three categories: antivirus (av), firewall (fw), and custom. Custom is used for customized or proprietary software that an organization may require. Administrators can configure av, fw, or both settings on the GUI or CLI, but custom setting is only available on the CLI.

Administrators can also configure OS versions and patch settings to allow or deny VPN connections from specific OS versions.

The disadvantage of enabling client integrity checking is that it can result in a lot of administrative overhead because of the following factors:

- All users must have their security software updated in order to successfully establish a connection.
- Software updates can result in a change to the registry key values, which can also prevent a user from successfully connecting.

As such, administrators must have in-depth knowledge of the Windows operating system and subsequent registry behavior in order to properly make extended use of, as well as maintain, this feature.

DO NOT REPRINT**© FORTINET**

Two-Factor Authentication Through Security Certificates

- 1. Requesting a client's certificates**
 - Clients authenticate using certificates
 - Install a local certificate in a client's browser
 - Install the corresponding CA certificate on FortiGate

```
config vpn ssl settings
    set reqclientcert enable
end
```

FortiGate prompts client browser for its client-side certificate

- 2. Using FortiGate-issued certificates**

- Use FortiGate CA certificate
- Install FortiGate CA certificate in a client's browser
- Default certificate is *Fortinet_CA_SSL*

```
config vpn ssl settings
    set servercert <certificate>
end
```

Use the certificate that FortiGate uses to identify itself to SSL-VPN clients

© Fortinet Inc. All Rights Reserved.

41

You can also harden your SSL-VPN connections by applying two-factor authentication through security certificates (X.509), by either:

- Requiring clients to authenticate using their certificates
When the remote client initiates a connection, FortiGate prompts the client browser for its client-side certificate as part of the authentication process.
- Installing FortiGate's CA certificates on your clients' browsers

DO NOT REPRINT**© FORTINET**

Restricting Hosts by IP Address

- Set up IP restriction rules to allow specific hosts
 - Using the GUI:
 - Select **Limit access to specific hosts**
 - Using the CLI, enter:
 - set source-address
- Set up IP restriction rules to exclude specific hosts by CLI



```
config vpn ssl setting
  set source-address REMOTE_WINDOWS
end
```

```
config vpn ssl setting
  set source-address-negate [enable|disable]
  set source-address6-negate [enable|disable]
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

42

You can secure SSL-VPN access by restricting host connection addresses. Setting up IP restriction rules can be very useful when considering proper security configuration. Not all IPs need access to the login page. This method allows you to set up rules to restrict access from specific IPs. One simple rule is to allow or disallow traffic based on geographic IP addresses.

You must select **Limit access to specific hosts** and specify the IP address or network in the **Hosts** field. This will allow only those users to access the login page. The **Allow access from any host** setting allows all IPs to connect.

On the CLI, you can configure the VPN SSL setting to disallow specific IPs.

DO NOT REPRINT**© FORTINET**

Restricting Hosts by MAC Address

- Check against the client's MAC address
- Ensure only specific computers or devices are connecting to the SSL-VPN
- Link clients to specific portals by MAC address
- Hooks into the Windows Security Center

```
config vpn ssl web portal
    edit <portal-name>
        set mac-addr-check [enable|disable]
        set mac-addr-action [allow | deny]
        config mac-addr-check-rule
            edit <rule-id>
                set mac-addr-list 01:01:01:01:01:01 08:00:27:d4:06:5d
                set mac-addr-mask 48
            end
        end
    end
```



© Fortinet Inc. All Rights Reserved.

43

You can also configure FortiGate to check against the client's MAC address when remote users attempt to log in to the SSL-VPN portal. This makes sure that only specific computers or devices are connecting to the SSL-VPN tunnel.

This setting offers better security because passwords might be compromised. MAC addresses can be tied to specific portals and can be either the entire MAC address or a subset of the address.

This setting is supported only with tunnel mode deployment.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Why is it necessary to run a client integrity check (host-check)?
 A. To check whether specific security software is running on SSL-VPN users' computers
 B. To check whether a specific security certificate is running on SSL-VPN users' web browsers

2. Which security action restricts SSL-VPN connections from users located in a specific country or region?
 A. Restricting hosts by MAC address
 B. Restricting hosts by IP address



© Fortinet Inc. All Rights Reserved.

44

DO NOT REPRINT**© FORTINET**

Lesson Progress



Describe SSL-VPN



SSL-VPN Deployment Modes



Configuring SSL-VPNs



Realms and Personal Bookmarks



Hardening SSL-VPN Access



Monitoring and Troubleshooting

Good job! You now understand how to strengthen security for SSL-VPN access.

Now, you'll learn how to monitor SSL-VPN sessions, review logs, configure SSL-VPN timers, and troubleshoot common issues.

DO NOT REPRINT

© FORTINET

Monitoring and Troubleshooting

Objectives

- Monitor SSL-VPN connected users
- Review SSL-VPN logs
- Configure SSL-VPN timers
- Troubleshoot common SSL-VPN issues
- Identify hardware acceleration components for SSL-VPN

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

By demonstrating competence in SSL-VPN monitoring and troubleshooting, you will be able to avoid, identify, and solve common issues and misconfigurations.

DO NOT REPRINT**© FORTINET**

Monitoring SSL-VPN Sessions

- Monitor which SSL-VPN users are connected
 - GUI: **Monitor > SSL-VPN Monitor**
- Shows SSL-VPN user names, connection times, and IP addresses
 - For tunnel mode, **Active Connections** displays IP address assigned to `fortissl` virtual adapter
- Force end user disconnection
 - Right-click the user name and select **End Session**

Dashboard > Network > SSL-VPN

Username	Last Login	Remote Host	Active Connections
student	2020/04/08 07:17:35	10.200.3.1	Tunnel: 10.212.134.200
Accountant-1	08/07/2020 07:17:20	10.200.3.1	

Right-click to terminate an active SSL-VPN session

web user

Tunnel mode user: shows SSL-VPN IP address assigned during the session

© Fortinet Inc. All Rights Reserved.

47

You can monitor which SSL-VPN users are connected on the **SSL-VPN** widget. This shows the names of all SSL-VPN users that are currently connected to FortiGate, their IP addresses (both inside the tunnel and outside), and connection times.

When a user connects using tunnel model, the **Active Connections** column shows the IP address assigned by FortiGate to the `fortissl` virtual adapter on the client's computer. Otherwise, the user is connected only to the web portal page.

DO NOT REPRINT

© FORTINET

SSL-VPN Logs

The screenshot shows the FortiGate Log & Report interface. In the main menu, the 'Events' button is highlighted with a red box and a red arrow points to it. The 'Log & Report' menu has several other options like Forward Traffic, Local Traffic, Sniffer Traffic, SSL, DNS Query, Application Control, Intrusion Prevention, Anomaly, Log Settings, Threat Weight, and Email Alert Settings.

In the sub-menu under 'Events', 'VPN Events' is selected and highlighted with a green box. Below it are other event types: SD-WAN Events, System Events, Router Events, User Events, HA Events, Security Rating Events, WiFi Events, and SDN Connector Events.

Two callout boxes show specific log entries:

- VPN Events:**

Date/Time	Level	Action	Status	Message
2020/01/21 04:50:...	INFO	ssl-new-con		SSL new connection
2020/01/21 04:50:...	INFO	tunnel-down		SSL tunnel shutdown
2020/01/21 04:49:...	INFO	tunnel-stats		SSL tunnel statistics
2020/01/21 04:39:...	INFO	tunnel-up		SSL tunnel established
2020/01/21 04:39:...	INFO	ssl-new-con		SSL new connection
- User Events:**

Date/Time	Level	User	Action	Message
2020/01/21 04:50:33	INFO	Student	auth-logout	User Student removed from auth logon
2020/01/21 04:39:02	INFO	Student	auth-logon	User Student added to auth logon

Review Points:

- Review if the SSL-VPN tunnel is established or closed
- Review the authentication action related to SSL-VPN users
- Review SSL-VPN connections in tunnel mode with FortiClient

FORTINET

© Fortinet Inc. All Rights Reserved.

48

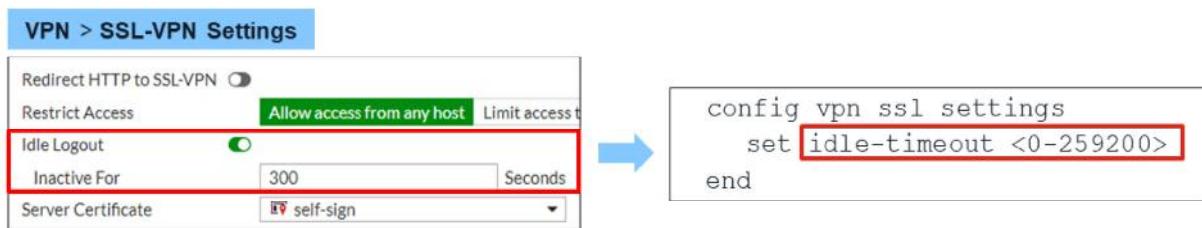
You can also review SSL-VPN logs. On **Log & Report > Events**:

- Select **VPN Events** to show new connection requests, and if the SSL-VPN tunnel is established or closed.
- Select **User Events** to see the authentication action related to SSL-VPN users.

DO NOT REPRINT**© FORTINET**

SSL-VPN Idle Timeout vs. Authentication Session

- Firewall policy authentication session is associated with SSL-VPN tunnel session
 - Firewall policy authentication session is forced to end when SSL-VPN tunnel session ends
 - Prevents reuse of authenticated SSL-VPN firewall sessions (not yet expired) by a different user, after the initial user terminates the SSL-VPN tunnel session
- SSL-VPN authentication is not subject to the firewall authentication timeout setting
 - It has a separate idle setting: default 300 seconds

**FORTINET**

© Fortinet Inc. All Rights Reserved.

49

When an SSL-VPN is disconnected, either by the user or through the SSL-VPN idle setting, all associated sessions in the FortiGate session table are deleted. This prevents the reuse of authenticated SSL-VPN sessions (not yet expired) after the initial user terminates the tunnel.

The SSL-VPN user idle setting is not associated with the firewall authentication timeout setting. It is a separate idle option specifically for SSL-VPN users. A remote user is considered idle when FortiGate does not see any packets or activity from the user within the configured timeout period.

DO NOT REPRINT**© FORTINET**

SSL-VPN Timers

- Set up timers to avoid logouts when SSL-VPN users are connected over high latency connections

- DTLS hello timeout—default 10 seconds
- Login timeout—default 30 seconds

```
config vpn ssl settings
    set login-timeout <10-180>
    set dtls-hello-timeout <10-60>
    set http-request-header-timeout <1-60>
    set http-request-body-timeout <1-60>
end
```

- Timers can also help to mitigate DoS attacks within SSL-VPN caused by partial HTTP requests, such as Slowloris and R-U-Dead-Yet



© Fortinet Inc. All Rights Reserved.

50

When connected to SSLVPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under `config vpn ssl settings` have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL-VPN connections.

Also, timers can help you to mitigate vulnerabilities such as Slowloris and R-U-Dead-Yet, that allow remote attackers to cause a denial of service through partial HTTP requests.

DO NOT REPRINT

© FORTINET

Best Practices for Common SSL-VPN Issues

- For web mode connections, make sure that:
 - Cookies are enabled and the internet privacy options are set to high in your web browser
 - SSL-VPN clients are following the proper URL structure: <https://<FortiGateIP>:<port>>
- For tunnel mode connections, make sure that:
 - The FortiClient version is compatible with the FortiOS firmware
 - Refer to release notes for product compatibility and integration
 - Split tunneling is enabled to allow internet access without backhauling all user's data to the remote network, or
 - Split tunneling is disabled and an egress firewall policy is created for SSL-VPN connections
- For general SSL-VPN connections, make sure that:
 - Users are connecting to the correct port number
 - To check SSL-VPN port assignment, click **VPN > SSL-VPN Settings**
 - Firewall policies include SSL-VPN groups or users, and the destination address
 - The timeout timer is configured to flush inactive sessions after a short time
 - Users are encouraged to log out if they are not using the network resources only accessible by SSL-VPN



© Fortinet Inc. All Rights Reserved.

51

The following are some best practices to keep in mind when using SSL-VPNs. These best practices can also be helpful in many SSL-VPN troubleshooting situations:

- Enable cookies in your web browser
- Set Internet privacy options to high in your web browser
- Use a FortiClient version that is compatible with your FortiOS firmware
- Enable split tunneling or create an egress firewall policy for SSL-VPN connections in order to allow access for external resources
- Connect to the correct port number
- Add SSL-VPN groups, SSL-VPN users, and destination addresses to the firewall policies
- Flush inactive sessions by timeout

DO NOT REPRINT**© FORTINET**

Useful Troubleshooting Commands

```
# diagnose debug enable  
# diagnose vpn ssl <...>  
    list → Show current connections  
    info → General SSL-VPN information  
    statistics → Show statistics about memory usage on FortiGate, maximum and  
                  current connections  
    debug-filter → Debug message filter for SSL-VPN  
    hw-acceleration-status → Display the status of SSL hardware acceleration  
    tunnel-test → Enable/disable SSL VPN old tunnel mode IP allocation method  
    web-mode-test → Enable/disable random session ID in proxy URL for testing
```

```
# diagnose debug application sslvpn -1 ] Display debug messages for SSL-VPN; -1 debug level  
# diagnose debug enable ] produces detailed results
```



© Fortinet Inc. All Rights Reserved.

52

There are several useful troubleshooting commands available under `diagnose vpn ssl`. They include:

- `list`: Lists logged-on users
- `info`: Shows general SSL-VPN information
- `statistics`: Shows statistics about memory usage on FortiGate
- `hw-acceleration-status`: Displays the status of SSL hardware acceleration
- `tunnel-test`: Enable or disable SSL VPN old tunnel mode IP allocation method
- `web-mode-test`: Enable or disable random session ID in proxy URL for testing

The command `diagnose debug application sslvpn` shows the entire list of debug messages for SSL-VPN connections.

Remember, to use the commands listed above, you must first run the `diagnose debug enable` command.

DO NOT REPRINT**© FORTINET**

Hardware Acceleration for SSL-VPN

- FortiGate devices with content processors (CP8 or CP9), which offload specific CPU-intensive operations, support high-performance SSL-VPN bulk data engines
 - SSL/TLS protocol processor
- Administrators can disable CP offloading through firewall policies
 - For example: test purposes

```
config firewall policy
    edit 1
        set auto-asic-offload [enable | disable]
    end
```

- To view the status of SSL-VPN acceleration, use the following command:

```
get vpn status ssl hw-acceleration-status
```

Acceleration hardware detected:
kxp=on cipher=on

No acceleration hardware detected

FORTINET

© Fortinet Inc. All Rights Reserved.

53

FortiGate devices that have CP8 or CP9 content processors, which accelerate many common resource-intensive, security-related processes, can offload SSL-VPN traffic to a high-performance VPN bulk data engine.

This specialized IPsec and SSL/TLS protocol processor processes most of the latest well-known algorithms for encryption.

By default, the offloading process is set up. If, for testing purposes you want to disable it, you can do it using the CLI only at the firewall policy configuration level.

You can also view the status of SSL-VPN acceleration using the CLI.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What does the SSL-VPN monitor feature allow you to do?
 - A. Monitor SSL-VPN user actions, such as authentication
 - B. Force SSL-VPN user disconnections

2. Which statements about SSL-VPN timers are correct?
 - A. SSL-VPN timers can avoid logouts when SSL-VPN users experience long network latency
 - B. The login timeout is a non-customizable hard value



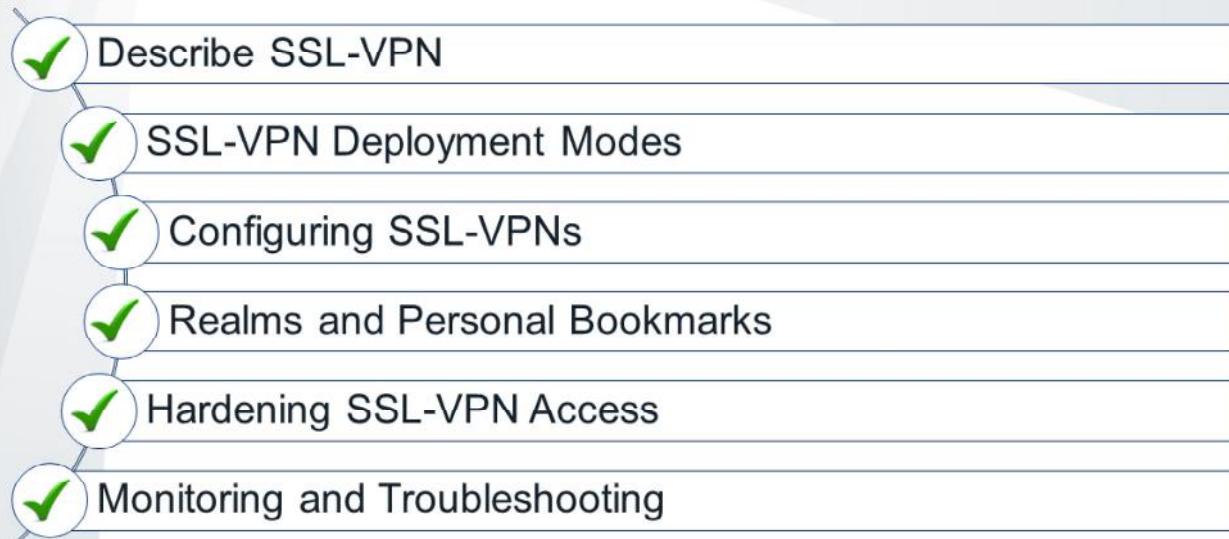
© Fortinet Inc. All Rights Reserved.

54

DO NOT REPRINT

© FORTINET

Lesson Progress



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Define a virtual private network (VPN)
- ✓ Describe the differences between SSL-VPN and IPsec VPN
- ✓ Describe the differences between SSL-VPN modes
- ✓ Define authentication for SSL-VPN users
- ✓ Configure SSL-VPN portals
- ✓ Configure SSL-VPN settings
- ✓ Define firewall policies for SSL-VPN
- ✓ Configure realms for SSL-VPN portal
- ✓ Configure personal bookmarks for SSL-VPN portal
- ✓ Configure client integrity checking
- ✓ Apply two-factor authentication using security certificates
- ✓ Restrict clients by IP and MAC address
- ✓ Monitor SSL-VPN connected users
- ✓ Review SSL-VPN logs
- ✓ Configure SSL-VPN timers
- ✓ Troubleshoot common SSL-VPN issues

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

By mastering the objectives covered in this lesson, you learned how to configure and use SSL-VPNs to give remote users access to your private network.

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., 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. 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. 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.