

DO NOT REPRINT
© FORTINET



FortiGate Security Study Guide

for FortiOS 7.2

FORTINET
Training Institute

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

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

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

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

Fortinet | Pearson VUE

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

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

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



TABLE OF CONTENTS

Change Log	4
01 Introduction and Initial Configuration	5
02 Firewall Policies	47
03 Network Address Translation	94
04 Firewall Authentication	134
05 Logging and Monitoring	172
06 Certificate Operations	213
07 Web Filtering	251
08 Application Control	293
09 Antivirus	338
10 Intrusion Prevention and Denial of Service	381
11 Security Fabric	422

Change Log

This table includes updates to the *FortiGate Security 7.2 Study Guide* dated 6/13/2022 to the updated document version dated 8/23/2022.

Change	Location
Various formatting fixes	Entire Guide
Fixed notes ("The DNS connection matches central SNAT "policy ID 2")	Lesson 3 slide 28
Fixed check mark on knowledge check, question 2	Lesson 7 slide 8

DO NOT REPRINT
© FORTINET



FortiGate Security

Introduction and Initial Configuration



Last Modified: 13 June 2022

In this lesson, you will learn about FortiGate administration basics and the components within FortiGate that you can enable 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



Fundamental Maintenance

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

DO NOT REPRINT**© FORTINET**

High-Level Features

Objectives

- Identify the 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, FortiGate features 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 perform.

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 multifaceted and multidevice 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.

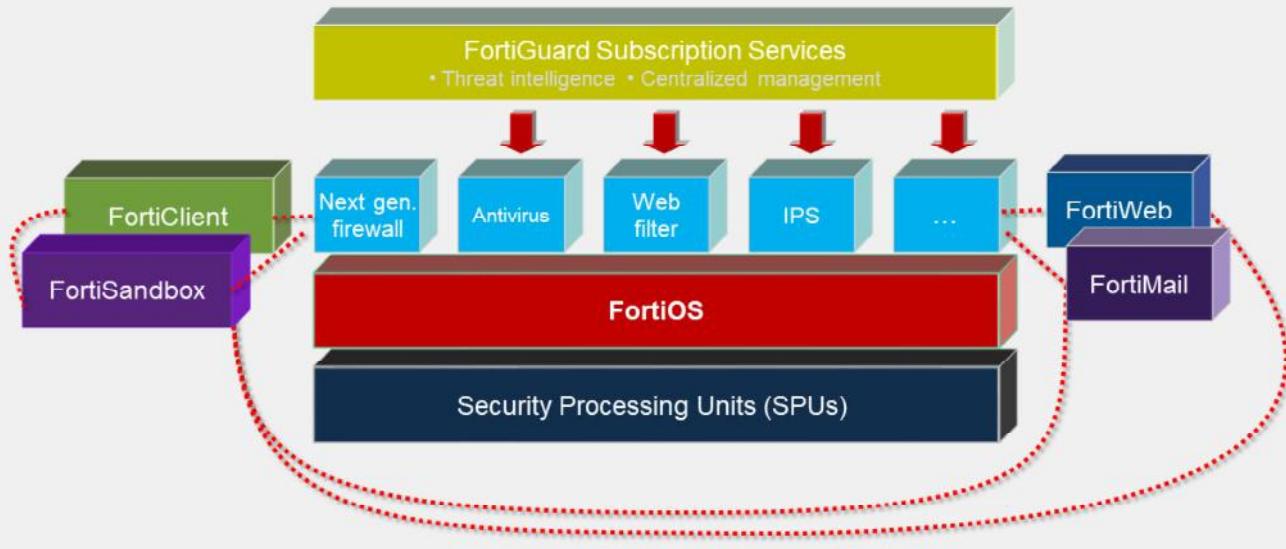
What's more, today's networks are highly complex environments whose borders are constantly changing. Networks run vertically from the LAN to the internet, and horizontally from the physical network to a private virtual network and to the cloud. A mobile and diverse workforce (employees, partners, and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

In response to this highly complex environment, firewalls have become robust multifunctional 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, antivirus, and IPS services.

DO NOT REPRINT
© FORTINET

Platform Design



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

5

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:

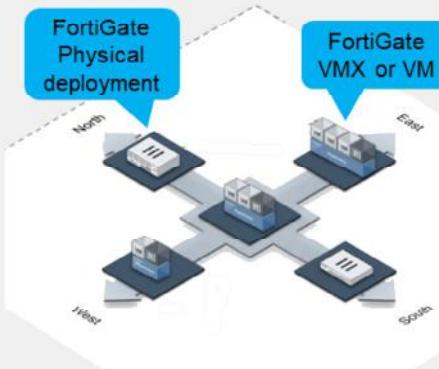
- **Devices add duplication.** Sometimes, dedication *doesn't* mean efficiency. If it's overloaded, can one device borrow free RAM from nine others? Do you want to configure policies, logging, and routing on 10 separate devices? Does 10 times the duplication bring you 10 times the benefit, or is it a 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, you can enable or disable UTM and next-generation firewall modules. 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
- VMs or physical appliances
 - Configuration is essentially the same



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

FortiGate VMs have the same features as physical FortiGate devices, *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 the Fortinet 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 anyone would 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.

Either VMs or physical appliances (low or high-end models), the configuration of the security instances is essentially identical, using same FortiOS version and FortiGuard real-time threat intelligence.

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. Which 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



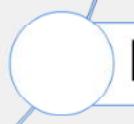
High-Level Features



Setup Decisions



Basic Administration



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 default settings
- Understand the FortiGate relationship with FortiGuard and distinguish between live queries and package updates

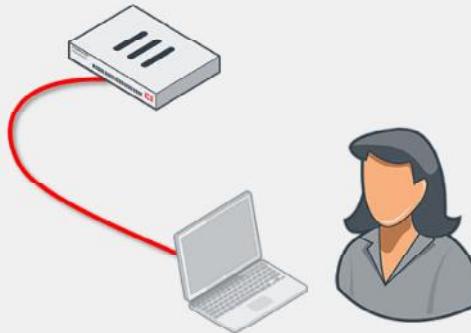
After completing this section, you should be able to achieve the objectives shown on this slide.

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

DO NOT REPRINT**© FORTINET**

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, 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



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 network cable to port1 or the internal switch ports (on the entry-level model). For high-end and mid-range models, connect to the MGMT interface. In most entry-level 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 visit <https://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 admin account. Once you logged in with default login details, you'll see a message to change the default blank password for the admin user password. Before you connect FortiGate to your network, you should set a complex password. You'll also be asked to apply additional configuration such as hostname, dashboard setup, register with FortiCare, and so on.

All FortiGate models have a console port and/or USB management port. The port provides CLI access without a network. You can access the CLI using 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 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
 - securewf.fortiguard.net for HTTPS over port 443, 53 or, 8888
- FortiOS uses FortiGuard server for DNS request
 - By default, uses DNS over TLS (DoT) to secure dns traffic



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 anywhere FortiGate selects a server based on server load, from any part of the world. However, you have the option to change the FortiGuard server location to USA. In this case, FortiGate selects 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 device 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 device must try repeatedly to download updates, it can't detect new threats during that time.

When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic. New FortiGuard DNS servers have been added as primary and secondary servers.

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 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 (webfiltering, antispam)	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

Now, 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 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 device is located.

The domain name of each FortiGuard service is the common name in the certificate of that service. 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 complete the TLS handshake only with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status results in a failed SSL connection.

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

FortiGate aborts the connection to the FortiGuard server if:

- The CN in the server 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 forces the rating process to use protocol HTTPS, and port 443. The table on this slide shows a list of some of the FortiGuard servers and their domain names and IP addresses.

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

DO NOT REPRINT**© FORTINET**

Lesson Progress

**High-Level Features****Setup Decisions****Basic Administration****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

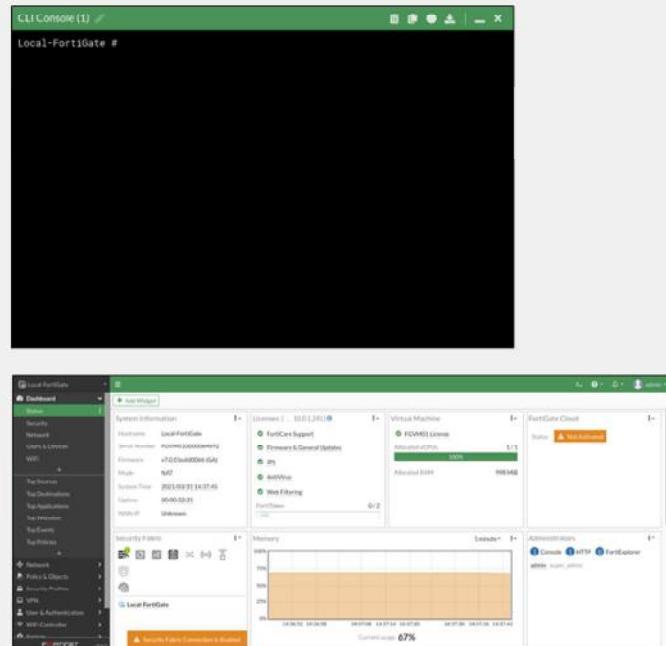
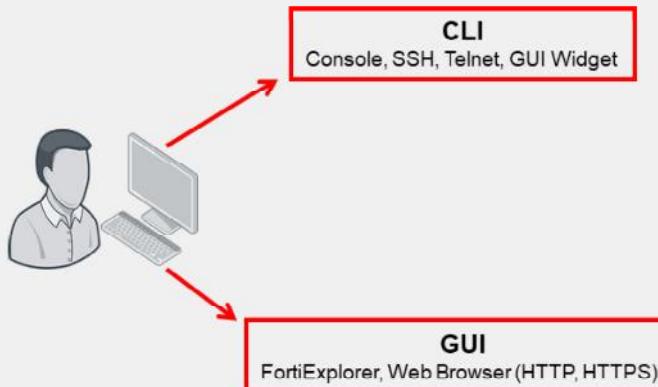
- Manage administrator profiles
- Manage administrative users
- Define the configuration method for administrative users
- Define and describe VDOMs
- Control administrative access to the FortiGate GUI and CLI
- Manage specific aspects of the network interfaces
- Describe VLANs and VLAN tagging
- Enable the DHCP and DNS services on FortiGate

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



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

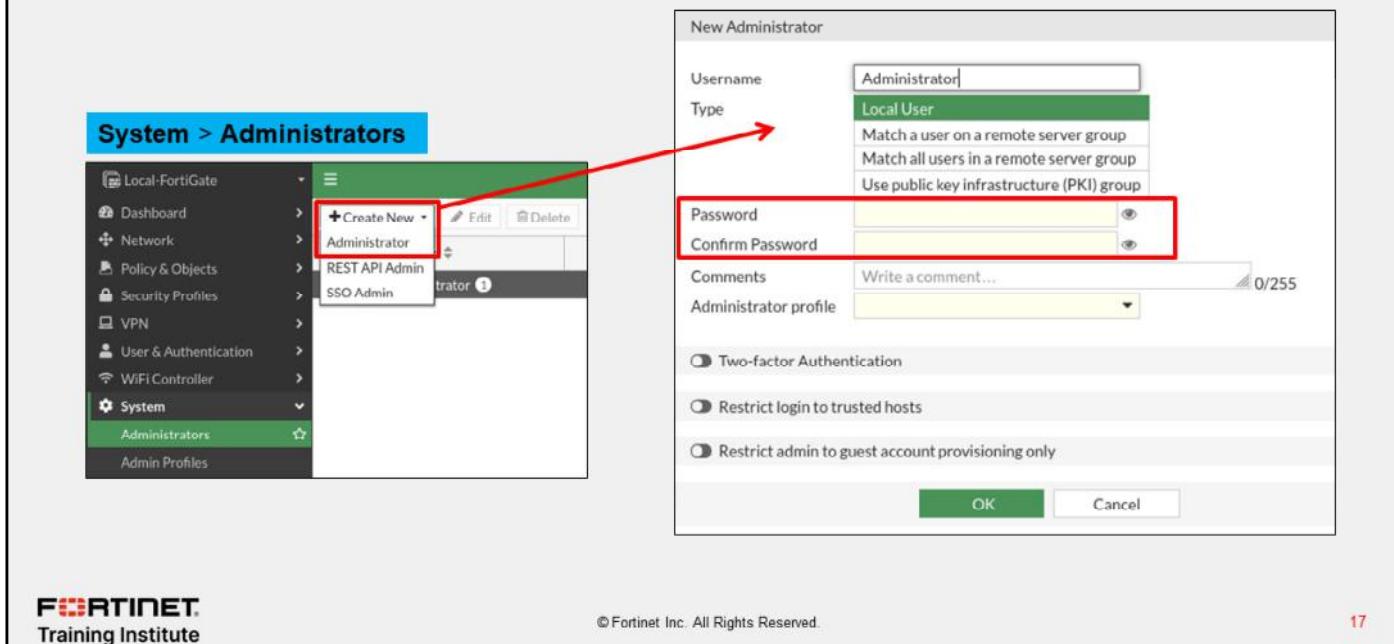
Most features are available on both the GUI and CLI, but there are a few exceptions. You can't view reports on the CLI. Also, advanced settings and diagnostic commands for super users are usually not available on the GUI.

As you become more familiar with FortiGate, and especially if you want to script its configuration, you might want to use the CLI in addition to the GUI. You can access the CLI through either the JavaScript widget on 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. You can't use them for basic setup.

DO NOT REPRINT
© FORTINET

Create an Administrative User



The screenshot shows the FortiGate Management Interface. On the left, the navigation menu is open, showing 'System > Administrators'. The main pane displays a list of administrators: 'Administrator' (selected), 'REST API Admin', and 'SSO Admin'. A red box highlights the 'Create New' dropdown menu. An arrow points from this dropdown to the 'Type' dropdown in a modal dialog box on the right. The dialog box is titled 'New Administrator' and contains fields for 'Username' (set to 'Administrator'), 'Type' (set to 'Local User'), 'Password', 'Confirm Password', 'Comments', and 'Administrator profile'. It also includes checkboxes for 'Two-factor Authentication', 'Restrict login to trusted hosts', and 'Restrict admin to guest account provisioning only'. The 'OK' and 'Cancel' buttons are at the bottom.

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

17

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.

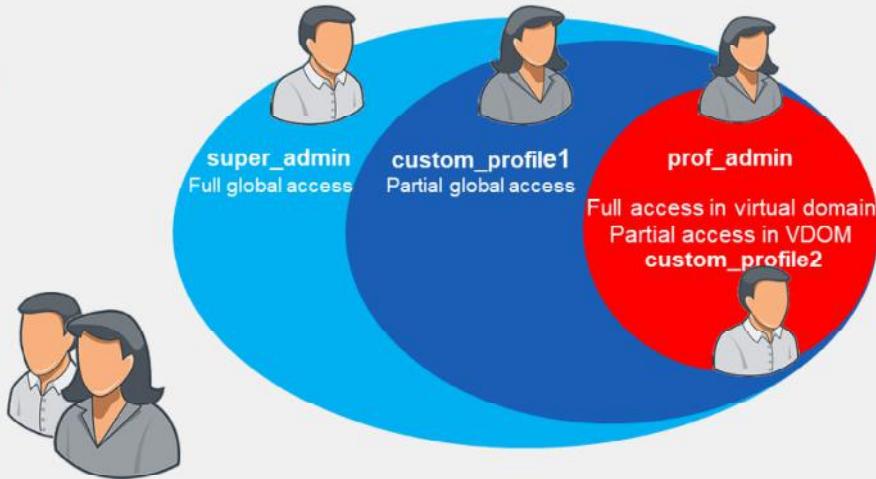
In order to restrict access to specific features, you can assign permissions.

DO NOT REPRINT
© FORTINET

Administrator Profiles

- Permissions

- Hierarchy



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**. You can't change it. 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 applies only to its virtual domain—not the global settings of FortiGate. Also, you can change its permissions.

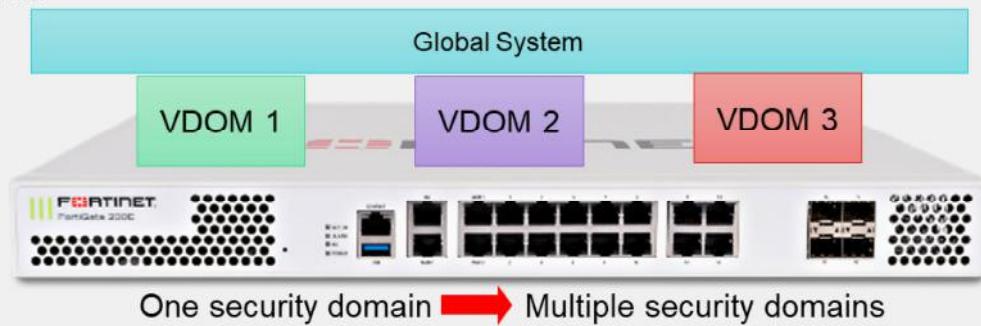
You aren't required to use a default profile. You could, for example, create a profile named **auditor_access** with read-only permissions. Restricting a person's permissions to those necessary for his or her job is a best practice, because even if that account is compromised, the compromise to your FortiGate device (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 `admindtimeout` value, under `config system accprofile`, to be overridden per access profile. You can configure administrator profiles to increase inactivity timeout and facilitate use of the GUI for central monitoring. Note that you can do this on a per-profile basis, to prevent the option from being unintentionally set globally. So, 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 device. 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.

DO NOT REPRINT
© FORTINET

VDOMs



- VDOMs split FortiGate into multiple virtual devices
 - They employ independent security policies, routing tables, and so on
- Packets are confined to same VDOM
- By default, FortiGate supports up to 10 VDOMs
 - High-end models allow for the purchase of additional VDOMs

What if, more than segmenting your network, you want to subdivide policies and administrators into multiple security domains?

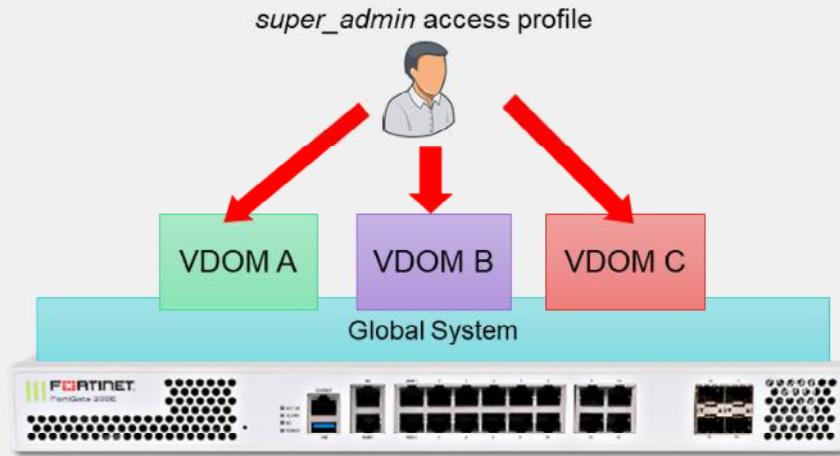
In that case, you can enable FortiGate VDOMs, which split your FortiGate into multiple logical devices. Each VDOM has independent security policies and routing tables. Also, and by default, traffic from one VDOM cannot go to a different VDOM. This means that two interfaces in different VDOMs can share the same IP address, without any overlapping subnet problems.

When you use VDOMs, a single FortiGate device becomes a virtual data center of network security, UTM inspection, and secure communication devices.

DO NOT REPRINT**© FORTINET**

VDOM Administration

- Only the account named **admin** or accounts with the **super_admin** profile can configure and back up all VDOMs

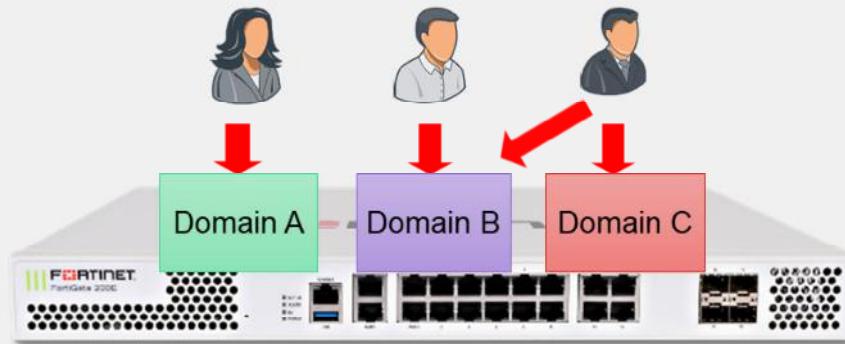


If you want to grant access to all VDOMs and global settings, select **super_admin** as the access profile when configuring the administrator account. Similar to the account named **admin**, this account can configure all VDOMs.

DO NOT REPRINT
© FORTINET

Per-VDOM Administration

- Other administrators can access only their *assigned* VDOMs
 - Cannot access the global settings



In most cases, you start by creating one administrator account per VDOM. That administrator is chiefly responsible for that domain, including the configuration backups of that VDOM. In larger organizations, you may need to make multiple VDOM administrators. You can assign multiple administrators to each VDOM. You can subdivide permissions using access profiles, in order to follow best practices for segregation of duties.

The converse is also possible. If required, you can assign an administrator to multiple VDOMs.

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, you can disable maintainer

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



© Fortinet Inc. All Rights Reserved.

22

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 devices and even some non-FortiGate devices, like FortiMail. There is no maintainer procedure in the VM. The administrator must revert to a snapshot or reprovision the VM and restore the 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. You must physically shut off FortiGate, then turn it back on, not reboot it through the CLI.

The `maintainer` login is available for login only 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, because you cannot recover access to your FortiGate device. In order to regain access in this scenario, you will need to reload the device. This will reset to the device to its factory default settings.

DO NOT REPRINT

© FORTINET

Administrative Access—Trusted Sources

The screenshot illustrates the configuration and enforcement of trusted hosts for administrative access. On the left, a configuration dialog shows the 'Restrict login to trusted hosts' option selected, with 'Trusted Host 1' set to '10.0.1.10/32'. A red arrow points from this dialog to a table on the right, which lists the 'System Administrator' account with 'admin' as the user and '10.0.1.10/32' as the trusted host. A blue callout box states: 'If **admin** attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message'. On the right, a login screen shows an 'Authentication failure' message, indicating that an attempt to log in from a different IP address was unsuccessful.

System > Administrators

Two-factor Authentication

Restrict login to trusted hosts

Trusted Host 1 10.0.1.10/32

OK Cancel

Create New Edit Delete Search

Name Trusted Hosts Profile Type Two-factor Authentication

System Administrator 1

admin 10.0.1.10/32 super_admin Local Disabled

Authentication failure

Username

Password

Login

If **admin** attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

23

Another way to secure 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 **admin** from which **admin** logs in. If **admin** 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 hosts 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 the 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 FortiGate, where the VDOM 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 five minutes

System > Settings

Administration Settings

- HTTP port: 80
- Redirect to HTTPS:
- HTTPS port: 443
- HTTPS server certificate: self-sign
- SSH port: 22
- Telnet port: 23
- Idle timeout: 5 Minutes (1 - 480)
- ACME interface: +

Password Policy

- Password scope: **Admin** (selected)
- Off
- IPsec
- Both
- Minimum length: 8
- Minimum number of new characters: 0
- Character requirements:
- Allow password reuse:
- Password expiration:

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

You can choose whether to allow concurrent sessions. You can use concurrent sessions to avoid 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 five 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 you can do this 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 Connection:
 - CAPWAP
 - FortiTelemetry
 - FMG-Access
 - FTM
 - RADIUS Accounting
- LLDP Support
 - Detecting an upstream Security Fabric FortiGate through LLDP

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, and SSH. By default, the HTTP and 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. You should disable protocols that do not encrypt data flow, such as HTTP and TELNET. 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 have FortiGate as a destination IP. Use the FortiTelemetry protocol specifically for managing FortiClient and the Security Fabric. Use the CAPWAP protocol for FortiAP, FortiSwitch, and FortiExtender when they are managed by FortiGate. Use the FMG-Access protocol specifically for communicating with FortiManager when that server is managing multiple FortiGate devices. Use the RADIUS accounting protocol 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 the Link Layer Discovery Protocol (LLDP) to detect if there's an upstream FortiGate in your network. If FortiGate discovers an upstream FortiGate, you're prompted to configure the upstream FortiGate device to join the Security Fabric.

DO NOT REPRINT

© FORTINET

Interface IPs

- In NAT mode, you can't use interfaces until they have an IP address:
 - Manually assigned
 - Automatic
 - DHCP
 - PPPoE

Network > Interfaces

Edit Interface	
Name	port5
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined
Address	
Addressing mode	Manual
IP/Netmask	0.0.0.0/0.0.0.0
Secondary IP address	

Edit Interface	
Name	port5
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined
Address	
Addressing mode	Manual
Retrieval default gateway from server	
Distance	5
Override Internal DNS	

When FortiGate is operating in NAT mode, every interface that handles traffic must have an IP address. When in NAT mode, FortiGate can use the IP address to source the traffic, if it needs to start or reply to a session, and 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 (available on the CLI)

DO NOT REPRINT
© FORTINET

Interface Role Compared to Alias

- Role defines interface settings typically grouped together:
 - Prevents 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

Network > Interfaces

Edit Interface

Name	port3
Alias	Internal_Network
Type	Physical Interface
VRF ID	0
Role	Undefined
Address	10.0.1.254/255.255.255.0
IP/Netmask	10.0.1.254/255.255.255.0
Secondary IP address	Off

Policy & Objects > Firewall Policy

Interface Pair View

Name	From	To	Source	Destination
Full_Access	Internal_Network (port3)	port1	LOCAL_SUBNET	all
Implicit Deny	any	any	all	all

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 role. The roles shown on 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

VLANs



- *Logically* subdivide your physical Layer 2 network into smaller segments
 - Each segment forms a separate broadcast domain
 - VLAN tags added to frames to identify their network segments

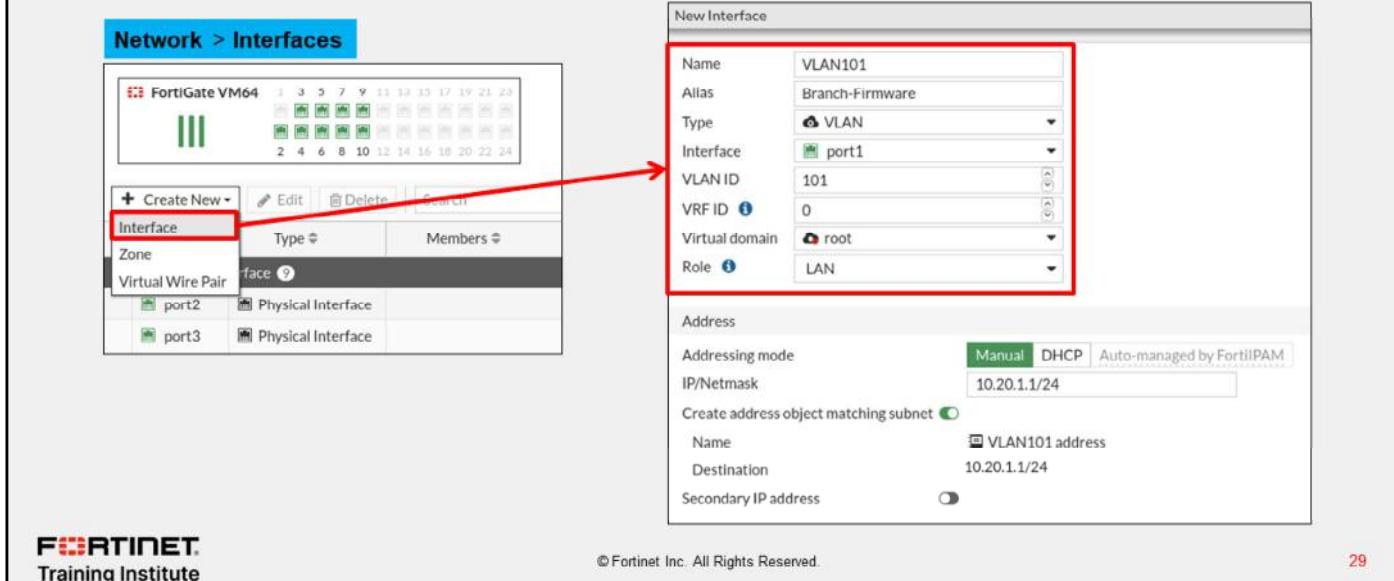
VLANs split your physical LAN into multiple, logical LANs. In NAT operation mode, each VLAN forms a separate broadcast domain. Multiple VLANs can coexist in the same physical interface, provided they have different VLAN IDs. In this way, a physical interface is split into two or more logical interfaces. A tag is added to each Ethernet frame to identify the VLAN to which it belongs.

DO NOT REPRINT

© FORTINET

Creating VLANs

- Frames sent or received by the physical interface segment are never tagged; they belong to the *native VLAN*



The screenshot shows the FortiGate VM64 interface configuration. On the left, the 'Network > Interfaces' page lists physical interfaces (port1, port2, port3) and a virtual wire pair. A red box highlights the 'Create New' button, and a red arrow points to the 'Name' field in the 'New Interface' dialog on the right. The 'New Interface' dialog is titled 'New Interface' and contains the following fields:

Name	VLAN101
Alias	Branch-Firmware
Type	VLAN
Interface	port1
VLAN ID	101
VRF ID	0
Virtual domain	root
Role	LAN

Below these fields, there is an 'Address' section with an 'Addressing mode' dropdown set to 'Manual', an IP/Netmask field containing '10.20.1.1/24', and a 'Create address object matching subnet' checkbox. The 'Name' field in this section is also highlighted with a red box and labeled 'VLAN101 address'.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

29

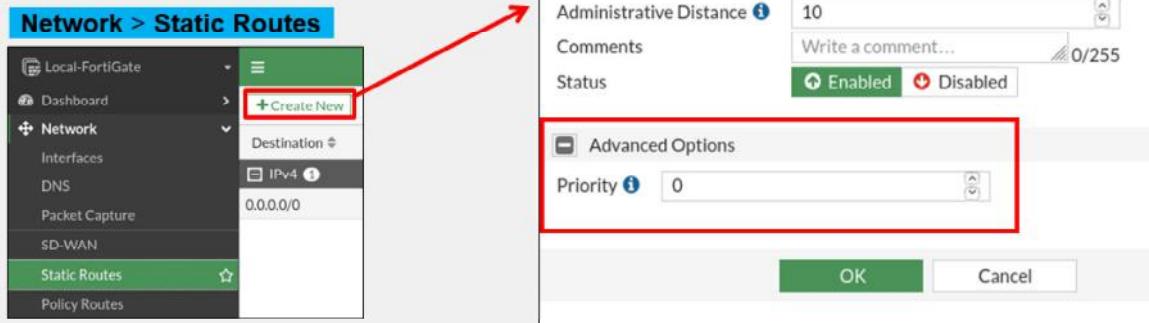
To create a VLAN using the GUI, click **Create New**, select **Interface**, and then, in the **Type** drop-down list, select **VLAN**. You must specify the VLAN ID and the physical interface to which the VLAN will be bound. Frames that belong to interfaces of that type are always tagged. On the other hand, frames sent or received by the physical interface segment are never tagged. They belong to what is called the *native VLAN* (VLAN ID 0).

Note that in a multi-VDOM environment, the physical interface and its VLAN sub-interface can be in separate VDOMs.

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



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 correctly 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

FortiGate as a DHCP Server

The screenshot displays the FortiGate interface for managing network interfaces and DHCP servers. On the left, the 'Edit Interface' screen for 'port3' is shown, with the 'Role' set to 'LAN'. The 'Address' section shows 'Address mode' as 'Manual' and 'IP/Netmask' as '10.0.129.4/255.255.255.0'. The 'DHCP Server' section is also visible. In the center, the 'DHCP Server' configuration for 'port3' is shown, with 'DHCP status' set to 'Enabled'. The 'Address range' is '10.0.1.10-10.0.1.253'. The 'IP Address Assignment Rules' section is highlighted with a red box, showing a table with one row: 'Type' (Implicit), 'Match Criteria' (Unknown MAC Addresses), and 'Action' (Assign IP). An arrow points from this table to the 'Create New' button. On the right, a 'Create New IP Address Assignment Rule' dialog box is open, showing 'Type' as 'MAC Address' and 'Description' as 'Write a comment...'. The 'Action type' is set to 'Assign IP | Block | Reserve IP', with 'Assign IP' selected. The 'IP' field is set to '0.0.0.0'. Buttons for 'OK' and 'Cancel' are at the bottom.

DO NOT REPRINT
© FORTINET

© Fortinet Inc. All Rights Reserved.

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 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 the screenshot on the middle of the slide shows that you can create IP address assignment rules in the **IP Address Assignment Rule** section. The **IP Address Assignment Rule** section allows you to assign, block or reserve the IP address to the host. It also allows you to select actions for unknown MAC addresses. The default action is **Assign IP**; however, you can change the default action type to **Assign IP** or **Block**.

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)

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 device or other devices that use DNS queries frequently. If your FortiGate device offers DHCP to your local network, you can use DHCP 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 the FortiGate DNS databases and does not forward unresolvable queries.
- Recursive: replies to queries for items in the FortiGate 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**

Knowledge Check

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

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

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

DO NOT REPRINT**© FORTINET**

Lesson Progress

**High-Level Features****Setup Decisions****Basic Administration****Fundamental Maintenance**

Good job! You now have the knowledge needed to carry out some basic administrative tasks. You also know how to enable DHCP and DNS services on FortiGate.

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 plaintext and encrypted configuration files
- Identify the current firmware version
- Upgrade firmware
- Downgrade firmware

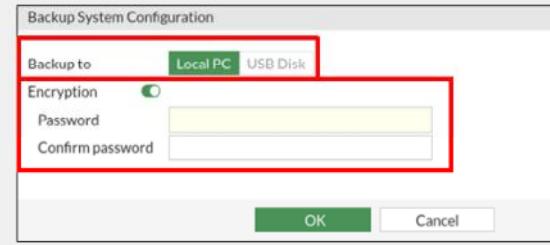
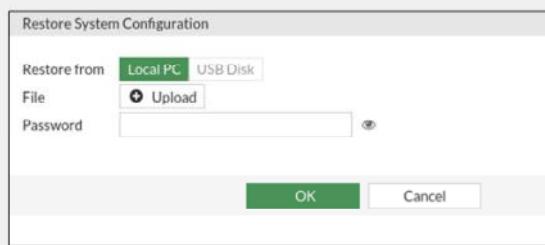
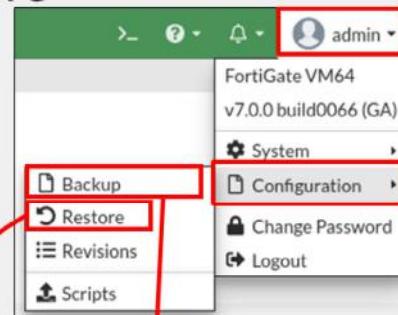
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the basic maintenance of FortiGate, you will be able to perform the vital activities of backing up and restoring configurations, upgrading and downgrading firmware, and ensuring 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



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.

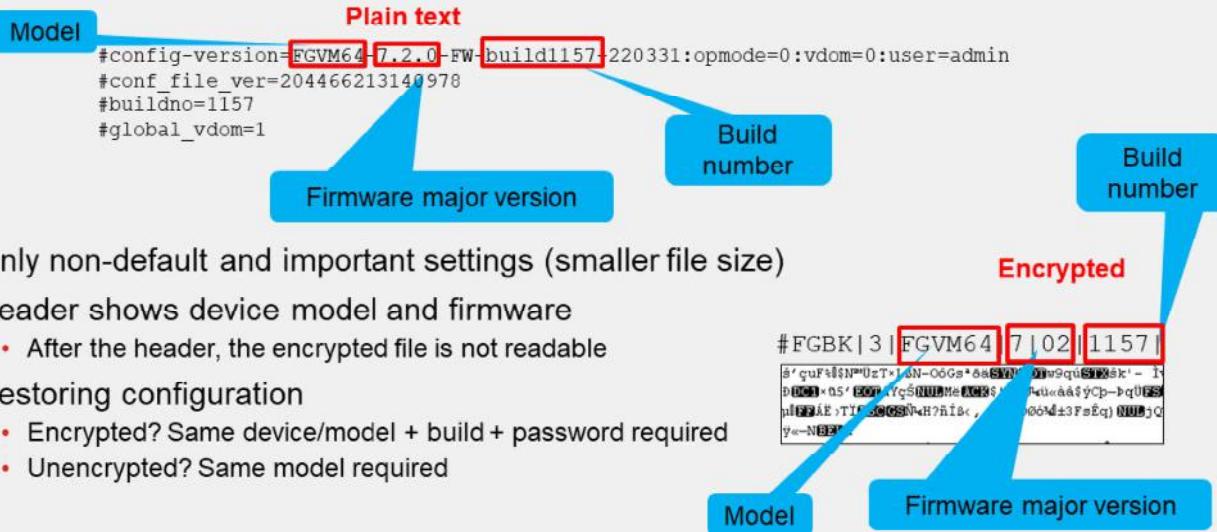
If you enable virtual domains (VDOMs), subdividing the resources and configuration of your FortiGate device, each VDOM administrator can back up and restore their own configurations. You don't have to back up the entire FortiGate configuration, however, it is still recommended.

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 FortiGate.

DO NOT REPRINT
© FORTINET

Configuration File Format



If you open the configuration file in a text editor, you'll see that both encrypted and unencrypted configuration files contain a cleartext 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 device 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 contains only non-default settings, plus few default, yet crucial, settings. This minimizes the size of the backup, which could otherwise be several megabytes in size.

DO NOT REPRINT
© FORTINET

Configuration File Format (Contd)

- Support YAML
- Configuration can be backedup and restored by CLI only

- # execute backup yaml-config {ftp | tftp} <filename> server [username] [password]
- # execute restore yaml-config {ftp | tftp} <filename> server [username] [password]

```
config system global
  set admintimeout 480
  set alias "FortiGate-100F"
end
config system settings
  set default-voip-alg-mode kernel-helper-based
  set gui-dynamic-routing enable
end
config system interface
  edit "port1"
    set vdom "root"
    set ip 204.126.10.3 255.255.254.0
    set allowaccess ping
    config secondaryip
      edit 1
        set ip 204.126.10.2 255.255.255.0
        set allowaccess ping
    end
```

Default Format

```
config_system_global:
  admintimeout:480
  alias:FortiGate-100F
config_system_settings:
  default-voip-alg-mode: kernel-helper-based
  gui-dynamic-routing: enable
config_system_interface:
  - port1:
    vdom: root
    ip: "204.126.10.3 255.255.254.0"
    allowaccess: ping
    secondaryip:
      - 0:
        ip: "204.126.10.2 255.255.255.0"
        allowaccess: ping
```

YAML Format

YAML format becomes more and more popular often use to create configuration files. FortiOS now supports YAML format, you can take a backup as well as restore YAML configuration file using CLI commands. You must provide server type: ftp or tftp, filename, server IP address, and user credential's to backup or restore configuration file in YAML format.

This slide shows the sample configuration to understand the difference between the default file format and YAML format.

DO NOT REPRINT**© FORTINET**

Upgrade Firmware

- You can view the current firmware version on the dashboard or in **System > Fabric Management** (or on the CLI: get system status)
- If there is an updated firmware version, you are notified
- Firmware can be updated by clicking **Upgrade** and then selecting the **All Upgrades** or **File Upload** option
- Make sure you read the *Release Notes* to verify the upgrade path and other details

The screenshot shows two windows. The top window is titled 'System > Fabric Management' and displays a dashboard with two green circles: one showing '1 Total' and 'Device Type FortiGate', and another showing '1 Total' and 'Upgrade Status Up to date'. Below these are buttons for 'Fabric Upgrade' (highlighted with a red box), 'Upgrade', 'Register', and 'Authorize'. A search bar and filter options for Device, Status, Registration Status, and Firmware Version are also present. The bottom window is titled 'FortiGate Upgrade' and shows the current version as 'v7.2.0 build1157 (Feature)'. It has a 'Select Firmware' section with buttons for 'Latest', 'All Upgrades', 'All Downgrades', and 'File Upload' (highlighted with a red box). A green message bar at the bottom states 'The firmware is up to date.'

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

39

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 can see the firmware version in the **System** widget. This information is also found at **System > Fabric Management**. 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 are notified on the dashboard and on the **Fabric Management** page. The **Fabric Management** page allows administrators to manage the firmware running on each FortiGate, FortiAP, and FortiSwitch in the Security Fabric, and to authorize and register these Fabric devices.

You can use **Upgrade** option to upgrade firmware of the selected device. The **Fabric Upgrade** option upgrades firmware for the root FortiGate as well as Fabric devices. You can also use this option to upgrade firmware for a non-Security Fabric FortiGate with managed FortiSwitch and FortiAP devices. The **Fabric Upgrade** option uses released firmware images from FortiGuard.

You can also use the **Register** option to register a selected device to FortiCare and an **Authorize** option to authorize a selected device for use in security fabric.

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**

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



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 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
- ✓ Define and describe VDOMs
- ✓ Execute backup and restore tasks and discuss the requirements for restoring an encrypted configuration file
- ✓ Initiate an upgrade 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
Training Institute



FortiGate Security

Firewall Policies

FortiOS 7.2

Last Modified: 13 June 2022

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

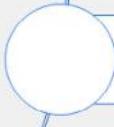
Lesson Overview



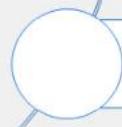
Firewall Policies



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

Policy & Objects > Firewall Policy											
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log		
1	Internet_Access_ISP1	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All		
2	Internet_Access_ISP2	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All		
0	Implicit	all	all	always	ALL	DENY	Disabled				

Implicit Deny



To begin, you will learn what firewall policies are.

Any traffic passing through a FortiGate must be associated with a firewall policy. A policy is a set of instructions that controls traffic flow through the FortiGate. These instructions determine where the traffic goes, how it's handled, and whether it's allowed to pass through the FortiGate. In summary, firewall policies are sets of rules that specify which traffic is allowed through the FortiGate and what FortiGate should do when traffic matches a policy.

Should the traffic be allowed? FortiGate bases this decision on simple criteria. FortiGate analyzes the source of the traffic, the destination IP address, and the service. 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. These inspections block the traffic if there is a security risk, for example, if the traffic contains a virus. Otherwise, the traffic is allowed.

Will network address translation (NAT) be applied? Is 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**

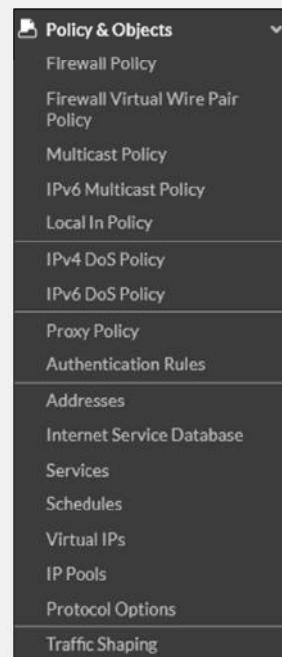
Components and Policy Types

Objects used by policies

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

Policy types

- Firewall Policy (IPv4, IPv6)
- Firewall Virtual Wire Pair Policy (IPv4, IPv6)
- Proxy Policy
- Multicast Policy
- Local-in Policy
- DoS Policy (IPv4, IPv6)
- Traffic Shaping



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

Common policy types are:

- Firewall Policy: A firewall policy consists of set of rules that control traffic flow through FortiGate.
- Firewall Virtual Wire Pair Policy: A virtual wire pair policy is used to control the traffic between the interfaces in a virtual wire pair.
- Multicast Policy: A multicast policy allows multicast packets to pass from one interface to another.
- Local In Policy: A local-in policy controls the traffic to a FortiGate interface and can be used to restrict administrative access.
- DoS Policy: A denial-of-service (DoS) policy checks for the anomalous patterns in the network traffic that arrives at a FortiGate interface.

By default, only **Firewall Policy** is visible under **Policy and Object**. Other policies are available based on the interface configurations and advanced features enabled through **Feature Visibility**.

In this lesson, you will learn about IPv4 firewall policies, because they are the most commonly used policies.

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 style="width: 100%;" type="text"/>
Incoming Interface	<input type="text"/>
Outgoing Interface	<input type="text"/>
Source	<input type="text"/> +
Destination	<input type="text"/> +
Schedule	<input type="text"/> <input checked="" type="checkbox"/> always
Service	<input type="text"/> +
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY



© 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**: Specific times to apply policy

If 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 allows the session and applies other configured settings for packet processing, such as user authentication, source NAT, antivirus scanning, web filtering, and so on.

When FortiGate receives traffic, it evaluates the packet's source IP address, destination IP address, and the requested service (protocol and port number). It also checks the incoming interface and the outgoing interface it needs to use. Based on this information, FortiGate identifies the firewall policy and evaluates the traffic. If the traffic matches the policy, then FortiGate applies the action (Accept/Deny) defined in the policy.

For example, to block incoming FTP traffic to all but a few FTP servers, define the addresses of the FTP servers 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 (FTP servers are usually always available, day or night). Finally, set the **Action** setting to **ACCEPT**.

DO NOT REPRINT

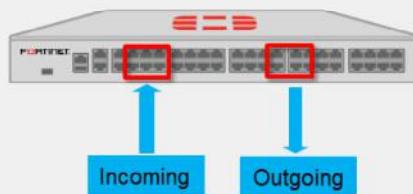
© FORTINET

Simplify—Interfaces and Zones

- The incoming and outgoing interfaces can function as individual interfaces or you can create a zone, which is a logical group of interfaces
- To match policies with traffic, select one or more interfaces

Network > Interfaces

	Type	Members	IP/Netmask
Interface	Physical Interface		10.200.1.1/255.255.255.0
Zone	Physical Interface		10.200.2.1/255.255.255.0
Virtual Wire Pair	Physical Interface		10.0.1.254/255.255.255.0
	Physical Interface		0.0.0.0.0.0.0
	Physical Interface		172.16.100.3/255.255.255.0
Tunnel Interface			
Zone	DMZ	Zone	port4 port5 port6 port7



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

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 will *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. You can create zones on the **Interfaces** page. However, you should note that you cannot reference an interface in a zone 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 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 on the GUI
- Can be made visible in the GUI

The screenshot illustrates the configuration of a firewall policy and the enabling of multiple interface policies.

Policy & Objects > Firewall Policy

New Policy

Name: Single_Interface

Incoming Interface: port4

Outgoing Interface: port5

A callout box points to the Outgoing Interface dropdown with the text "Multiple interface policies disabled".

System > Feature Visibility

Multiple Interface Policies

Allow the configuration of policies with multiple source/destination interfaces.

A red arrow points from the "Multiple Interface Policies" checkbox to the "Policy & Objects > Firewall Policy" section.

Policy & Objects > Firewall Policy

New Policy

Name: Multiple_Interface

Incoming Interface: port9, port10

Outgoing Interface: any

A callout box points to the Outgoing Interface dropdown with the text "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 the example shown on this slide, 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
- Dynamic
 - 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



FORTINET
Training Institute

© 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 the source in the firewall policy, which you will learn about later in this lesson.

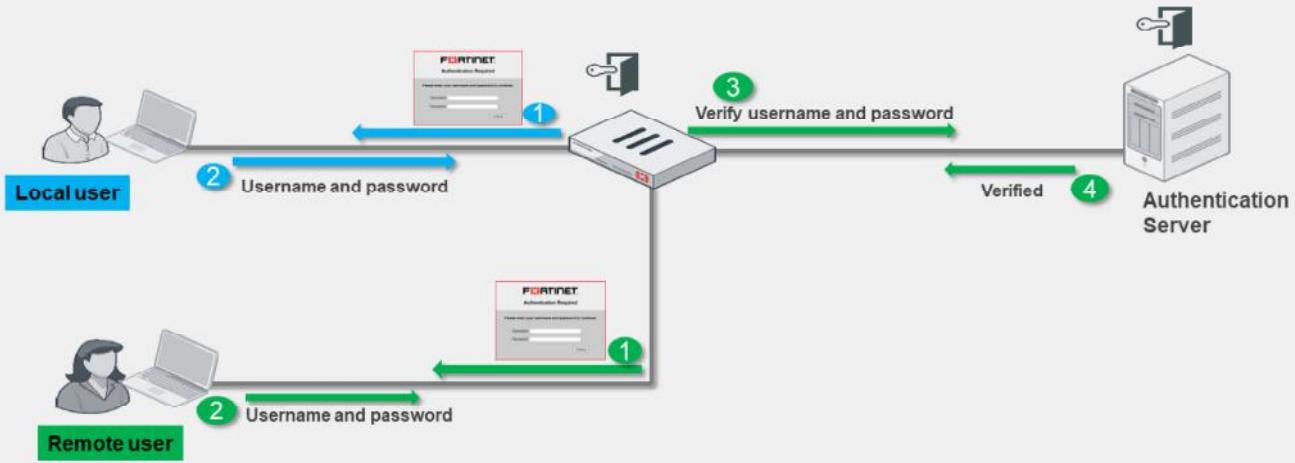
When selecting a fully qualified domain name (FQDN) as the source address, it must be resolved by DNS and cached in FortiGate. Make sure FortiGate is configured properly for DNS settings. If FortiGate is not able to resolve an FQDN address, it will present a warning message, and a firewall policy configured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



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

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

Policy & Objects > Firewall Policy

Name: Training
Incoming Interface: port3
Outgoing Interface: port1
Source: LOCAL SUBNET (selected), student

Select Entries: Address, User, Internet Service
Address: Local (3), guest, student
User: Local (3), guest, student

Annotations: 'User' and 'Address' are highlighted with blue arrows pointing to the selected items.

Policy & Objects > Firewall Policy

Name: Training
Incoming Interface: port3
Outgoing Interface: port1
Source: am Amazon-AWS (selected)

Select Entries: Address, User, Internet Service
Address: INTERNET SERVICE (55), Aerohive-Aerohive.Cloud, Akamai-CDN, Alibaba-Alibaba.Cloud, am Amazon-AWS, Apple-APNs
User: Local (3), guest, student

Annotations: 'Internet Service' is highlighted with a blue arrow pointing to the selected item.

© Fortinet Inc. All Rights Reserved.
11

In the example shown on this slide, 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
 - Dynamic
 - Fabric connector address
- Internet service database (ISDB) objects

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 device with DNS servers. FortiGate uses DNS to resolve those FQDN host names to IP addresses, that appear in the IP header.

You can also choose geographic addresses, which are groups or ranges of addresses that are assigned to a country. FortiGuard is used to update these objects.

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 the user is successfully authenticated.

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

Policy & Objects > Internet Service Database

Name	Direction	Number of Entries
Alibaba-SSH	Destination	4,347
Alibaba-Web	Destination	4,347
Amazon-AWS	Both	14,015
Amazon-AWS,WorkSpaces,Gateway	Destination	27
Amazon-DNS	Destination	41,821
Amazon-FTP	Destination	41,821

Policy & Objects > Firewall Policy

The screenshot shows the 'Policy & Objects > Firewall Policy' configuration. It includes fields for Name (Training), Incoming Interface (port3), Outgoing Interface (port1), Source (all), Destination (all, Facebook-Web), and Schedule (always). A 'Select Entries' sidebar lists various services: Facebook-SSH, Facebook-Web (highlighted in green), Facebook-Whatsapp, Fastly-CDN, Forcepoint-Forcepoint.Cloud, Fortinet-DNS, Fortinet-FortiCloud, and Fortinet-FortiGuard. A red box highlights the 'Facebook-Web' entry in the sidebar. A red arrow points from the 'Facebook-Web' entry to the 'Destination' field in the main configuration table. A red box also surrounds the 'Destination' field in the main table. A red warning message 'Addresses/groups cannot be mixed with Internet services' is displayed below the destination list.

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. You can select these 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

The screenshot shows the FortiGate Firewall interface with the following components:

- Header:** Policy & Objects > Internet Service Database
- Toolbar:** + Create New, Edit, Delete. The "Geographic Based Internet Service" object is selected, highlighted with a red box.
- Table:** Google-Other

IP	Port	Protocol	Status
62.24.215.76 - 62.24.215.79	1 - 65535	TCP	Enabled
62.24.215.76 - 62.24.215.79	1 - 65535	UDP	Enabled
62.24.215.81 - 62.24.215.83	1 - 65535	TCP	Enabled
- Modal:** New Internet Service

Name: Training-Location-ISDB	Type: Predefined Geographic Based
Primary Internet Service: Google-Other	Primary Internet Service Name: Google-Other
Country/Region: United Kingdom	Primary Internet Service ID: 65536
Region: England	Direction: Destination
City: Birmingham	Entries: View/Edit Entries
- Footer:** FORTINET Training Institute, © 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

Internet Service Database (ISDB)—Updates

- You can disable ISDB updates so they occur only during a change control window
 - Control ISDB updates by using CLI command:

```
# config system fortiguard
    set update-ffdb [enable | disable]
    next
end
```

- Once ISDB updates are disabled, other scheduled FortiGuard updates do not update ISDB
- By default, ISDB updates are enabled



© Fortinet Inc. All Rights Reserved.

15

You can disable ISDB updates, so they occur only during a change control window. Once ISDB updates are disabled, other scheduled FortiGuard updates for IPS, AV, and so on, do not update ISDB. By default, ISDB updates are enabled.

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 Recurring One Time

Name: Maintenance

Color: Change

Days: Monday Tuesday Wednesday
 Thursday Friday Saturday
 Sunday

All Day:

Start Time: 12:00:00,000 AM

Stop Time: 12:00:00,000 AM

Policy & Objects > Schedules

New Schedule

Type Recurring One Time

Name: Maintenance

Color: Change

Start Date: 04/21/2021 06:58:00,000 PM

End Date: 04/21/2021 07:58:00,000 PM

Pre-expiration event log:

Number of days before: 1

© Fortinet Inc. All Rights Reserved.

16

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:

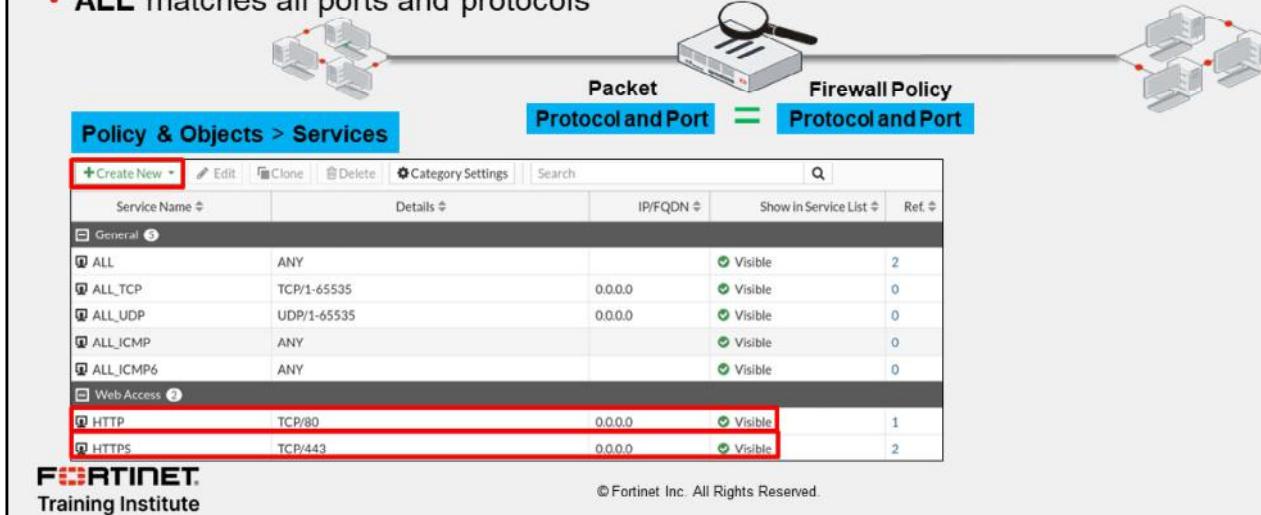
- Recurring:** If you enable **All Day**, traffic will be allowed for 24 hours for the days selected. When configuring recurring schedules, if you set the stop time earlier than the start time, the stop time will occur the next day. For example, if you select Sunday as the day, 10:00 as the start time, 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



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 last for only a short time and, therefore, are 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

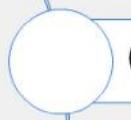
DO NOT REPRINT

© FORTINET

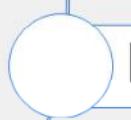
Lesson Progress



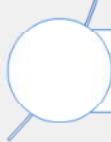
Firewall Policies



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 uid 2204966e-47f7-51..
```

Universally unique identified (UUID)

The screenshot shows the FortiGate configuration interface. On the left, a 'Firewall Policy' configuration window is open with the following fields:

- Name:** Training (highlighted with a red box)
- Incoming Interface:** LAN (port3)
- Outgoing Interface:** ISP1 (port1)
- Source:** LOCAL_CLIENT (highlighted with a red box)
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (highlighted with a green checkmark)

A callout bubble points to the 'Source' field with the text: "Enabled by default MUST specify unique name". Another callout bubble points to the 'LOCAL_CLIENT' entry in the list with the text: "Highlights selected entry".

On the right, the 'System > Feature Visibility' page is shown, with the 'Allow Unnamed Policies' checkbox selected (highlighted with a red box). A callout bubble points to this checkbox with the text: "Relax the requirement for every policy to have a name when created in GUI".

Below these, a 'Select Entries' window is open, showing a list of entries under the 'Address' tab. The 'LOCAL_CLIENT' entry is highlighted with a yellow box and a red box, indicating it is selected. Other entries include 'all', 'FABRIC_DEVICE', 'FIREWALL_AUTH_PORTAL_ADDRESS', 'FORTINET', 'gmail.com', 'LINUX ETH1', and 'LOCAL_SUBNET'.

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, while it is optional on 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 identifier (UUID) attribute is added so that logs can record these UUIDs 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="checkbox"/> AV default <input type="button" value=""/>
Web Filter	<input checked="" type="checkbox"/> WEB default <input type="button" value=""/>
Video Filter	<input checked="" type="checkbox"/> VF New Profile <input type="button" value=""/>
DNS Filter	<input checked="" type="checkbox"/> DNS default <input type="button" value=""/>
Application Control	<input checked="" type="checkbox"/> APP default <input type="button" value=""/>
IPS	<input checked="" type="checkbox"/> IPS default <input type="button" value=""/>
File Filter	<input checked="" type="checkbox"/> FF default <input type="button" value=""/>
VoIP	<input checked="" type="checkbox"/> VOIP default <input type="button" value=""/>
Web Application Firewall	<input checked="" type="checkbox"/> WAF default <input type="button" value=""/>
SSL Inspection 	<input checked="" type="checkbox"/> SSL deep-inspection <input type="button" value=""/>

Default profile not available, you need to manually create a profile

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.

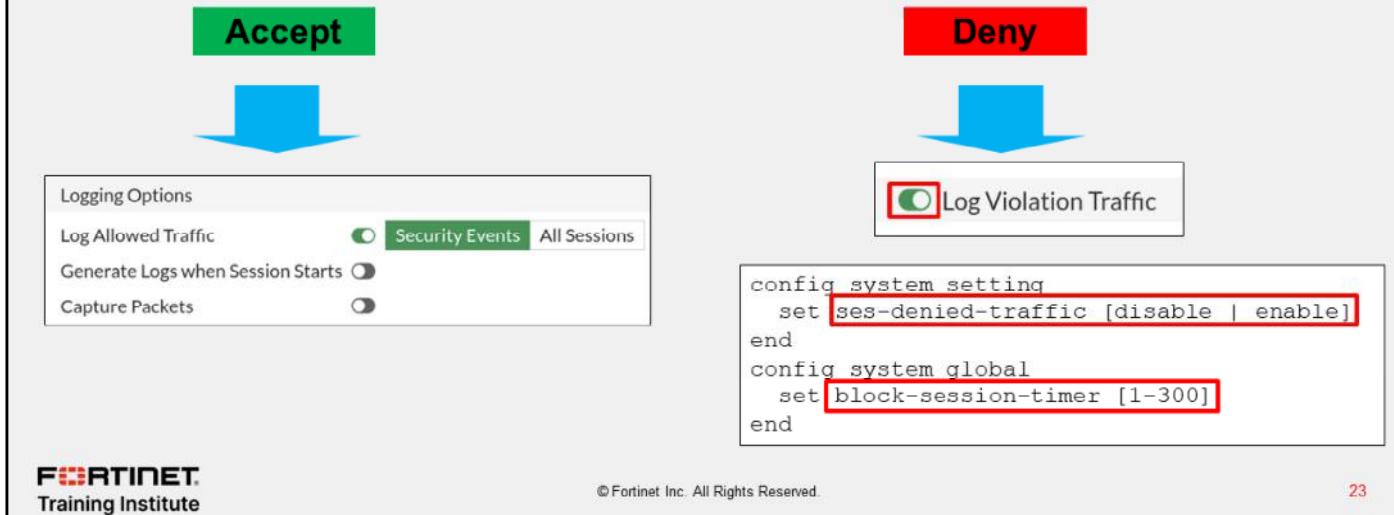
Note that by default, the **Video Filter**, **VOIP**, and **Web Application Firewall** security profile option is not visible in the policy page on the GUI. You need to enable them on the **Feature Visibility** page.

DO NOT REPRINT

© FORTINET

Logging

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



If you have enabled logging in the policy, FortiGate generates 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 number 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 on 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



You can configure two types of traffic shapers: 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

Policy & Objects > Firewall Policy

ID	Name	From	To	Source	Destination	Schedule	Service	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	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> certificate-inspection <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> no-inspection <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> no-inspection <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> certificate-inspection <input checked="" type="checkbox"/> UTM
0	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY		<input checked="" type="checkbox"/> Disabled

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

25

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 the 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 on the GUI. You must enable **IPv6** on the **Feature Visibility** page.

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 specific subnets
 B. To protect your network from threats, and control access to specific applications and URLs

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 the 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	Service	Action	NAT	Security Profiles	Log	Bytes
Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	✓ ACCEPT	Enabled	no-inspection	UTM	0 B
Full_Access	all	all	always	ALL	✓ ACCEPT	Enabled	no-inspection	All	912.05 kB
Backup_Access	all	all	always	ALL	✓ ACCEPT	Enabled	no-inspection	UTM	0 B

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	Service	Action	NAT	Security Profiles	Log	Bytes
Fortinet	port3	port1	LOCAL_CLIENT	FORTINET	always	Web Access	✓ ACCEPT	Enabled	no-inspection	UTM	0 B
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	0 B

Multiple interfaces

any interface

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

By default, the policy list appears in **Interface Pair View**. Each section contains policies in the order that they are evaluated for matching traffic and are arranged by ingress-egress interface pair. Alternatively, you can view your policies as a single, comprehensive list by selecting **By Sequence** at the top of the page. In this view the policies are also listed in the order in which they are evaluated for traffic matching, but they are not grouped.

In some cases, you cannot choose the view. For example, if you use multiple source or destination interfaces, or the **any** interface in a firewall policy, you cannot separate policies into sections by interface pairs—some would be triplets or more. In this case, policies always appear in a single list (**By Sequence**).

To help you remember the use of each interface, you add 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
 - ID
 - Last used
 - First used
 - Active sessions
 - Hit count
 - Total bytes
 - Current bandwidth
 - Usage graph

Policy & Objects > Firewall Policy

Edit Policy

Statistics (since last reset)

ID	1
Last used	0 second(s) ago
First used	46 minute(s) ago
Active sessions	3
Hit count	198
Total bytes	196.44 kB
Current bandwidth	0 B/s

Graph options

Usage graph

Last 7 Days | Bytes

Bytes
Packets
Hit Count

© Fortinet Inc. All Rights Reserved.

30

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

This feature is very useful if an administrator 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	Service	Action	NAT
	port3 → port1 2						
2	Block_FTP	all	all	always	FTP	DENY	
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled
	port3 → port2 1						
3	DMZ	DMZ	all	always	ALL	ACCEPT	Enabled

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

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 a policy ID, while creating a new policy. If a duplicate entry is found, the system produces an error, so you can assign a different available policy ID number.

Policy Advanced Options is not available on the GUI by default, you must 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

The screenshot illustrates the configuration of a firewall policy. At the top, a policy is defined for port3 to port2, with source address '2' and destination 'Web_FTP'. The source address is expanded to show 'Lan1' and 'Lan2' (highlighted with a red box). The destination 'Web_FTP' is expanded to show 'DNS', 'FTP', 'HTTP', and 'HTTPS' (also highlighted with a red box). Below the policy, two groups are defined: 'Local_LANS' (an address group containing 'Lan1' and 'Lan2') and 'Web-FTP' (a service group containing 'DNS', 'FTP', 'HTTP', and 'HTTPS'). In the final policy summary, the source address is now 'Local_LANS' and the destination is 'Web-FTP', demonstrating how groups simplify 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.

This slide shows that 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 websites 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

Number of times object used

Usage of Address: all

Edit View List View Properties Current Usage Possible Uses

Object Name Ref.

Address Group 1 (1 Reference) 1 Reference of group

Training (1 Reference) 1

Firewall Policy 2 (2 References) 0 Referenced by policy ID

Internet_Access_ISP1 (1 Reference) 0

DMZ (3 References) 0

Properties of Firewall Policy: 1

Attribute	Policy
policyid	1
status	enable
name	Internet_Access_ISP1
uuid	b11ac58c-791b-51e7-4
srcintf0.name	port3
dstintf0.name	port1
srcaddr0.name	all
dstaddr0.name	all

© Fortinet Inc. All Rights Reserved. 33

You've just seen 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. Take a look at 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.

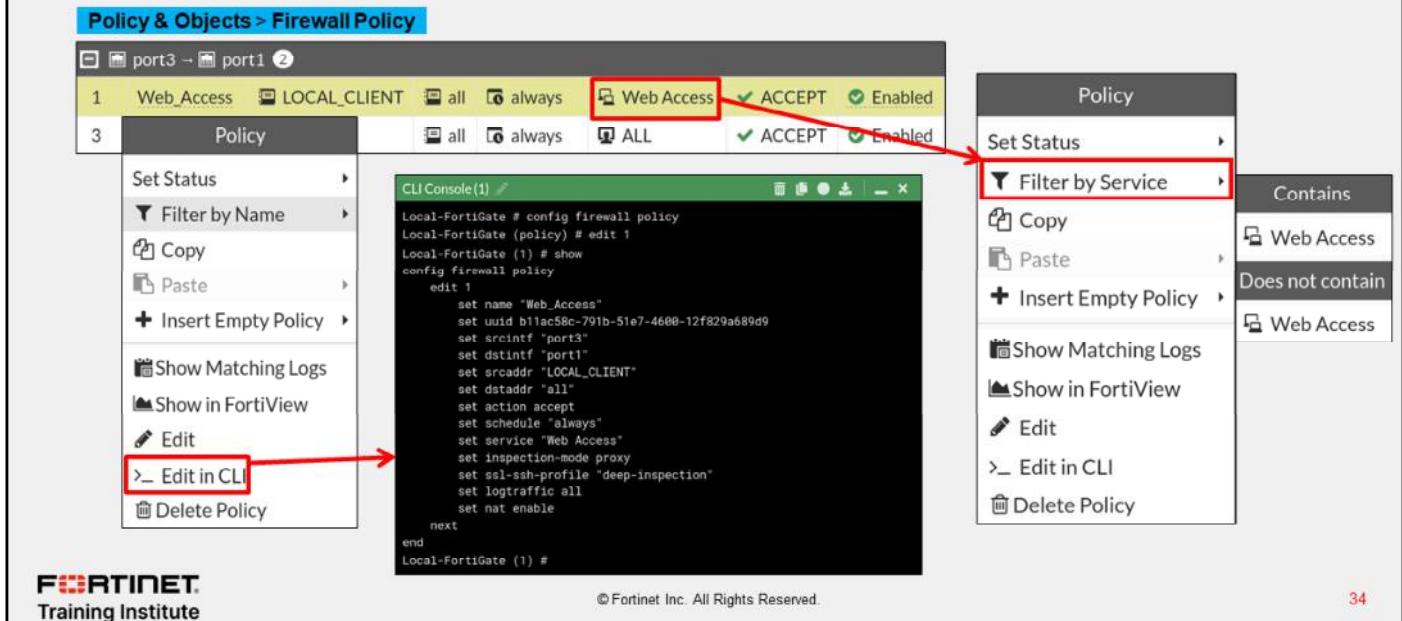
In the example shown on this slide, the **all** address object is being used by the **Training** address group and three firewall policies. If you select a firewall policy, you can use the **Edit**, **View List**, and **View Properties** tabs.

- Edit:** allows you to edit the selected object. In this example, it shows the edit page for the firewall policy ID 1.
- 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 on the CLI and can modify the selected firewall policy or object directly on the **CLI Console**.

DO NOT REPRINT

© FORTINET

Filter Column

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

Policy & Objects > Firewall Policy

The screenshot shows the FortiGate GUI for managing firewall policies. At the top, the title 'Policy & Objects > Firewall Policy' is visible. Below it is a table of policies:

ID	Name	Source	Destination	Schedule	Service	Action
1	Training1	port3 → pc	all	always	ALL_ICMP	ACCEPT
2	FTP	all	all	always	FTP	ACCEPT
3	Training2	port3 → pc	all	always	ALL_ICMP	ACCEPT
0	Implicit Deny	all	all	always	Web Access	DENY

A red box highlights the 'Name' column header. A 'Filter' dialog box is open over the table, with 'Contains' selected and 'FTP' entered in the search field. An 'Apply' button is at the bottom of the dialog. A red arrow points from the 'Name' column header to the 'Name' column in the resulting table below, which shows only the policy for 'FTP'.

ID	Name	Source	Destination	Schedule	Service	Action
2	FTP	all	all	always	FTP	ACCEPT

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

35

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

Policy & Objects > Addresses

New Address	
Category	Address
Name	Training(LAN)
Color	Change
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	any
Static route configuration	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

When configuring names for firewall objects, only specific 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 a 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.

40

Always plan a maintenance window and create a test case for a few IP addresses and 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 to only those resources. For example, use correct subnets when configuring address objects.

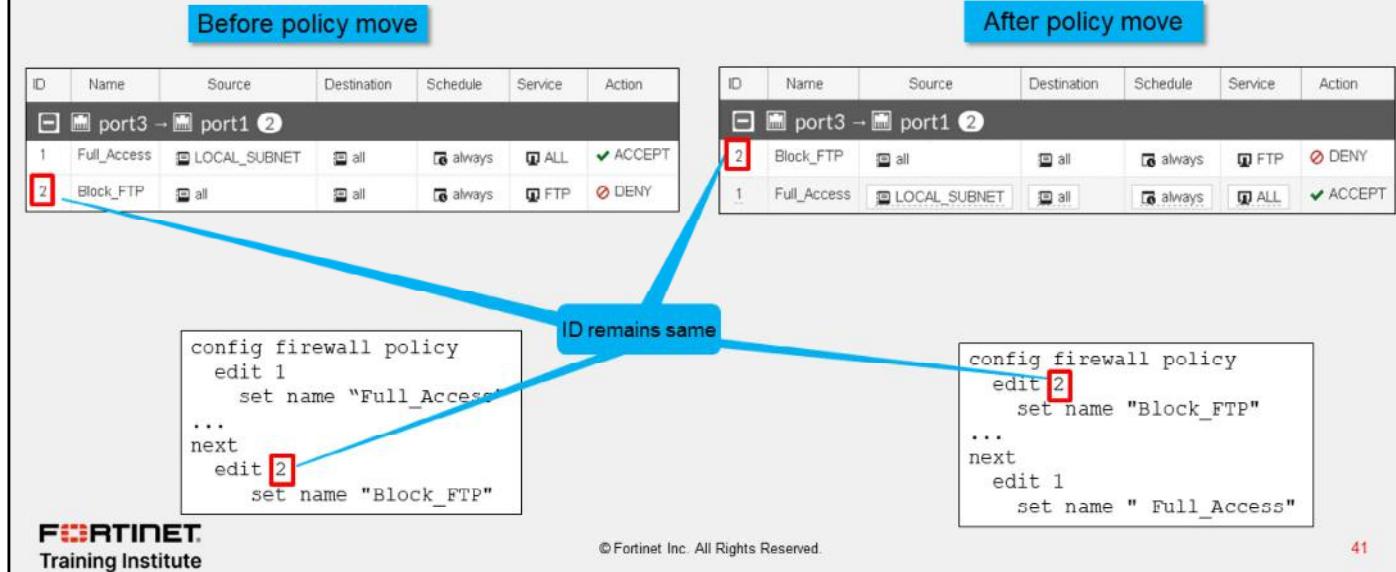
Another setting worth mentioning is security profiles. Security profiles help to provide appropriate security for your network. Proper logging configuration can also help you to analyze, diagnose, and resolve common network issues.

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 section of the applicable interface pair, 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 the **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
Training Institute

© Fortinet Inc. All Rights Reserved.

42

In order to optimize and consolidate firewall policies, always check all configured settings. In the example shown on this slide, 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

Policy & Objects > Firewall Policy

Policy Lookup

Incoming Interface	▼
IP Version	IPv4
Protocol	IP
Protocol Number	1-255
Source	IP Address
Destination	IP Address/FQDN

Search **Close**

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.

When FortiGate is in Transparent mode, it does not support the policy lookup function.

DO NOT REPRINT
© FORTINET

Policy Lookup Example (GUI)

- Highlights matching policy after search

Policy & Objects > Firewall Policy

Policy Lookup

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

Search

Policy Table (After Search):

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

Fortinet Training Institute © Fortinet Inc. All Rights Reserved. 44

Based on the input criteria, after clicking **Search**, the trace result is 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

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
Training Institute



FortiGate Security

Network Address Translation

FortiOS 7.2

Last Modified: 23 August 2022

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

DO NOT REPRINT

© FORTINET

Lesson Overview



Introduction to NAT



Firewall Policy NAT



Central NAT



Best Practices and Troubleshooting

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.

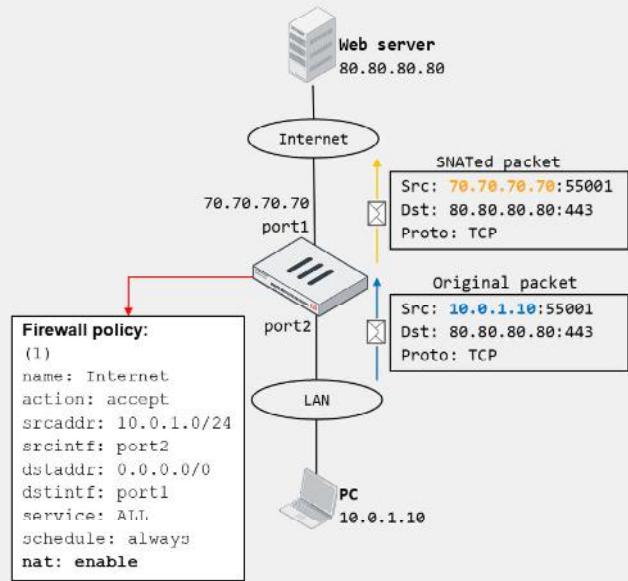
By demonstrating competence in understanding how NAT and PAT work, and the available NAT configuration modes, you will be well-positioned to plan the implementation of NAT in your network.

DO NOT REPRINT

© FORTINET

NAT

- Method of translating IP addresses in a packet
 - If ports are also translated, it is called PAT
- Benefits:
 - Real address is hidden from external networks
 - Prevents depletion of public IP address space
 - Private address space flexibility
- Types:
 - SNAT
 - Translates source IP address and source port
 - Enabled on firewall policy or using central SNAT rules
 - DNAT
 - Translates destination IP address and destination port
 - Requires VIP object on firewall policy
 - In central NAT, no need to reference VIP on firewall policy
- NAT64 and NAT46
 - Translates IPv6 to IPv4, and the reverse
- NAT66
 - NAT between two IPv6 networks



NAT is a method that enables a NAT device such as a firewall or router, to translate (or map) the IP address in a packet to another IP address, usually for connectivity purposes. If the port information in the packet is also translated, then the translation method is called PAT. NAT provides the following benefits:

- Security: The real address of a device is hidden from external networks.
- Public address depletion prevention: Hundreds of computers can share the same public IPv4 address.
- Private address flexibility: The addresses can stay the same, even if ISPs change. You can reuse private addresses in multiple networks.

There are two types of NAT: SNAT and DNAT. In SNAT, a NAT device translates the source IP address and source port in a packet. In DNAT, a NAT device translates the destination IP address and destination port. You can configure FortiGate to perform SNAT and DNAT as follows:

- For SNAT, you enable NAT on the matching firewall policy. Alternatively, you can enable central NAT to configure central SNAT rules for the VDOM.
- For DNAT, you configure virtual IPs (VIPs) and then reference them on the matching firewall policy. If you enable central NAT, you configure central DNAT rules and VIP objects for DNAT.

The example on this slide shows the most common use case for NAT: SNAT. FortiGate, acting as a NAT device, translates the private IP address assigned to the PC to the public address assigned by your ISP. The private-to-public source address translation is needed for the PC to access the internet web server.

NAT64 and NAT46 refer to the methods that translate an IPv6 address to an IPv4 address and the reverse, respectively. They enable you to communicate IPv6 networks with IPv4 networks, and the reverse. NAT66 consists of translating addresses between two IPv6 networks.

DO NOT REPRINT**© FORTINET**

Configuration Modes for NAT

- There are two ways to configure SNAT and DNAT:
 - Firewall policy NAT
 - You configure SNAT and DNAT on firewall policies
 - SNAT uses the outgoing interface address or configured IP pool
 - DNAT uses the configured VIP as the destination address
 - Central NAT
 - You configure SNAT and DNAT per virtual domain
 - It applies to multiple firewall policies, based on SNAT and DNAT rules
 - Configure SNAT rule in central SNAT policy
 - Configure DNAT using DNAT and VIP objects

You configure NAT using firewall policy NAT mode or central NAT.

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

When you use central NAT, you configure NAT per virtual domain by configuring SNAT and DNAT rules. The result is that SNAT and DNAT settings automatically apply to multiple firewall policies, 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 a benefit of using NAT?

- A. Prevents depletion of IPv4 public address
- B. Enhanced content inspection

2. Which statement about NAT66 is true?

- A. It is used to translate addresses between two IPv6 networks.
- B. It is used to translate addresses between two IPv4 networks.

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to NAT

Firewall Policy NAT

Central NAT

Best Practices and Troubleshooting

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 firewall 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

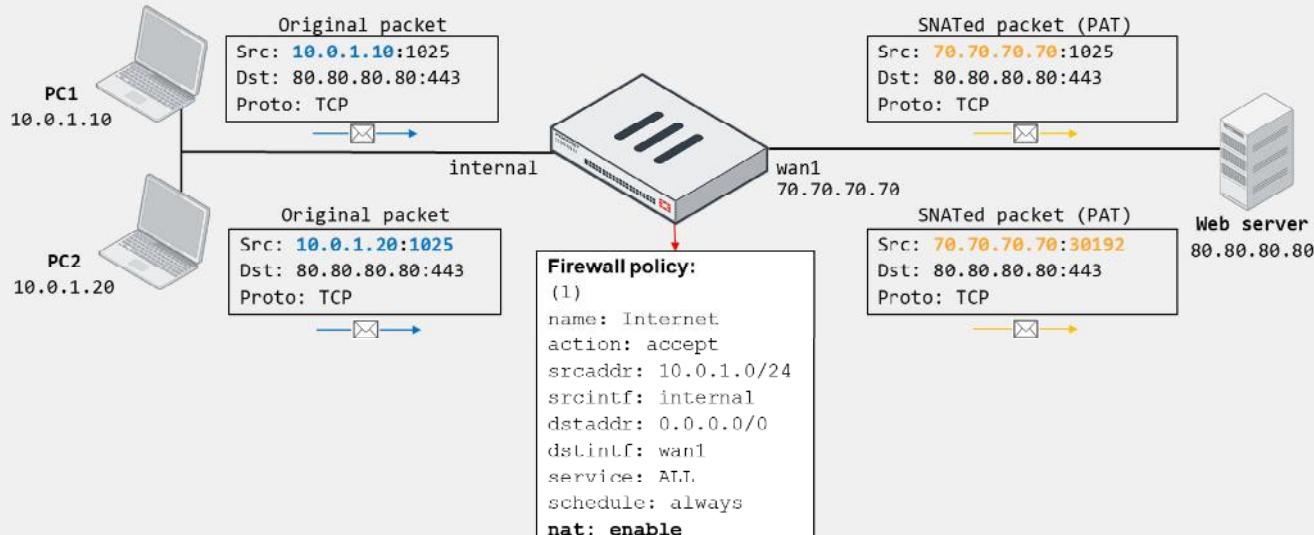
Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT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

There are 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
 Training Institute

© Fortinet Inc. All Rights Reserved.

10

When you select **Use Outgoing Interface Address** on the matching firewall policy, FortiGate uses the egress interface address as the NAT IP for performing SNAT.

If there are multiple devices behind FortiGate, FortiGate performs many-to-one NAT. This is also known as PAT. FortiGate assigns to each connection sharing the egress interface address a port number from a pool of available ports. The assignment of a port enables FortiGate to identify packets associated with the connection and then perform the corresponding translation. 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 is established.

The example on this slide shows two PCs behind FortiGate that share the same public IP address (70.70.70.70) to access the internet web server 80.80.80.80. Because **Use Outgoing Interface Address** is enabled on the firewall policy—set `nat enable` on the CLI—the source IP address of the PCs is translated to the egress interface address. The source port, however, is not always translated. It depends on the available ports and the connection 5-tuple. In the example shown on this slide, FortiGate translates the source port of the connection from PC2 only. Otherwise, the two connections would have the same information on the session table for the reply traffic, which would result in a session clash.

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

Useful for CGN



Policy & Objects > IP Pools

New Dynamic IP Pool	
Name	<input type="text"/>
Comments	<input type="text" value="Write a comment..."/>
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" value="0.0.0.0-0.0.0"/>
NAT64	<input type="checkbox"/>
ARP Reply	<input type="checkbox"/>

Policy & Objects > Firewall Policy

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

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 are 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 you can configure on the FortiGate firewall:

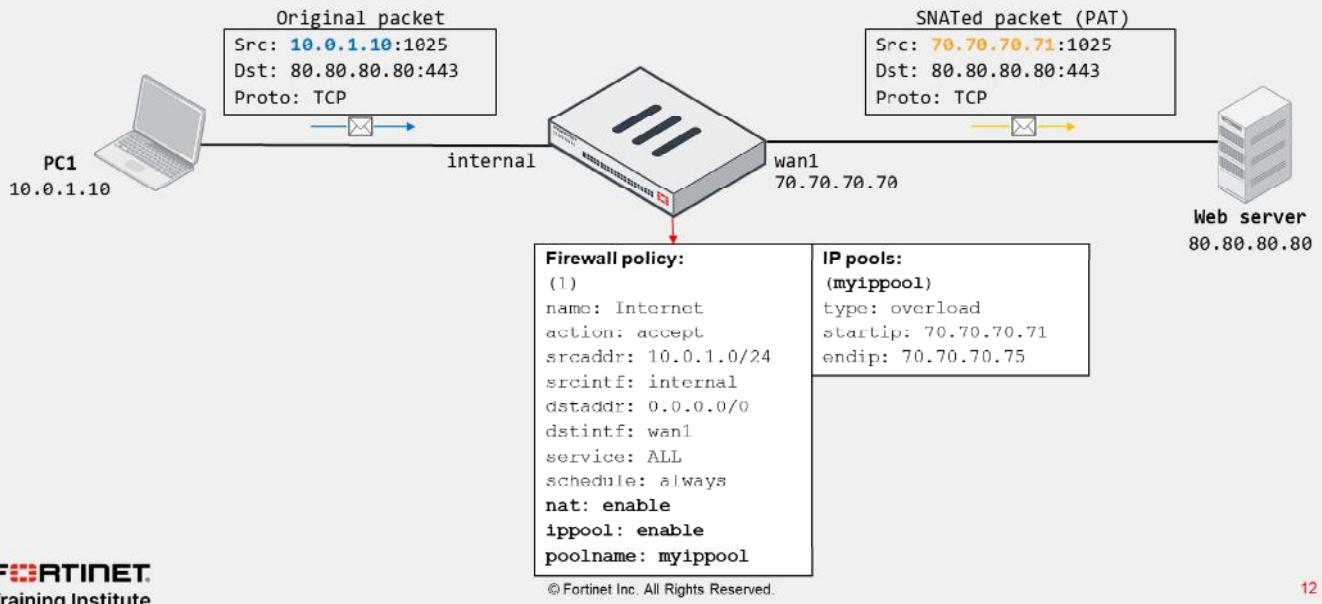
- Overload
- One-to-one
- Fixed port range
- Port block allocation

The fixed port range and port block allocation types are more common carrier-grade NAT (CGN) deployments.

DO NOT REPRINT

© FORTINET

IP Pool Type—Overload



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 the pool can support.

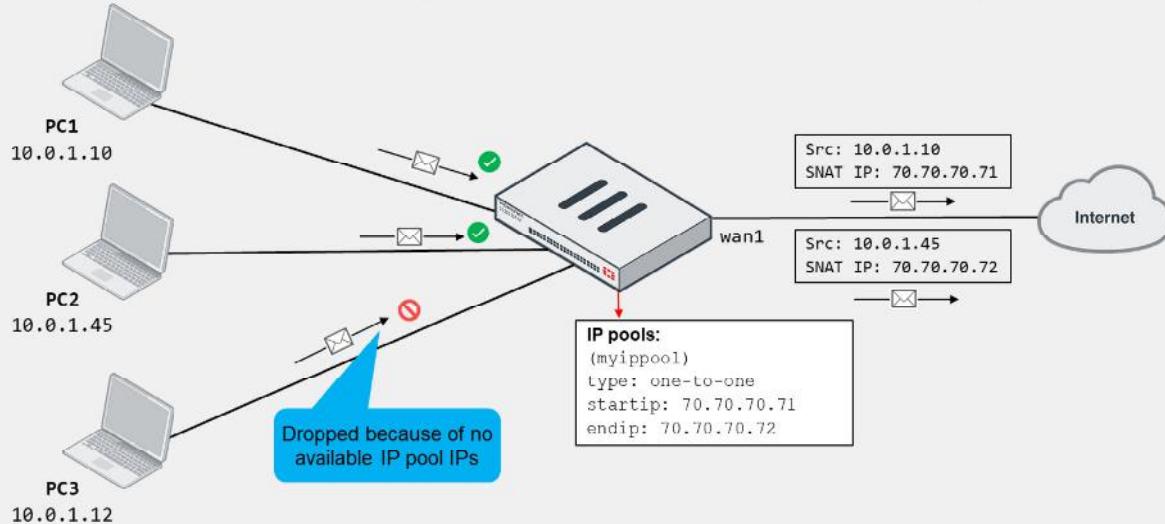
The default IP pool type is overload. In the overload IP pool type, a many-to-one or many-to-few relationship and port translation is used.

In the example shown on this slide, source IP 10.0.1.10 is translated to the address 70.70.70.71, which is one of the addresses defined in the IP pool (70.70.70.71 – 70.70.70.75).

DO NOT REPRINT
© FORTINET

IP Pool Type—One-to-One

- Assigns an IP pool address to an internal host on a first-come, first-served basis
 - Packets from unserved hosts are dropped if there are no available addresses in the IP pool



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

13

In the one-to-one pool type, FortiGate assigns an IP pool address to an internal host on a first-come, first-served basis.

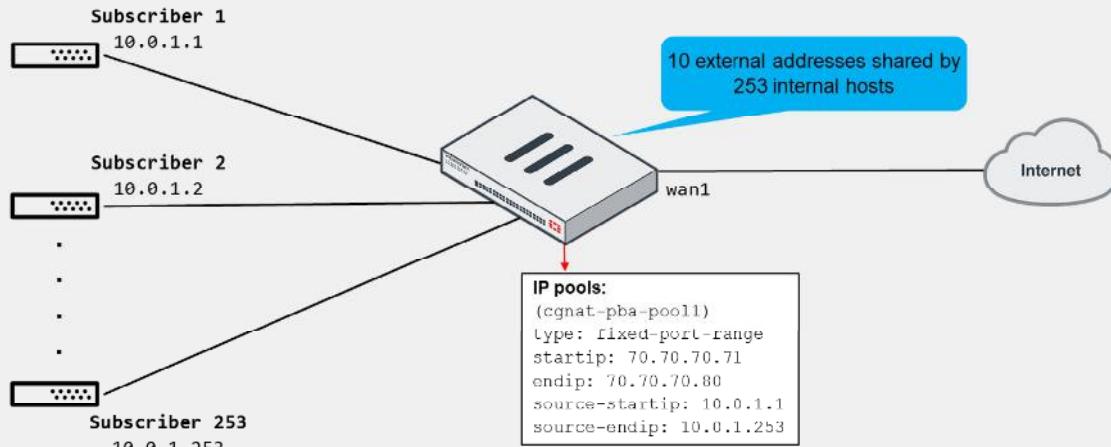
There is a single mapping of an internal address to an external address. That is, an IP pool address is not shared with any other internal host, thus the name one-to-one. If there are no more addresses available in the IP pool, FortiGate drops packets from unserved hosts.

The example on this slide shows three internal hosts accessing the internet. PC1 and PC2 packets are received first by FortiGate and, therefore, served with addresses 70.70.70.71 and 70.70.70.72, respectively. However, FortiGate drops packets sourced from PC3 because they arrived last, which is when there are no more available addresses in the IP pool to choose from.

DO NOT REPRINT
© FORTINET

IP Pool Type—Fixed Port Range

- Useful for service providers in CGN environments
 - Ability to identify the subscriber of a connection by public IP address and port (no traffic log required)



ISPs must be able to identify the subscriber responsible for a given connection should authorities require it. If the ISP performs NAT to subscriber traffic, then the traffic will share one or more public addresses. One way to track the traffic and, therefore, the NAT details for each connection, is by logging them. However, this can result in a huge number of resources that the ISP needs to dedicate for logging purposes only.

Another option is to deploy a CGN-focused feature such as a fixed port range IP pool. Fixed port range IP pools enable administrators to track connections by public address and port without having to log every session. When you configure a fixed port range IP pool, you indicate a range of external IP addresses that FortiGate uses to perform NAT on traffic sourced from a range of internal IP addresses. It is called fixed port range because FortiGate calculates the port block size and the number of available port blocks for the IP pool based on the number of configured internal and external IP addresses. FortiGate then allocates one or more port blocks to internal hosts when performing NAT, which is what enables the administrator to track connections without having to log them.

The example on this slide shows a fixed port range IP pool. The internal address range 10.0.1.1 to 10.0.1.253 maps to the external address range 70.70.70.71 to 70.70.70.80. That is, FortiGate shares ten external addresses with 253 internal addresses.

DO NOT REPRINT

© FORTINET

IP Pool Type—Fixed Port Range (Contd)

- Port block size and the number of available port blocks by external address:

```
# diagnose firewall ippool list
list ippool info:(vf=root)
ippool cgnat-pba-pool1: id=1, block-sz=2323, num-block=1, fixed-port=no, use=2
    nat ip-range=70.70.70.71-70.70.70.80 start-port=5117, num-pba-per-ip=26
    source ip-range=10.0.1.1-10.0.1.253 deterministic NAT
    clients=0, inuse-NAT-IPs=0
    total-PBAs=260, inuse-PBAs=0, expiring-PBAs=0, free-PBAs=100.00%
    allocate-PBA-times=0, reuse-PBA-times=0

# diagnose firewall ippool-fixed-range list natip 70.70.70.71
ippool name=cg nat-pba-pool1, ip shared num=26, port num=2323
internal ip=10.0.1.1, nat ip=70.70.70.71, range=5117~7439
internal ip=10.0.1.2, nat ip=70.70.70.71, range=7440~9762
...
internal ip=10.0.1.26, nat ip=70.70.70.71, range=63192~65514

# diagnose firewall ippool-fixed-range list natip 70.70.70.71 5900
ippool name=cg nat-pba-pool1, ip shared num=26, port num=2323
internal ip=10.0.1.1, nat ip=70.70.70.71, range=5117~7439
```

Check block size and number of blocks for IP pool

Detailed external address and port assignment per internal address

Add source port to obtain specific port block for internal address

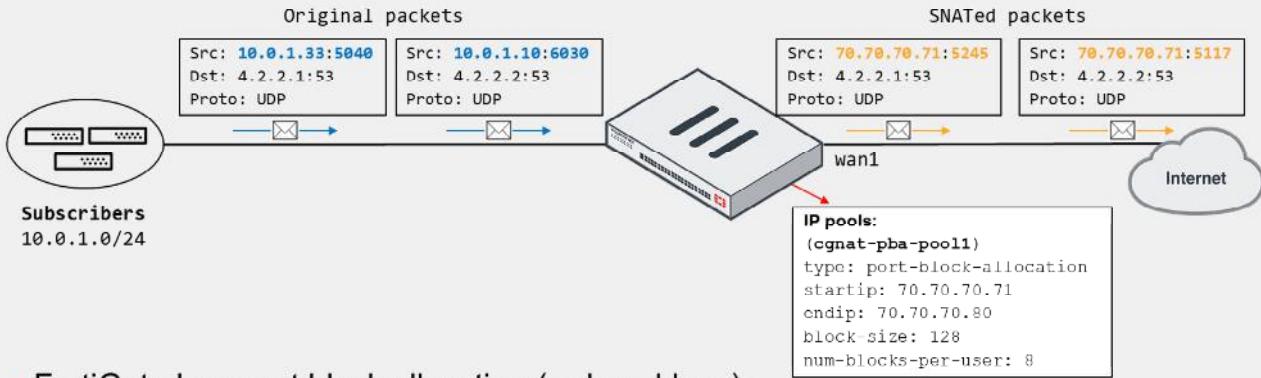
You can use the `diagnose firewall ippool list` command to identify the block size and number of blocks assigned to each external address in the fixed port range IP pool.

You can also use the `diagnose firewall ippool-fixed-range list natip` command to view detailed external address and port assignment information per internal address, as shown on this slide. The result is that you can identify subscribers by providing the public address and port of a connection.

DO NOT REPRINT
© FORTINET

IP Pool Type—Port Block Allocation

- FortiGate allocates a block size and number per host for a range of external addresses
 - Another useful option for CGN



- FortiGate logs port block allocation (reduced logs):

```
System event logs:
action="ippool-create" saddr="10.0.1.33" nat=70.70.70.71 portbegin=5245 portend=5372 poolname="cgnat-pba-pool1"
action="ippool-create" saddr="10.0.1.10" nat=70.70.70.71 portbegin=5117 portend=5244 poolname="cgnat-pba-pool1"
```

The port block allocation IP pool is also a useful option for CGN. It give administrators a more flexible way to control user port allocation for NAT. Unlike the fixed port range IP pool, which requires you to define internal and external IP address ranges, with port block allocation, you define the external IP address range only. You must also indicate the block port size and the number of blocks that FortiGate allocates to each host (or source IP address). The result is that each source IP address is limited to the number of blocks and ports configured in the IP pool, thus preventing port exhaustion caused by a few hosts.

For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator. The administrator can then look at the system event logs to identify internet connections made by a device should the authorities require such information. That is, like the fixed port block case, the administrator doesn't have to log the traffic for connection identification purposes.

The example on this slide shows how port block allocation assignment takes place. FortiGate allocates port blocks on a first-come, first-served basis. The port block allocation is made when FortiGate receives a packet from unserved hosts. In the example, 10.0.1.10 and 10.0.1.33 are unserved hosts that try to access the internet. FortiGate then allocates the port blocks to each host and performs the respective SNAT on traffic. Upon allocation, FortiGate also generates system event logs with the port block allocation details to inform the administrator.

Note that the system event logs shown on this slide have been cut to fit the slide.

DO NOT REPRINT

© FORTINET

VIPs

- DNAT objects
- Default type is **Static NAT**
 - One-to-one mapping, applies to both:
 - Ingress traffic (DNAT; use internal IP as NAT IP)
 - Egress traffic (SNAT; use external IP as NAT IP)
 - Reference IP addresses or FQDN objects (set **Type** to **FQDN**)
- Enable **Port Forwarding** to:
 - Redirect traffic destined to external IP and port to mapped internal address and port
 - Reuse external IP on multiple VIPs

The screenshot shows two configuration windows. The top window, 'Policy & Objects > Virtual IPs', displays a 'New Virtual IP' form. The 'Name' field is 'VIP-INTERNAL-HOST', 'VIP type' is 'IPv4', 'Interface' is 'port1', 'type' is 'Static NAT', 'External IP address/range' is '100.64.100.22', and 'Map to' is '10.0.1.10'. The bottom window, 'Policy & Objects > Firewall Policy', shows a 'New Policy' configuration. In the 'Destination' field, 'VIP INTERNAL HOST' is selected. A blue callout box with the text 'VIP used as destination in firewall policy' points to this selection. A red arrow points from the 'VIP INTERNAL HOST' entry in the destination field to the 'VIP INTERNAL HOST' entry in the 'Map to' field of the Virtual IP form.

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

The default VIP type is **Static NAT**. This is a one-to-one mapping. This means that:

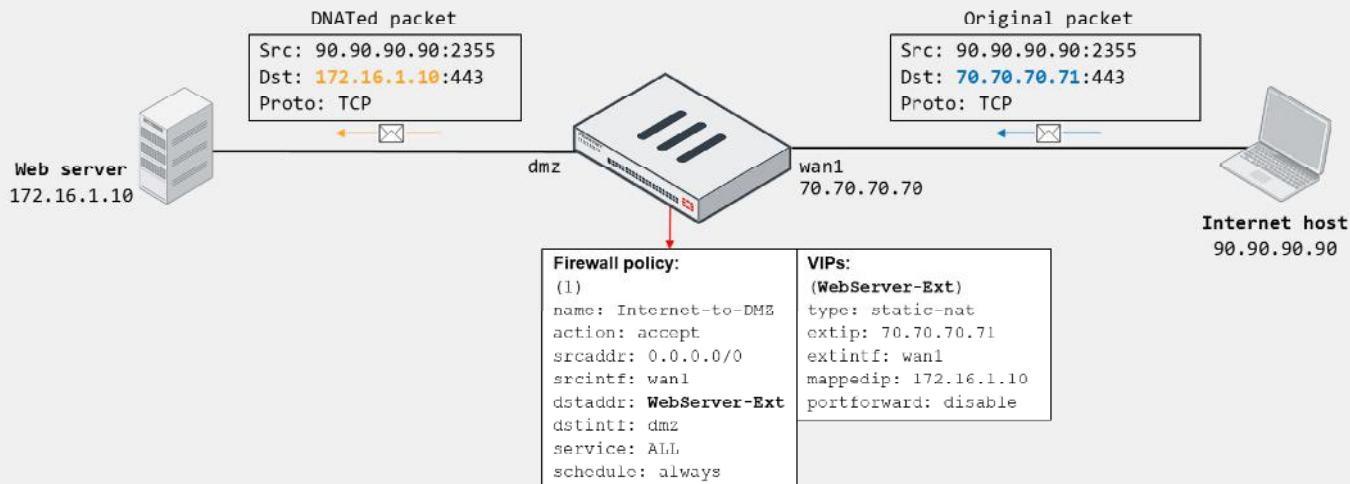
1. FortiGate performs DNAT on ingress traffic destined to the external IP address defined in the VIP, regardless of the protocol and port of the connection, provided the matching firewall policy references the VIP as **Destination**.
2. FortiGate uses as NAT IP the external IP address defined in the VIP when performing SNAT on all egress traffic sourced from the mapped address in the VIP, provided the matching firewall policy has NAT enabled. That is, FortiGate doesn't use the egress interface address as NAT IP.

Note that you can override the behavior described in step 2 by using an IP pool. You can also select **FQDN** as **Type**. When you select **FQDN**, you can configure FQDN address objects as external and internal IP addresses. This enables FortiGate to automatically update the external and internal IP addresses used by the VIP in case the FQDN resolved address changes.

Optionally, you can enable **Port Forwarding** on the VIP to instruct FortiGate to redirect the traffic matching the external address and port in the VIP to the mapped internal address and port. When you enable port forwarding, FortiGate no longer performs one-to-one mapping. This means that you can reuse the same external address and map it to different internal addresses and ports provided the external port is unique. For example, you can configure a VIP so connections to the external IP 70.70.70.70 on port 8080 map to the internal IP 192.168.0.70 on port 80. You can then configure another VIP so connections to the external IP 70.70.70.70 on port 8081 map to the internal IP 192.168.0.71 on port 80.

DO NOT REPRINT
© FORTINET

VIP Example—Static NAT—Incoming Connection

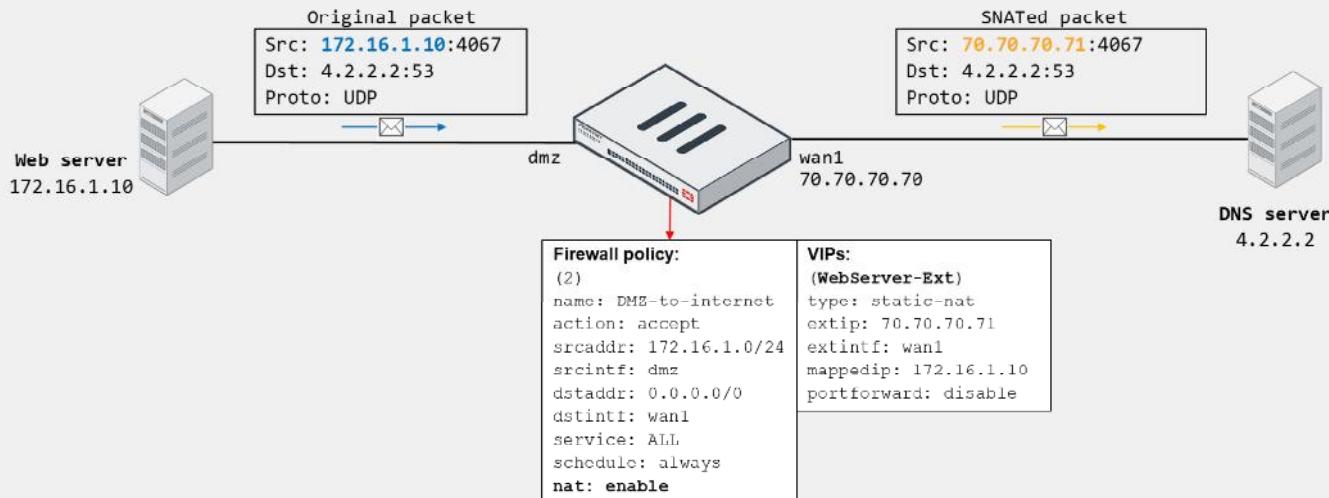


In the example shown on this slide, the internet host initiates a connection to 70.70.70.71 on TCP port 443. On FortiGate, the traffic matches the firewall policy ID 1, which references the WebServer-Ext VIP as destination. Because the VIP is configured as static NAT and has port forwarding disabled, then FortiGate translates the destination address of the packet to 172.16.1.10 from 70.70.70.71. Note that the destination port doesn't change because port forwarding is disabled.

Also note that the external interface address is different from the external address configured in the VIP. This is not a problem as long as the upstream network has its routing properly set. You can also enable ARP reply on the VPN (enabled by default) to facilitate routing on the upstream network. You will learn more about ARP reply in this lesson.

DO NOT REPRINT
© FORTINET

VIP Example—Static NAT—Outgoing Connection

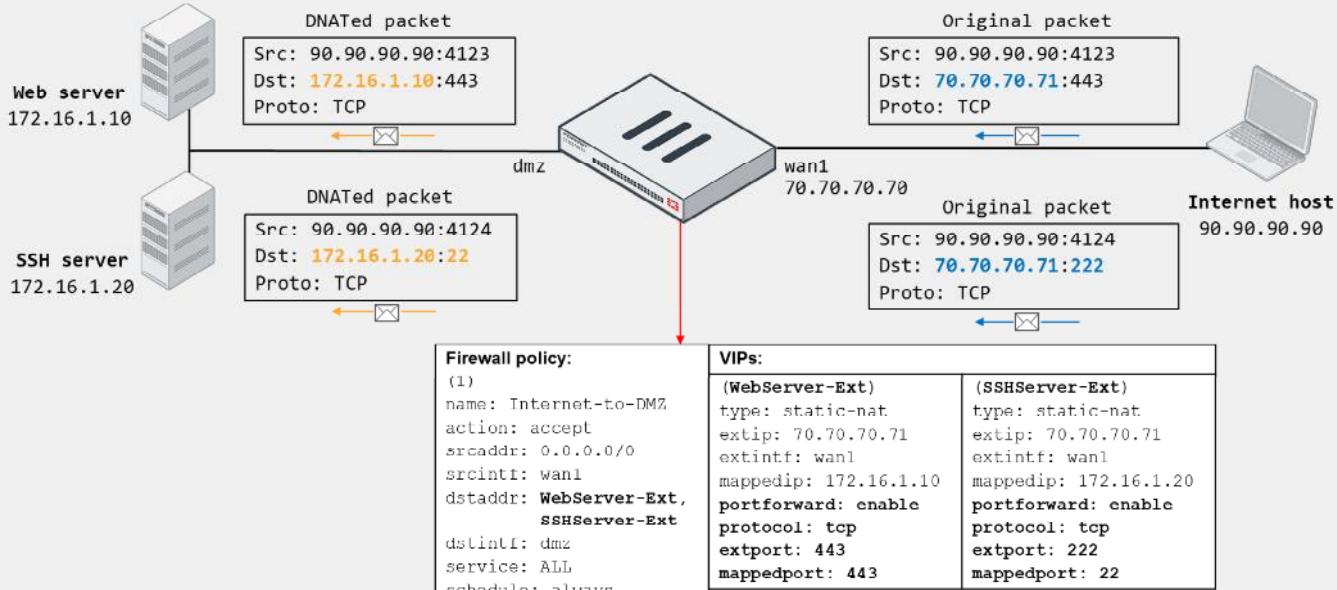


Now, suppose that the internal web server (172.16.1.10) initiates a DNS connection to the internet DNS server (4.2.2.2). On FortiGate, the traffic matches the firewall policy ID 2, which has `nat` enabled. Because the source address matches the internal address of the VIP, and because the VIP is configured as static NAT with port forwarding disabled, FortiGate translates the source address of the packet to 70.70.70.71 from 172.16.1.10. Note that FortiGate doesn't have to perform PAT because the static NAT VIP equals one-to-one mapping. That is, the external IP is used by the web server only for SNAT.

Also note that FortiGate uses the VIP external address for SNAT if the VIP is referenced in an incoming firewall policy. That is, if you don't configure firewall policy ID 1, which is shown on the previous slide, or if you disable the firewall policy, then FortiGate doesn't automatically use the external IP for translating the source address of the web server. Instead, FortiGate uses the egress interface address (70.70.70.70).

DO NOT REPRINT
© FORTINET

VIP Example—Port Forwarding—Incoming Connection



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

20

The example on this slide shows how FortiGate handles two incoming connections to the same external address, but on different ports. FortiGate forwards each connection to a different internal host based on the VIP mapping settings. This is possible because port forwarding is enabled on the VIPs, which enables FortiGate to redirect the external traffic to the corresponding internal address and port, while using the same external address.

Both connections match the firewall policy ID, which references two VIPs as destination. The HTTPS connection matches the WebServer-Ext VIP, and the SSH connection matches the SSHServer-Ext VIP. Note that for the SSH connection, FortiGate also translates the destination port to 22 from 222.

Although not shown on this slide, outgoing connections sourced from the web and SSH server would result in FortiGate using as NAT IP the egress interface address for SNAT, providing there is a matching firewall policy with `nat` enabled.

DO NOT REPRINT

© FORTINET

VIP—Matching Policies

- 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						
2	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Web_server	always	ALL	ACCEPT

Action = DENY

- Two solutions:

- Enable **match-vip** on the deny policy

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

Setting available only
when policy action is set
to deny

- Set the VIP as destination

```
config firewall policy
  edit <deny policy ID>
    set dstaddr <VIP>
  next
end
```

In FortiOS, VIPs and firewall address objects are completely different. They are stored separately with no overlap. This means that, by default, firewall address objects do not match VIPs.

In the example shown on this slide, the destination of the first firewall policy is set to **all**. Even though this means all destination addresses (0.0.0.0/0), by default, this doesn't include the external addresses defined on the VIPs. The result is that traffic destined to the external address defined on the **Web_server** VIP skips the first policy and matches the second policy instead.

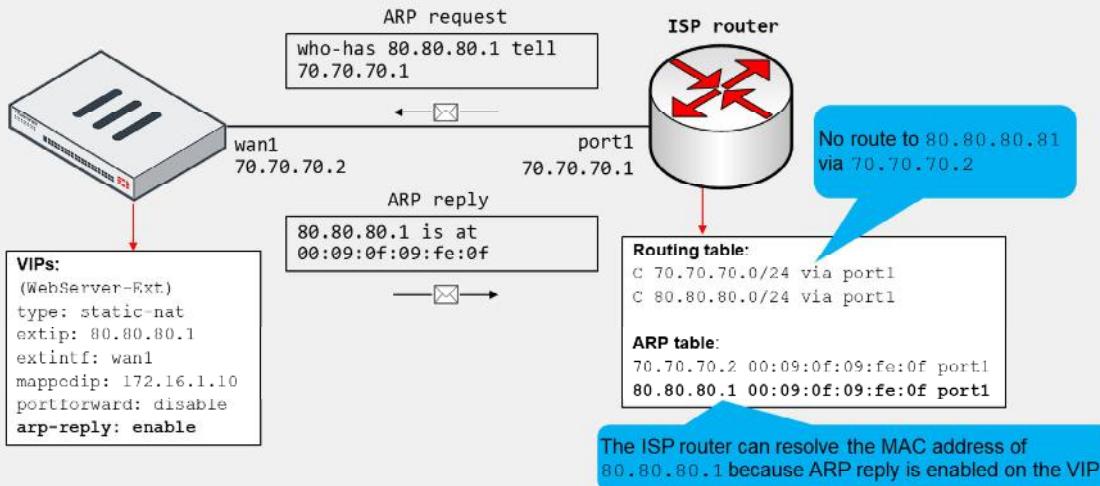
But what if you want the first policy to block all incoming traffic to all destinations, including the traffic destined to any VIPs? This is useful if your network is under attack, and you want to temporarily block all incoming external traffic. You can do this by enabling **match-vip** on the first firewall policy. Enabling **match-vip** instructs FortiGate to also check for VIPs during policy evaluation. Note that the **match-vip** setting is available only when the firewall policy action is set to **DENY**.

In case you want to block only traffic destined to one or more VIPs, you can reference the VIPs as the destination address on the deny firewall policy.

DO NOT REPRINT
© FORTINET

ARP Reply Option in VIPs and IP Pools

- Enabled by default; instructs FortiGate to reply to ARP requests for external address
- Sometimes required to overcome routing misconfigurations
 - Example:



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

22

When you configure a VIP or an IP pool, ARP reply is enabled by default. When ARP reply is enabled, FortiGate replies to incoming ARP requests for the external address configured in the VIP and IP pools.

Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled.

Consider the example shown on this slide, which shows an internet connection between FortiGate and an ISP router. The example also shows a simplified version of the ISP router routing table and ARP table.

The ISP assigns the FortiGate administrator the public subnet 80.80.80.0/24 to deploy internet-facing services. The administrator configured the VIP shown on this slide to provide internet users with access to the company web server. While testing, the administrator confirms that internet users can reach the web server at 80.80.80.1.

However, the administrator is likely unaware that having ARP reply enabled was key for a successful connectivity. The reason is that the ISP router doesn't have a route in its routing table to access the 80.80.80.0/24 subnet through the 70.70.70.2 gateway. Instead, the routing table contains a connected route for the subnet through port1. The result is that the ISP router generates ARP requests out of port1 to resolve the MAC address of any of the addresses in the 80.80.80.0/24 subnet. Nonetheless, because FortiGate responds to ARP requests for the external address in the VIP, the ISP router is able to resolve the MAC address successfully.

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

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Introduction to NAT****Firewall Policy NAT****Central NAT****Best Practices and Troubleshooting**

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

- Enable or disable on the GUI or CLI (default = disable)

System > Settings > Central SNAT

NGFW Mode **Profile-based** Policy-based

Central SNAT

```
config system settings
    set central-nat enable
end
```

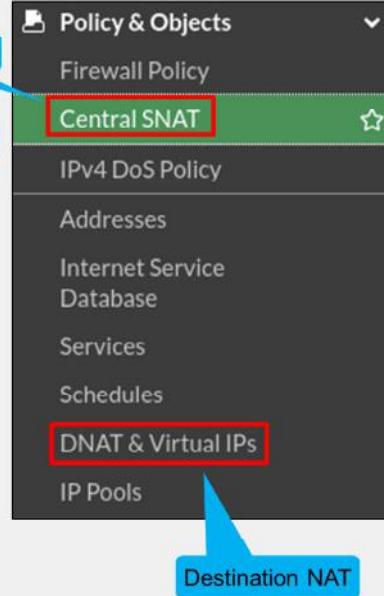
Source NAT

Enable central NAT from GUI or CLI

- Must remove VIP and IP pool references from existing policies

```
# config system settings
(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



By default, central NAT is disabled. You can enable it on the CLI or the GUI. After central NAT is enabled, the following 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 pools or VIPs configured in firewall policies?

The CLI does not allow this and presents 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 policy-based mode. This means SNAT behaves only according to the NAT settings found by clicking **Policy & Objects > Central SNAT**.

DO NOT REPRINT

© FORTINET

Central SNAT

- Configure SNAT on central SNAT policies
 - Useful for advanced SNAT
 - Firewall policy and central SNAT policy segregation
 - Simplifies firewall policy configuration
- Central SNAT policy matching criteria:
 - Incoming interface
 - Outgoing interface
 - Source address
 - Destination address
 - Protocol
 - Source port (explicit port mapping)
- SNAT policies are evaluated from top to bottom
 - If no match is found, traffic is not SNATed

Policy & Objects > Central SNAT

New Policy

Incoming Interface	port3	x
Outgoing Interface	port1	x
Source Address	LOCAL_SUBNET	x
Destination Address	all	x

NAT

NAT NAT IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Protocol any TCP UDP SCTP Specify 6

Explicit port mapping

Comments 0/1023

Enable this policy

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

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

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

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

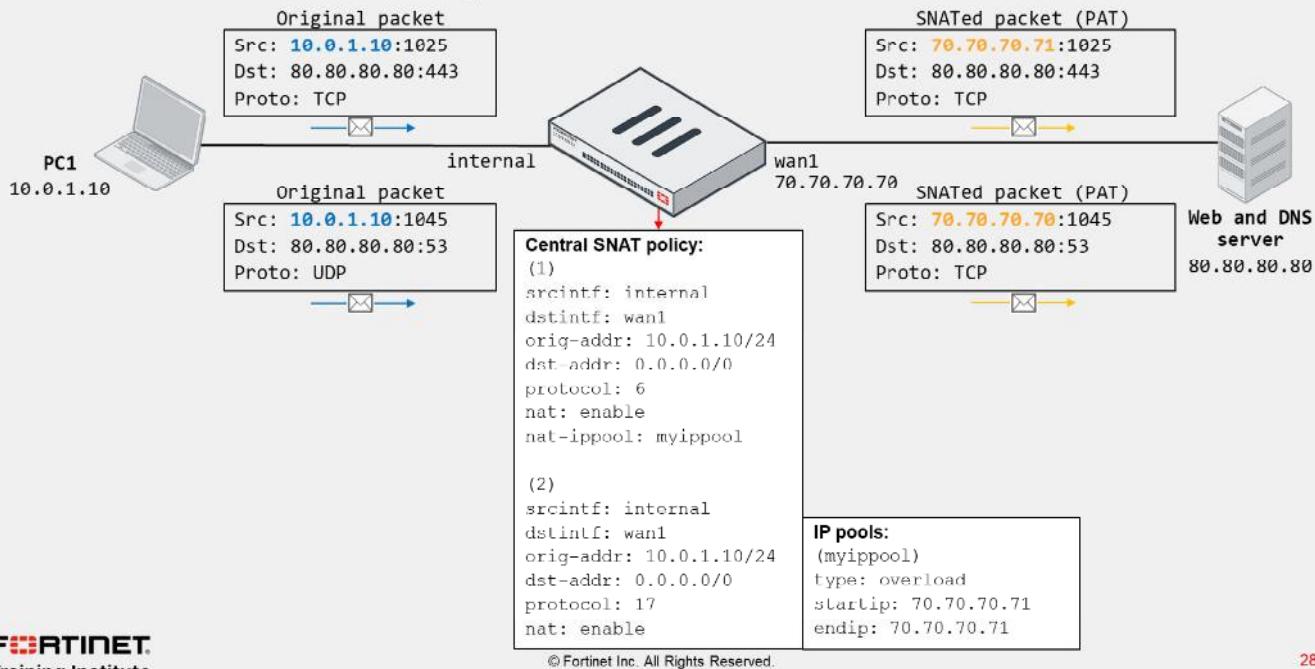
You must also indicate whether you want to perform SNAT using the outgoing interface address or an IP pool. Note that if you enable central NAT mode, FortiGate doesn't perform SNAT on traffic unless you configure the corresponding matching central SNAT policy. Similarly, if the traffic doesn't match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

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

DO NOT REPRINT

© FORTINET

Central SNAT Example



28

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

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

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

DO NOT REPRINT

© FORTINET

Central DNAT and VIPs

- Kernel has DNAT rules based on configured VIPs
 - You no longer reference VIPs in firewall policies
- Firewall policy
 - Destination address must match the VIP mapped address
 - DNAT takes place before firewall policy lookup

Policy & Objects > DNAT and Virtual IPs

Edit DNAT & Virtual IP

DNAT & VIP type: IPv4 DNAT

Name: VIP-INTERNAL-HOST

Comments: Write a comment... 0/255

Status: Disable to exclude VIP from DNAT

Network

Interface: port1

Type: Static NAT

Source interface filter:

External IP address/range: 70.70.70.71

Map to

IPv4 address/range: 10.0.1.10

Optional Filters

Port Forwarding

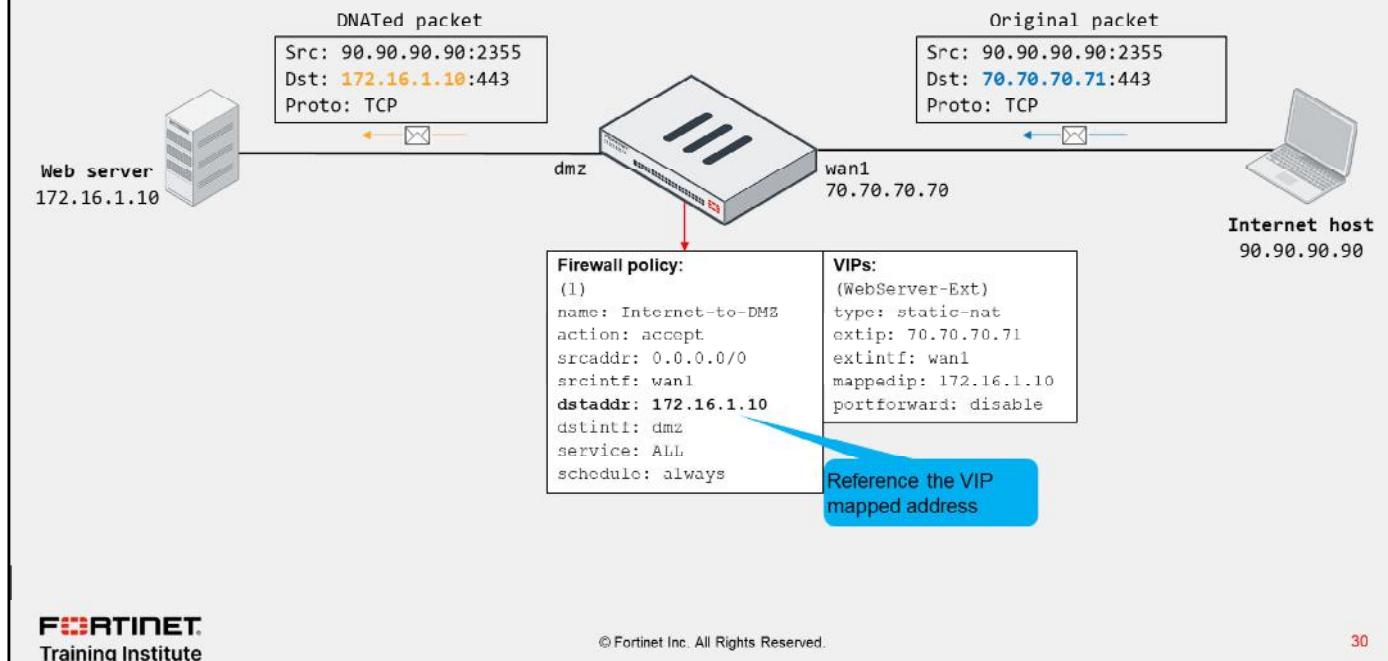
When you enable central NAT, you no longer reference VIPs on firewall policies. Instead, FortiGate automatically creates a rule in the kernel to perform DNAT for the matching traffic based on the configured VIPs. You configure the VIPs on the **DNAT and Virtual IPs** page.

Like in the central SNAT case, you must also have a matching firewall policy that accepts the traffic you want to DNAT. However, instead of referencing the VIP, you reference the mapped internal address as destination in the firewall, and *not* the external address. This is because for ingress traffic, DNAT takes place before the firewall policy lookup. That is, FortiGate considers the translated destination address during the firewall policy lookup process.

In central NAT mode, VIPs take effect right after you create them. In case you want to exclude a VIP from DNAT, you can disable the object on the FortiGate GUI by using the **Status** button.

DO NOT REPRINT
© FORTINET

DNAT and VIPs Example



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

30

In the example shown on this slide, the internet host initiates a connection to 70.70.70.71 on TCP port 443. On FortiGate, the traffic matches the firewall policy ID 1, which references the web server internal address (172.16.1.10) as the destination. Because the VIP is configured as static NAT and has port forwarding disabled, then FortiGate translates the destination address of the packet to 172.16.1.10 from 70.70.70.71.

Note that you configure the firewall policy to match the VIP mapped address as the destination, and *not* the VIP external address.

DO NOT REPRINT**© FORTINET**

Disabling Central NAT

- Disable central NAT on the FortiGate CLI:

```
config system settings
    set central-nat disable
end
```

- When disabled, FortiGate stops performing NAT on traffic
 - FortiGate requires NAT configuration on firewall policies
- Configure SNAT by enabling NAT on firewall policy
 - Optionally, reference IP pool
- Configure DNAT by referencing VIP as destination on firewall policy



© Fortinet Inc. All Rights Reserved.

31

You can disable central NAT on the FortiGate CLI by disabling `central-nat` under `config system settings`.

However, note that when you disable central NAT, FortiGate stops performing NAT on traffic because it now requires the NAT configuration to be applied on the corresponding firewall policies. For FortiGate to perform SNAT, you must enable NAT on the respective firewall policy and, optionally, reference the IP pool. For DNAT, you must reference the VIP object as the destination on the corresponding firewall policies.

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 is used.
- B. NAT is not be applied to the firewall session.

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to NAT

Firewall Policy NAT

Central NAT

Best Practices and Troubleshooting

Good job! You now understand central NAT.

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 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, and best practices for NAT implementation, you should be able to monitor and troubleshoot common NAT issues, and successfully implement NAT in your network.

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

```
# diagnose firewall ippool-all list
vdom:root owns 1 ippool(s)
name:myippol
type:overload
nat-ip-range:10.200.1.100-10.200.1.100
```



© Fortinet Inc. All Rights Reserved.

35

You can run the `diagnose firewall ippool-all list` command to display the configured IP pools and their settings.

DO NOT REPRINT

© FORTINET

Monitoring NAT Sessions With Diagnose Commands (Contd)

- 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 shows only stats of IP pool named 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 shows 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
```

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

The `stats` command provides 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 a specific IP pool by using the name of the IP pool.

DO NOT REPRINT**© FORTINET**

NAT Implementation Best Practices

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IPs of each IP pool
 - Ensure that the IP pool address range does not overlap with addresses assigned to FortiGate and hosts
 - If internal and external users are accessing the same servers, configure your DNS service so internal users resolve to the destination internal address
- Don't configure a 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.

37

Use the following best practices when implementing NAT:

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IPs of each IP pool.
 - Ensure that the IP pool address range 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, configure your DNS services so internal users resolve to use the destination internal address instead of its external address defined in the VIP.
- Don't configure a NAT rule for inbound traffic unless it is required by an application. 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

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to NAT

Firewall Policy NAT

Central NAT

Best Practices and Troubleshooting

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
- ✓ 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 lesson.

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

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Security

Firewall Authentication

FortiOS 7.2

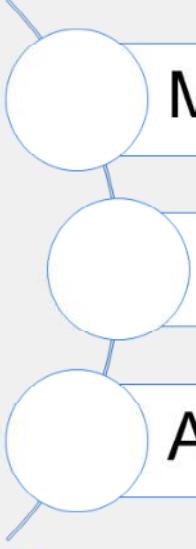
Last Modified: 13 June 2022

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

DO NOT REPRINT

© FORTINET

Lesson Overview



Methods of Firewall Authentication

User Groups

Authentication Using Firewall Policies

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
- Understand the roles of LDAP and RADIUS
- Describe active and passive authentication and order of operations

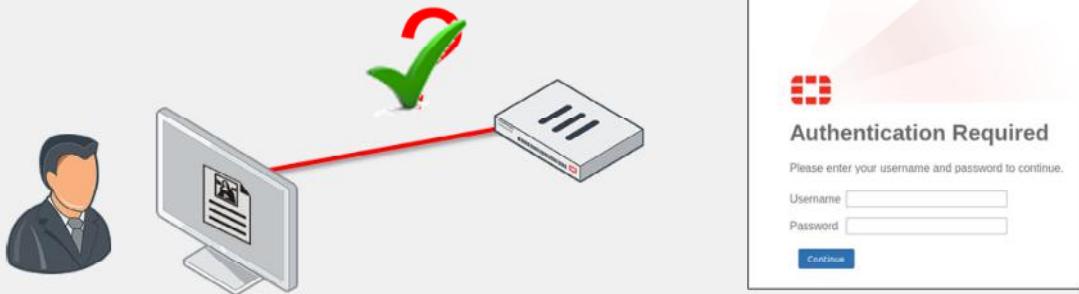
After completing this section, you should be able to achieve the objectives shown on this slide.

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



 **Authentication Required**

Please enter your username and password to continue.

Username

Password

Traditional firewalling grants 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:

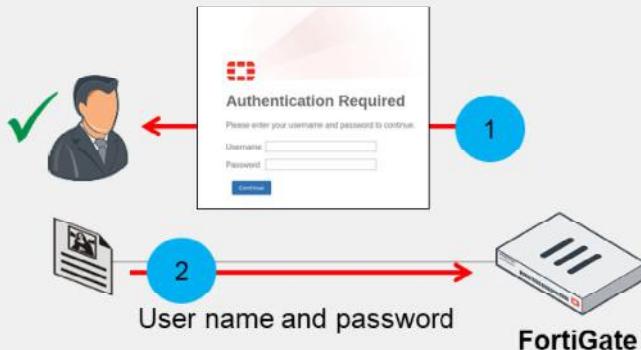
- Local password authentication
- Server-based password authentication (also called remote password authentication)
- Two-factor authentication
This is a system of authentication that is enabled on top of an existing method—it cannot be enabled without first configuring one of the other methods. It requires 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 stored locally on FortiGate
 - Works well for single FortiGate installations



User & Authentication > User Definition

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Username: Student

Password: *****

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Two-factor Authentication

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

User Account Status: Enabled

User Group:

6

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

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.

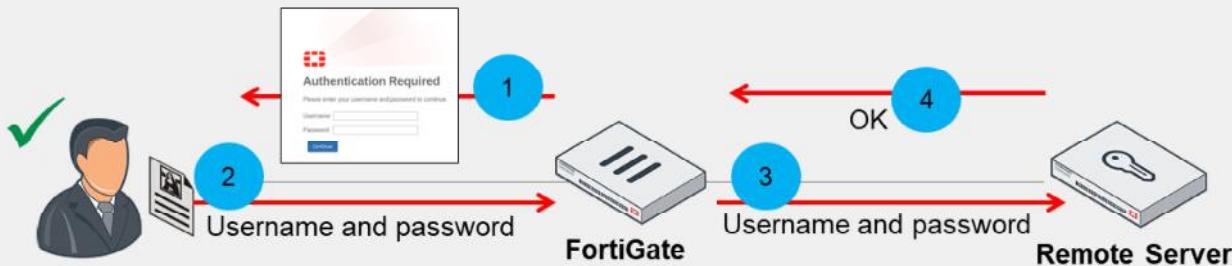
After you create the user, you can add the user—or any preconfigured user group in which the user is a member—to a firewall policy, in order to authenticate. You will learn about user groups and firewall policies in this lesson.

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



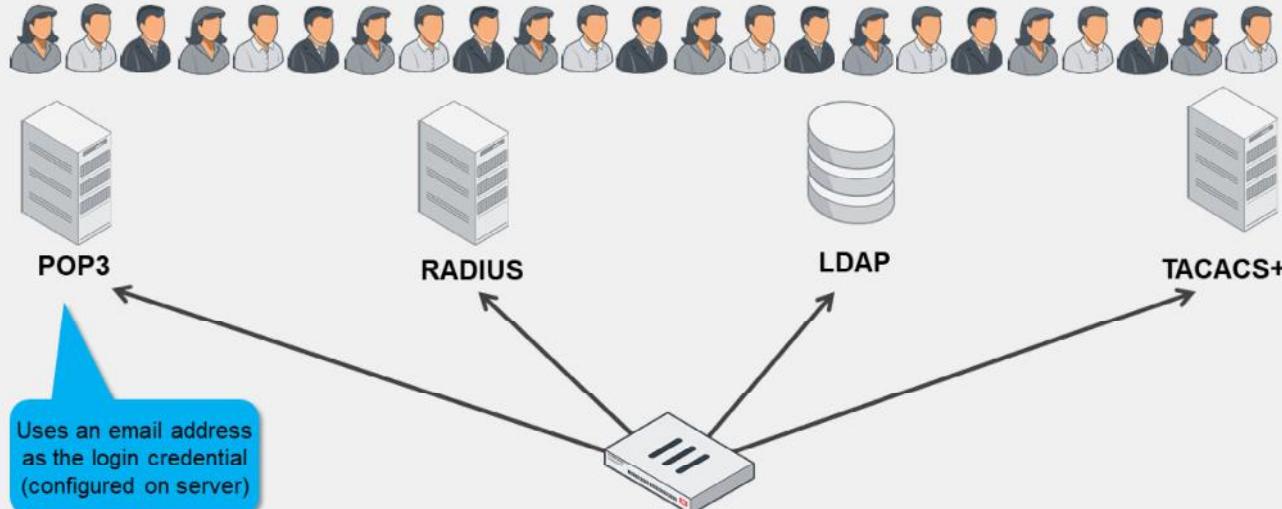
When server-based password authentication is used, a remote authentication server authenticates users. This method is desirable when multiple FortiGate devices need to authenticate the same users or user groups, or when adding FortiGate to a network that already contains an authentication server.

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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 you can configure LDAP 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

Must be preconfigured on FortiGate

User & Authentication > User Definition

FORTINET.
 Training Institute

© Fortinet Inc. All Rights Reserved.

9

You can configure FortiGate to use external authentication servers in the following two ways:

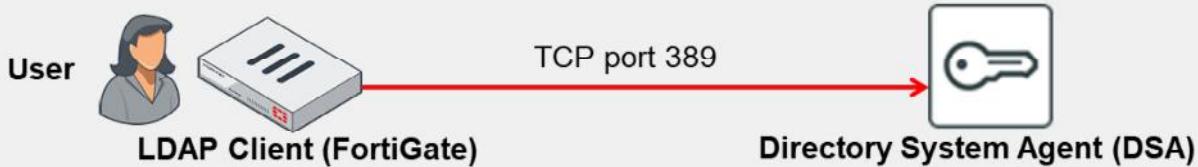
- Create user accounts on FortiGate. With this method, you must select the remote authentication server type (RADIUS, TACACS+, or LDAP), point FortiGate to your preconfigured remote authentication server, and add the user to an appropriate group. This is usually done when you want to add two-factor authentication 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 servers, 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. You will learn about user groups and firewall policies later in this lesson.

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

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

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

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
Exchange server	<input checked="" type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
Username	uid=adadmin,cn=Users,dc=trainingAD,dc=local
Password	*****
Secure Connection	<input checked="" type="checkbox"/>
Connection status	✓ Successful
<input type="button" value="Test Connectivity"/> Test User Credentials	

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 you use to find the user name. Some schemas allow you to use the attribute userid. 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. You must use the setting **Regular** (to specify a regular bind) 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. LDAPS uses port 636 for communication.

The **Test Connectivity** button tests only whether the connection to the LDAP server is successful or not. To test whether a user's credentials can successfully authenticate, you can use the **Test User Credentials** button or use the CLI.

DO NOT REPRINT**© FORTINET**

RADIUS Overview

- RADIUS is a standard protocol that provides AAA services



RADIUS is much different from LDAP, because there is no directory tree structure to consider. RADIUS is a standard protocol that provides authentication, authorization, and accounting (AAA) services.

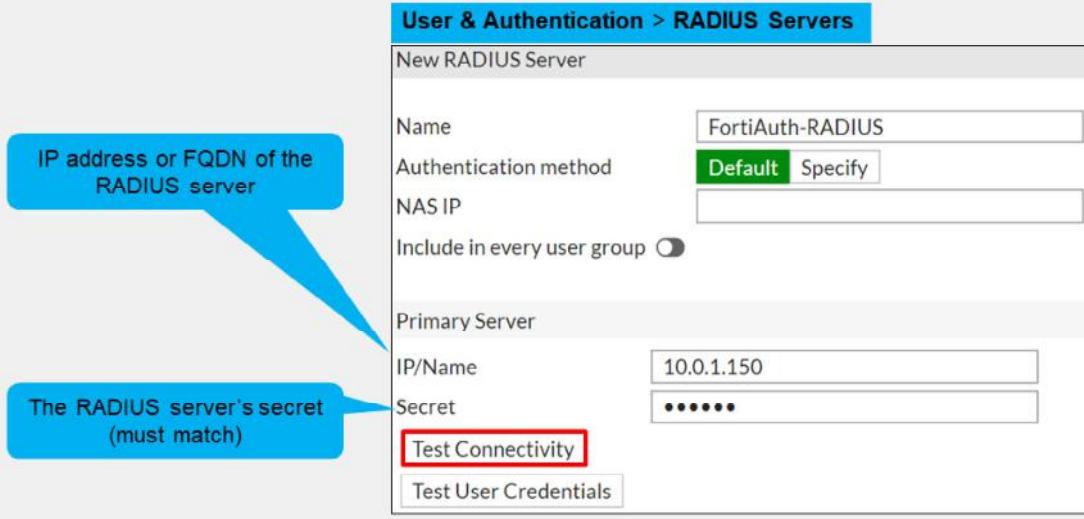
When a user is authenticating, the client (FortiGate) sends an ACCESS-REQUEST packet to the RADIUS server. The reply from the server is one of the following:

- 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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

13

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**, FortiGate will use pap, mschap2, and chap (in that order).

Unlike LDAP configurations, the **Test Connectivity** button used in the example shown on this slide 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 FortiGate. So, you should enable this option only 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 the LDAP and RADIUS Query on the CLI

- diagnose test authserver ldap <server_name> <username> <password>
- Example:

```
# diagnose test authserver ldap External_Server aduser1 Training!
authenticate 'aduser1' against 'External_Server' succeeded!
Group membership(s) - CN=AD-users,OU=Training,DC=trainingAD,DC=training,DC=lab
```

- diagnose test authserver radius <server_name> <scheme> <user> <password>
- Example:

```
# diagnose test authserver radius FortiAuth-RADIUS pap student fortinet
authenticate 'student' against 'pap' succeeded, server=primary
assigned_rad_session_id=810153440 session timeout=0 secs!
Group membership(s) - remote-RADIUS-admins
```

Group memberships are provided by vendor-specific attributes configured on the RADIUS server

Use the diagnose test authserver command on the CLI to test whether a user's credentials can successfully authenticate. You want to ensure that authentication is successful, before implementing it on any of your firewall policies.

The response from the server reports success, failure, and group membership details.

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

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 a 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.

15

Traditional user authentication requires your user name plus something you know, such as a password. The weakness in this traditional method of authentication is that if someone obtains your username, they need only 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.

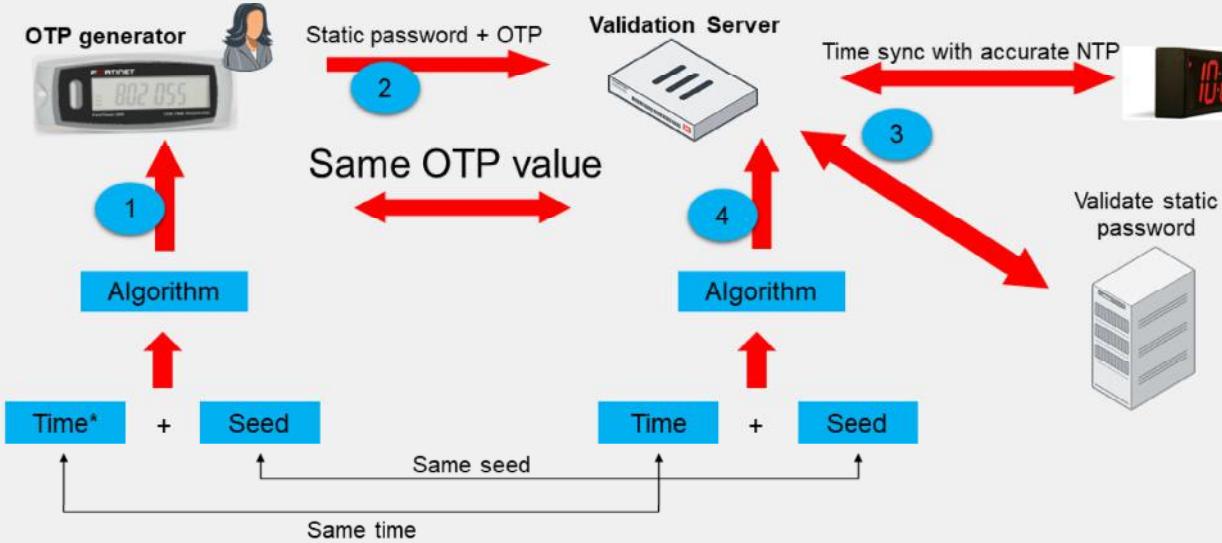
You can use one-time passwords (OTPs) as your second factor. OTPs are more secure than static passwords because the passcode changes at regular intervals and is valid for only a short amount of time. Once you use the OTP, you can't use it again. So, even if it is intercepted, it is useless. FortiGate 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 accept the authorization request from their FortiToken mobile app, without the need to enter an additional code.

DO NOT REPRINT

© FORTINET

FortiTokens



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

16

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 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 FortiGate, or link it to an NTP server (which is recommended).

DO NOT REPRINT
© FORTINET

Assigning a FortiToken to a User

User & Authentication > FortiTokens

The screenshot shows the FortiAuthenticator interface. At the top, there's a toolbar with 'Create New', 'Edit', 'Delete', 'Activate', 'Provision', 'Refresh', and 'Search' buttons. Below is a table with columns: Type, Serial Number, Status, User, Drift, and Comments. Two rows are listed: 'Mobile Token' with serial FTKMOB781E57E34F and status 'Available', and another 'Mobile Token' with serial FTKMOB783867923E and status 'Available'. Below the table are two modal windows: 'New FortiToken' and 'New FortiAuthenticator'. The 'New FortiToken' window has 'Mobile Token' selected and an 'Activation Code' field with '0000-0000-0000-0000-0000'. The 'New FortiAuthenticator' window shows a user 'student' with 'Enabled' status, 'Local User' type, 'Remote-users' group, and 'Two-factor Authentication' selected. It also lists 'FortiToken' and 'FortiToken Cloud' as authentication types, with 'FTKMOB6B91B33BES' as the token.

Two free FortiToken Mobile activations

- Enable **Two-factor Authentication** and select the registered FortiToken

Can add a user to a group and create a firewall policy based on the user group

You can add a FortiToken 200 or FortiToken Mobile to FortiGate on the **FortiTokens** page.

A hard token has a serial number that provides 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.

A soft token requires an activation code. Note that each FortiGate (and FortiGate VM) provides two free FortiToken Mobile activations. You must purchase any additional tokens 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.

After you have registered the FortiToken devices 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**. On 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.

18

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. 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.

3. 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

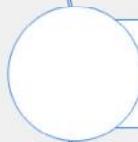
DO NOT REPRINT

© FORTINET

Lesson Progress



Methods of Firewall Authentication



User Groups



Authentication Using Firewall Policies

Good job! You now understand the basics of firewall authentication.

Now, you will learn about user groups.

DO NOT REPRINT

© FORTINET

User Groups

Objectives

- Configure user groups

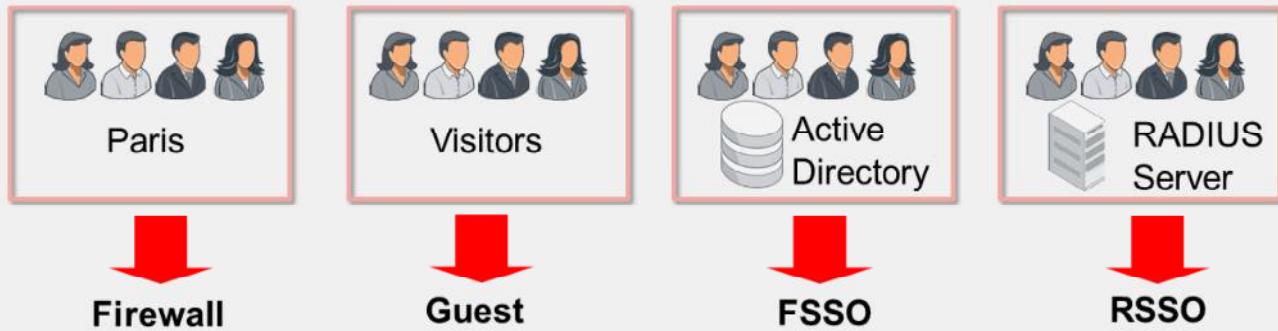
After completing this section, you should be able to achieve the objective shown on this slide.

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

FortiGate allows administrators to assign users to groups. Usually, 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: Guest (highlighted in red)

Batch Guest Account Creation:

User ID: Email Auto Generated Specify

Maximum Accounts:

Guest Details:

- Enable Name:**
- Enable Email:**
- Enable SMS:**
- Password:** Auto Generated Specify
- Sponsor:** Optional Required
- Company:** Optional Required

Expiration:

Start Countdown: On Account Creation After First Login

Time: Days: 0 Hours: 4 Minutes: 0 Seconds: 0

Account expiry

© Fortinet Inc. All Rights Reserved.

FORTINET
 Training Institute

23

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 who have access only to create and manage guest user accounts.

DO NOT REPRINT
© FORTINET

Configuring User Groups

User & Authentication > User Groups

Name: Training-users
 Type: Firewall
 Members: +
 Remote Groups:

Remote Server	Group Name
External_Server	cn=AD_users,ou=Training,dc=trainingAD,dc=training,dc=...

Add members to group (local or PKI peer)

Can add preconfigured remote servers to the group

Select Entries

USER (2)

Local (2)

guest

student

Can select specific LDAP groups as defined on the LDAP server

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, you require different configurations. 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 purposes?
 A. To provide temporary visitor access to corporate network resources
 B. To provide temporary visitor access to wireless networks

DO NOT REPRINT

© FORTINET

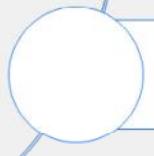
Lesson Progress



Methods of Firewall Authentication



User Groups



Authentication Using Firewall Policies

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
- Monitor firewall users

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

By demonstrating competence in 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

Policies & Objects > Firewall Policy

Source	
Full_Access	port3
port1	
LOCAL_SUBNET	
External-Server-Users	
Destination	
all	
Schedule	
always	
Service	
ALL	
Action	
<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	

Select Entries

Address User Internet Service

Q Search + Create

USER (2)

Local (2)

guest

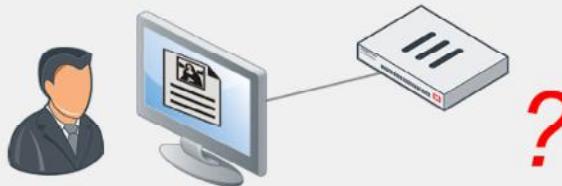
student

USER GROUP (3)

External-Server-Users

Guest-group

SSO_Guest_Users



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

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 before 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, before 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 listed above



© Fortinet Inc. All Rights Reserved.

30

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

port5 → port1									
Sequence	User	Source	Action	AV	SSL	Auth	Condition	Action	Enabled
17	Guest	LOCAL_SUBNET	all	Guest_AV	certificate-inspection		always	ALL	ACCEPT Enabled
18	Contractor	LOCAL_SUBNET	all	Contractor_AV	certificate-inspection		always	ALL	ACCEPT Enabled
19	Other	LOCAL_SUBNET	all	default	certificate-inspection		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 does not prompt the user for login credentials when it can identify the user passively
 - By default, active authentication is intended to be used as a backup when passive authentication fails

In the example shown on this slide, assuming active authentication is used, any initial traffic from LOCAL_SUBNET will not match policy sequence 17 (Guest). Policy sequence 17 looks for both IP and user, and user group information (LOCAL_SUBNET and Guest-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 18 to see if the traffic matches. It will not for the same reason it did not match 17.

Finally, FortiGate evaluates policy sequence 19 to see if the traffic matches. It matches all criteria, so traffic is allowed with no need to authenticate.

When you use only active authentication, 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 19 also had authentication enabled, the users would receive login prompts.

If you use passive authentication and it can successfully obtain user details, then traffic from LOCAL_SUBNET with users that belong to Guest-group will apply to policy sequence 17, even though policy sequence 19 does not have authentication enabled.

If you use both active and passive authentication, and FortiGate can identify a user's credentials through passive authentication, the user never receives 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 identify who the user is passively. When you combine active and passive authentication methods, active authentication is

DO NOT REPRINT

© FORTINET

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 are not 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
 - You must place passive authentication policies on top of active authentication policy
- Enable a captive portal on the ingress interface for the traffic:
 - Authentication happens at an interface level
 - Traffic is not allowed without valid authentication unless it matches an exemption
 - All users are prompted for authentication before they can access any resource

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 are not asked to authenticate. By default, all traffic passes 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 must authenticate before traffic is placed on the egress interface.

Alternatively, only on the CLI, you can change the auth-on-demand option to always. This instructs FortiGate to trigger an authentication request, if there is a firewall policy with active authentication enabled. In this case, the traffic is allowed until authentication is successful.

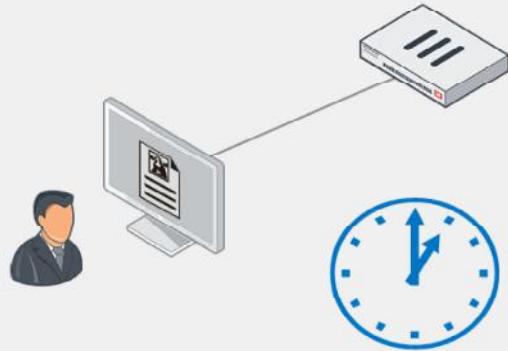
If you want to have all users connect to a specific interface, then it is better to enable captive portal authentication at the interface level. This way, all devices must authenticate before they are allowed to access any resources.

DO NOT REPRINT**© FORTINET**

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 five 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



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 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

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 9 second(s)	10.43 kB	Firewall

Confirm

⚠ Are you sure you want to deauthenticate the selected user(s)?

OK Cancel

© Fortinet Inc. All Rights Reserved. 34

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, at the same time.

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.
3. 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

DO NOT REPRINT

© FORTINET

Lesson Progress



Methods of Firewall Authentication



User Groups



Authentication Using Firewall Policies

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

36

Congratulations! You have completed this 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 and firewall policies
- ✓ Monitor firewall users



© Fortinet Inc. All Rights Reserved.

37

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

By mastering the objectives covered in this lesson, you learned how to use authentication on the firewall policies of FortiGate.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Security

Logging and Monitoring

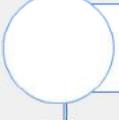
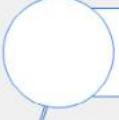
FortiOS 7.2

Last Modified: 13 June 2022

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

**Log Basics****Local and Remote Logging****Log Settings and Log Search****Protect Log Data**

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.

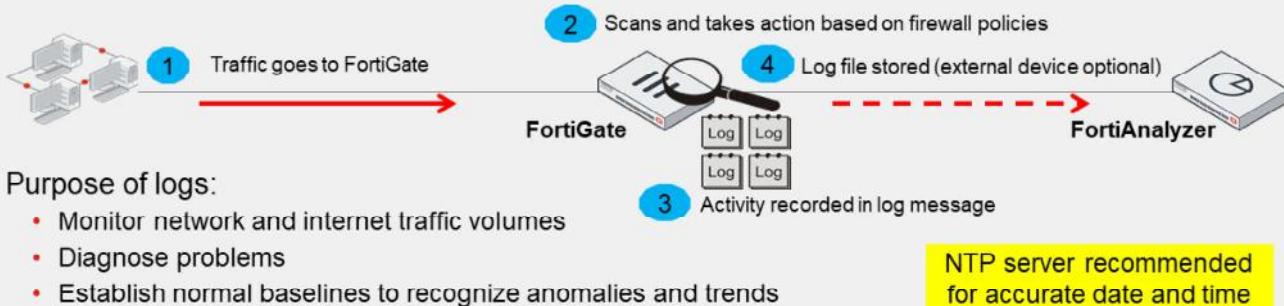
By demonstrating competence in log basics, you will be able to more effectively analyze log data from your database.

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)



- Purpose of logs:
 - Monitor network and internet traffic volumes
 - Diagnose problems
 - Establish normal baselines to recognize anomalies and trends

NTP server recommended
for accurate date and time

FORTINET
Training Institute

© 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 adjust your network security settings 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)

Traffic	Event	Security
Forward	Endpoint	Application Control
Local	High Availability	Antivirus
Sniffer	General System	DNS Query
	User	File Filter
	Router	Web Filter
	VPN	Intrusion Prevention
	SD-WAN	Anomaly
	WiFi	SSL
	CIFS	SSH
	Security Ratings	
	SDN Connector	

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 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 the subtypes listed on the slide.

- System event logs contain information related to operations, such as automatic FortiGuard updates and GUI logins.
- User logs contain login and logout events for firewall policies with user authentication.
- Router, VPN, 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 the subtype listed on the slide.

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

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 that includes 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=2022-03-14 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=52.84.14.233 dstport=80 dstintf="port1" proto=6 service="HTTP"
hostname="miniclip.com" profile="default" action=blocked reqtype=direct
url="/lavicon.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
```

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 the 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**

Effect of Logging on Performance

- More logs = more CPU, memory, and disk space used
- 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
```

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 the logging behavior with security profiles. Security profiles can, depending on the logging settings, create log events when a traffic matching the profile is detected. Depending on the amount of traffic you have, and the logging settings that are enabled, your traffic logs can swell and, ultimately, impact the performance of your firewall.

When using remote logging devices, such as FortiAnalyzer and syslog, you can enable performance statistic logging to occur every 1-15 minutes (0 to disable). This is not available for local disk logging or FortiCloud.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which type of logs are application control, web filter, and antivirus?
 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

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Log Basics****Local and 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 and Remote Logging

Objectives

- Identify log storage options
- Enable local and remote logging
- Understand disk allocation and reserved space
- 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 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

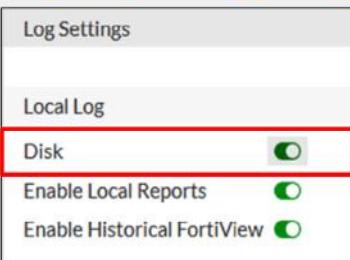
Log Storage—Local

- To store logs locally on FortiGate, you must enable disk logging


```
# config log disk setting
      set status enable
```
- If disk logging is 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



- FortiGate devices that have a hard drive store logs in an SQL database
- Data is extracted from the SQL database for reports



Hard drive

Performance may be impacted under heavy strain

Typically, mid-level to high-end FortiGate models have a hard drive. FortiGate can store logs on its hard drive. This operation is known as local logging or disk logging. Depending on the model series, disk logging may be enabled by default.

FortiGate 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, disk logging 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. If your device has two separate disks, you can use one for WAN optimization and the other for logging. If you are using the local hard disk for WAN optimization, and only one disk is available, you can log to remote FortiAnalyzer devices or syslog servers.

If you want to store logs locally on FortiGate, you must enable disk logging on the **Log Settings** page. Only some FortiGate models support disk logging. If your FortiGate does not support disk logging, you can log to an external device instead.

You must enable disk logging 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 days are deleted from the disk. This value 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%)

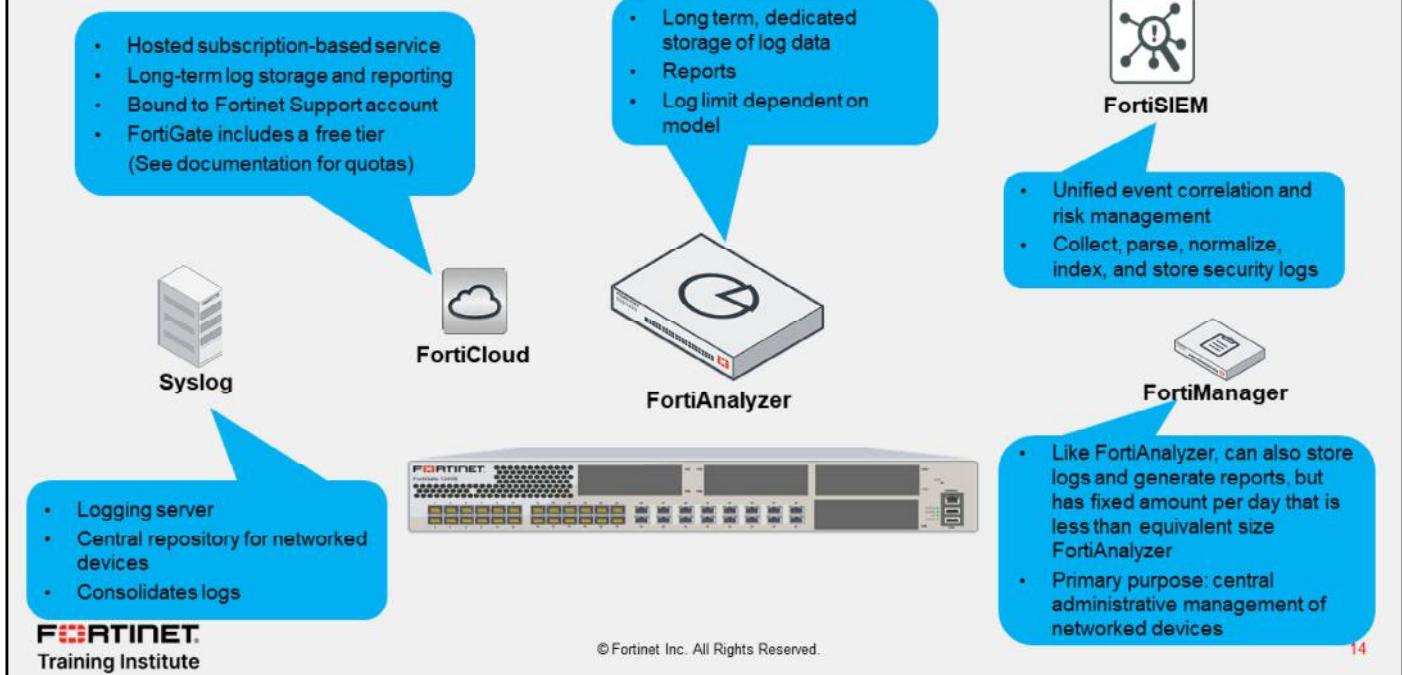
If you decide to log locally on FortiGate, be aware that the entire disk space is not available to store logs. The FortiGate system reserves approximately 25% of its disk space for system usage and unexpected quota overflow.

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

Log Storage—Remote



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. Whenever possible, it is preferred to store logs externally.

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 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)



- Can configure up to three separate FortiAnalyzer and FortiManager devices or one cloud FortiAnalyzer instance using the CLI
 - Multiple devices may be needed for redundancy
 - Generating and sending logs requires resources—be aware!

Log & Report > Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager Disabled

IP address: 10.0.1.210

Connection status: Connected

Storage usage: 56.07 MiB / 1000.00 MiB

Analytics usage: 20.82 MiB / 700.00 MiB

Archive usage: 35.25 MiB / 300.00 MiB

Upload option: Real Time | Every Minute | Every 5 Minutes

Allow access to FortiGate REST API:

Verify FortiAnalyzer certificate: FAZ-VM0000065040

```
# config log [fortianalyzer | fortianalyzer-cloud|fortianalyzer2|fortianalyzer3] setting
  set status enable
  set server <server_IP>
end
```

Commands **not** cumulative

The process to configure FortiGate to send logs to FortiAnalyzer or FortiManager is identical. For FortiGate to send logs to either device, you must register FortiGate with FortiAnalyzer or FortiManager. After it is registered, 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 CLI.

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.

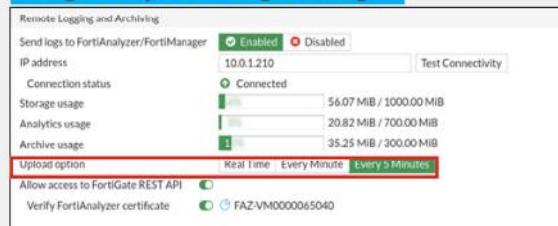
DO NOT REPRINT

© 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



```
# configure log fortianalyzer setting
  set upload-option [store-and-upload |realtime/1-minute/5-minute]
```

- By default, if the FortiAnalyzer disk is full, the oldest logs are overwritten; however, you can configure FortiAnalyzer to stop logging

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.

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=0, alert=0, alarm=0, sys=0, faz=19, faz-cloud=0, webt=0, fds=0
interface-missed=0
Queues in all miglogds: cur:0 total-so-far:153
global log dev statistics:
faz 0: sent=15, failed=0, cached=0, dropped=0, relayed=0

Local-FortiGate # diagnose log kernel-stats

fgtlog: 1
fgtlog 0: total-log=32, failed-log=0 log-in-queue=0
```

Current cache size and total cache size

If there are bursts or link is overloaded, failed increases

If queue is full, failed-log value increases

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, FortiGate can 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

FortiGate Cloud

Status: Not Activated

Cloud Logging Settings

Type: FortiGate Cloud

Activate FortiGate Cloud account first

```
# 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

Syslog and FortiSIEM

Log & Report > Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager: Enabled

Send logs to syslog: Enabled

IP Address/FQDN

```
# config log [syslogd | syslogd2 | syslogd3 | syslogd4] setting
  set status enable
  set server <syslog_IP>
end
```

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
```

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, which is 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. The 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 FortiAnalyzer 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
```

If you have a FortiGate with virtual domains (VDOMs) configured, you can globally add multiple FortiAnalyzer and syslog servers. You can configure up to three FortiAnalyzer devices and up to four syslog servers under global settings.

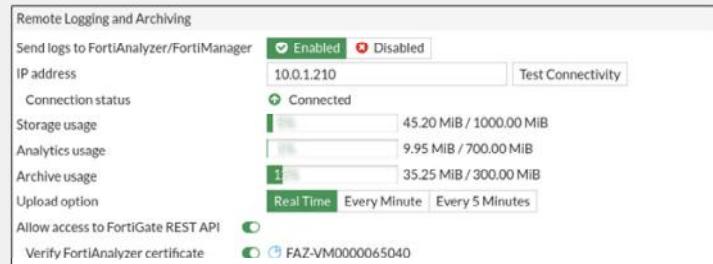
DO NOT REPRINT

© FORTINET

Log Transmission

- FortiGate uses UDP 514 for log transmission by default

```
config log fortianalyzer setting
  set status enable
  set server "10.0.1.210"
  set serial "FAZ-VM0000065040"
  set enc-algorithm high-medium
  set upload-option realtime
end
```



- 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

FortiGate uses UDP port 514 for log transmission by default .

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 and OFTPS

- Changes the log transport delivery method from UDP to TCP
- TCP provides reliable data transfer
- 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 it using the CLI command shown in the screenshot below
- FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (default setting is high)
- 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
```

When you enable reliable logging on FortiGate, the log transport delivery method changes from User Datagram Protocol (UDP) to Transmission Control Protocol (TCP). TCP provides reliable data transfer, guaranteeing that the transferred data 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 encryption setting is high.

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 choose the level of SSL protection used by configuring the `enc-algorithm` setting on the CLI.

When both FortiGate and FortiAnalyzer are running version 7.2 or later, and reliable logging is configured, FortiGate keeps logs in a *confirm queue* until it verifies those logs were received by FortiAnalyzer. This is achieved by using sequence numbers (`seq_no`) to track the logs received. FortiOS periodically queries FortiAnalyzer for the latest `seq_no` of the last log received, and clears logs from the *confirm queue* up to the `seq_no`.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which storage type is preferred for logging?
 A. Remote logging
 B. Hard drive

2. Which 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

DO NOT REPRINT

© FORTINET

Lesson Progress



Log Basics



Local and Remote Logging



Log Settings and Log Search



Protect Log Data

Good job! You now understand remote logging.

Now, you will learn about log settings.

DO NOT REPRINT**© FORTINET**

Log Settings and Log Search

Objectives

- Configure log settings
- Enable logging on firewall policies
- Hide user names in logs
- View and search for log messages
- 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 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 Settings: If, Where, and How

Log & Report > Log Settings

Local Log

- Disk
- Enable Local Reports
- Enable Historical FortiView

Event Logging

<input checked="" type="checkbox"/> All <input type="button" value="Customize"/>	<input checked="" type="checkbox"/> Local Traffic Log <input type="button" value="Customize"/>
<input type="checkbox"/> Log Allowed Traffic <input type="checkbox"/> Log Denied Unicast Traffic	
<input type="checkbox"/> Log Local Out Traffic <input type="checkbox"/> Log Denied Broadcast Traffic	

GUI Preferences

- Resolve Hostnames
- Resolve Unknown Applications

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IP address	10.0.1.210 <input type="button" value="Test Connectivity"/>
Connection status	Connected
Storage usage	45.20 MB / 1000.00 MB
Analytics usage	9.95 MB / 700.00 MB
Archive usage	35.25 MB / 300.00 MB
Upload option	Real Time Every Minute Every 5 Minutes
Allow access to FortiGate REST API <input checked="" type="checkbox"/>	
Verify FortiAnalyzer certificate <input checked="" type="checkbox"/> FAZ-VM0000065040	

- 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

- Translate IPs to host names for convenience? (Can impact CPU usage and page responsiveness.)

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

25

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. 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. 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.

FortiGate Security 7.2 Study Guide

196

DO NOT REPRINT

© FORTINET

Log Filtering

- 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 or FortiManager devices or one cloud FortiAnalyzer instance:

```
# config log [fortianalyzer | fortianalyzer-cloud | 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]
- ZTNA-traffic [enable/disable]
- GTP [enable/disable]
- Filter [string]
- Filter type [include | exclude]



© Fortinet Inc. All Rights Reserved.

26

While you use the log settings on the GUI to configure which event logs and local traffic logs to capture, you can set more granular options using the CLI.

You can configure FortiGate to send logs to external servers. You can control which 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 or FortiManager 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`.

For example, the following commands configure the log filter for the first syslog server to include only logs related to traffic directly to and from the FortiGate management IP addresses, with a severity level of *critical* or higher:

```
#config log syslogd filter
#(filter) set severity critical
#(filter) set local-traffic enable
```

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
- Hardware acceleration affects logging**
 - Traffic offloaded to NP6 and NP6Lite processors does not log traffic statistics.
 - Traffic offloaded to NP7 processors have improved logging of traffic statistics capabilities
 - Can disable hardware acceleration
 - Can enable NP packet logging (degrades NP performance)

Must enable one or more security profiles on your firewall policy to generate a log message for that profile

Policy & Objects > Firewall Policy

Must enable and set which traffic to log. If disabled, you will not receive logs of any kind—even if you have enabled a security profile on your firewall policy.

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 are also enabled, security log events appear in the forward traffic log and security log.

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=2021-03-16 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"
```

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

Viewing and Searching Log Messages—GUI

Log & Report

Forward Traffic

Date/Time % Source Device Destination

Local Traffic 2 minutes ago 10.0.1.20 94.102.51.124

Sniffer Traffic 2 minutes ago 10.0.1.20 139.99.113.97 (homeschoolingpena.com)

System Events 3 minutes ago 10.0.1.20 34.102.136.180 (taxtube.com)

Security Events 3 minutes ago 10.0.1.20 87.247.245.130 (www.oxtown.net)

Log Settings 3 minutes ago 10.0.1.20 35.208.12.102 (jowriter.com)

Threat Weight 3 minutes ago 10.0.1.20 31.170.1.86 (www.drvnlnclusmaykeh.com)

3 minutes ago 10.0.1.20 172.67.25.155 (cpanel.cow.stackit.net)

Set log filters to narrow search

Log location = disk

Application Name Disk Result

Log Details

Details Security

General

Absolute Date/Time 2022/01/04 11:55:52

Time 11:55:52

Duration 1s

Session ID 3524

Virtual Domain root

NAT Translation Source

Source

IP 10.0.1.20

NAT IP 10.200.1.1

Source Port 55362

Country/Region Reserved

Source Interface port3

User

Destination

IP 34.102.136.180

Port 80

Country/Region United States

Destination Interface port1

Application Control

© Fortinet Inc. All Rights Reserved.

29

You can access your logs on the GUI in the **Log & Report** menu.

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 it 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 in 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.

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 in the drop-down list that appears. If you see data that you want to filter on in a log that is already in the table, 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 opens, allowing you to filter on all logs with that botnet name.

By default, the most common columns are shown and less common columns are hidden. To add columns, right-click any column field and, in the pop-up menu that opens, select the column in the **Available Columns** section.

DO NOT REPRINT
© FORTINET

Viewing Logs Associated With a Firewall Policy

- Access log messages generated by individual policies

Policy & Objects > Firewall Policy

Create New		Edit	Delete	Policy Lookup	Search	<input type="text"/>	Interface Pair View	By Sequence																																																				
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes																																																			
P3_to_P1	LOCAL_SUBNET	<input type="checkbox"/> all	<input type="checkbox"/> always	<input type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	wta default	<input checked="" type="checkbox"/> All	8.47 MB																																																			
<div style="border: 1px solid #ccc; padding: 5px;"> Policy Set Status Filter by Name Copy Paste Insert Empty Policy Show Matching Logs Show in FortiView Edit Edit in CLI Delete Policy </div>																																																												
<table border="1"> <thead> <tr> <th colspan="2">Policy UUID: b11ac58c-791b-51e7-4600-12fb29a687d9</th> <th>Add Filter</th> </tr> <tr> <th>Date/Time</th> <th>%</th> <th>Source</th> <th>Device</th> <th>Destination</th> <th>Application Name</th> <th>Result</th> <th>Policy</th> </tr> </thead> <tbody> <tr> <td>2 minutes ago</td> <td></td> <td>10.0.1.10</td> <td></td> <td>8.8.8.8 (dns.google)</td> <td></td> <td><input checked="" type="checkbox"/> 69 B / 165 B</td> <td>P3_to_P1 (1)</td> </tr> <tr> <td>3 minutes ago</td> <td></td> <td>10.0.1.10</td> <td></td> <td>8.8.8.8 (dns.google)</td> <td></td> <td><input checked="" type="checkbox"/> 138 B / 370 B</td> <td>P3_to_P1 (1)</td> </tr> <tr> <td>3 minutes ago</td> <td></td> <td>10.0.1.10</td> <td></td> <td>184.24.144.126 (data.cnn.com)</td> <td></td> <td><input checked="" type="checkbox"/> 2.06 KB / 4.49 KB</td> <td>P3_to_P1 (1)</td> </tr> <tr> <td>3 minutes ago</td> <td></td> <td>10.0.1.10</td> <td></td> <td>34.213.37.14 (push.services.mozilla.com)</td> <td></td> <td><input checked="" type="checkbox"/> 69 B / 165 B</td> <td>P3_to_P1 (1)</td> </tr> <tr> <td>3 minutes ago</td> <td></td> <td>10.0.1.10</td> <td></td> <td>8.8.8.8 (dns.google)</td> <td></td> <td><input checked="" type="checkbox"/> 138 B / 370 B</td> <td>P3_to_P1 (1)</td> </tr> </tbody> </table>										Policy UUID: b11ac58c-791b-51e7-4600-12fb29a687d9		Add Filter	Date/Time	%	Source	Device	Destination	Application Name	Result	Policy	2 minutes ago		10.0.1.10		8.8.8.8 (dns.google)		<input checked="" type="checkbox"/> 69 B / 165 B	P3_to_P1 (1)	3 minutes ago		10.0.1.10		8.8.8.8 (dns.google)		<input checked="" type="checkbox"/> 138 B / 370 B	P3_to_P1 (1)	3 minutes ago		10.0.1.10		184.24.144.126 (data.cnn.com)		<input checked="" type="checkbox"/> 2.06 KB / 4.49 KB	P3_to_P1 (1)	3 minutes ago		10.0.1.10		34.213.37.14 (push.services.mozilla.com)		<input checked="" type="checkbox"/> 69 B / 165 B	P3_to_P1 (1)	3 minutes ago		10.0.1.10		8.8.8.8 (dns.google)		<input checked="" type="checkbox"/> 138 B / 370 B	P3_to_P1 (1)
Policy UUID: b11ac58c-791b-51e7-4600-12fb29a687d9		Add Filter																																																										
Date/Time	%	Source	Device	Destination	Application Name	Result	Policy																																																					
2 minutes ago		10.0.1.10		8.8.8.8 (dns.google)		<input checked="" type="checkbox"/> 69 B / 165 B	P3_to_P1 (1)																																																					
3 minutes ago		10.0.1.10		8.8.8.8 (dns.google)		<input checked="" type="checkbox"/> 138 B / 370 B	P3_to_P1 (1)																																																					
3 minutes ago		10.0.1.10		184.24.144.126 (data.cnn.com)		<input checked="" type="checkbox"/> 2.06 KB / 4.49 KB	P3_to_P1 (1)																																																					
3 minutes ago		10.0.1.10		34.213.37.14 (push.services.mozilla.com)		<input checked="" type="checkbox"/> 69 B / 165 B	P3_to_P1 (1)																																																					
3 minutes ago		10.0.1.10		8.8.8.8 (dns.google)		<input checked="" type="checkbox"/> 138 B / 370 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 and Searching 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
40 logs found.
10 logs returned.

1: date=2021-04-13 time=08:45:49 eventtime=1618328749810305885 tz="-0700" logid="0000000020" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.0.1.10 srcport=40570 srcintf="port3" srcintfrole="undefined"
dstip=74.6.143.25 dstport=443 dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="United
States" sessionid=4201 proto=6 action="accept" policyid=1 policytype="policy" poluid="b11ac58c-791b-51e7-4600-
12f829a689d9" policyname="Full Access" service="HTTPS" trandisp="snat" transip=10.200.1.10 transport=40570
duration=153 sentbyte=6623 rcvdbyte=23201 sentpkt=40 rcvdpkt=40 appcat="unscanned" sentdelta=6623 rcvddelta=23201

2: date=2021-04-13 time=08:45:46 eventtime=1618328746107660006 tz="-0700" logid="0000000020" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.0.1.10 srcport=35908 srcintf="port3" srcintfrole="undefined"
dstip=54.243.191.211 dstport=443 dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="United
States" sessionid=4255 proto=6 action="accept" policyid=1 policytype="policy" poluid="b11ac58c-791b-51e7-4600-
12f829a689d9" policyname="Full Access" service="HTTPS" trandisp="snat" transip=10.200.1.10 transport=35908
duration=147 sentbyte=2932 rcvdbyte=8084 sentpkt=23 rcvdpkt=19 appcat="unscanned" sentdelta=2932 rcvddelta=8084
```

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

```
# config alertemail setting
  set username "fortigate@training.lab"
  set mailto "admin@training.lab"
  set filter-mode category | threshold
  set email-interval 1
  set IPS-logs enable
  set HA-logs enable
  set antivirus-logs enable
  set webfilter-logs enable
  set log-disk-usage-warning enable
end
```

System > Settings

Email Service <small>i</small>	Use custom settings <input checked="" type="checkbox"/>
SMTP Server	Default <input type="button" value="Specify"/> 10.200.1.254
Port <small>i</small>	Use default (25) <input type="button" value="Specify"/>
Authentication	<input checked="" type="checkbox"/>
Security Mode	None <input type="button" value="SMTPS"/> STARTTLS
Default Reply To	admin@training.lab

Configure up to three recipients

Send alert by category or threshold

Set how often to send alert

Because 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 using the CLI. 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

Threat Weight Definition				
Log Threat Weight				Reset
Application Protection				
P2P	Low	Medium	High	Critical
Proxy	Low	Medium	High	Critical
Intrusion Prevention Detection Severity				
Informational	Off	Low	Medium	High
Low	Off	Low	Medium	High
Medium	Off	Low	Medium	High
High	Off	Low	Medium	High
Critical	Off	Low	Medium	High
Botnet Communication	Off	Low	Medium	High
Malware Detection				
Virus Detected	Off	Low	Medium	High
FortiNDR Virus Detected	Off	Low	Medium	High
FortiSandbox Virus Detected	Off	Low	Medium	High
File Blocked	Off	Low	Medium	High
Blocked Command	Off	Low	Medium	High
Oversized File	Off	Low	Medium	High
Virus Scan Error	Off	Low	Medium	High
Switch Protocol	Off	Low	Medium	High
MIME Fragmented	Off	Low	Medium	High
Virus File Type Executable	Off	Low	Medium	High
Virus Outbreak Prevention Event	Off	Low	Medium	High
Content Disarm	Off	Low	Medium	High
Malware List	Off	Low	Medium	High
EMS Threat Feed	Off	Low	Medium	High
FortiSandbox Malicious	Off	Low	Medium	High
FortiSandbox High Risk	Off	Low	Medium	High
FortiSandbox Medium Risk	Off	Low	Medium	High
Packet Based Inspection				
Blocked Connection	Off	Low	Medium	High
Failed Connection	Off	Low	Medium	High
Web Activity				
Blocked URLs	Off	Low	Medium	High
Malicious Websites	Off	Low	Medium	High
Phishing	Low	Medium	High	Critical
Spam URLs	Low	Medium	High	Critical
Drug Abuse	Low	Medium	High	Critical
Hacking	Low	Medium	High	Critical
Illegal or Unethical	Low	Medium	High	Critical
Discrimination	Low	Medium	High	Critical
Explicit Violence	Low	Medium	High	Critical
Extremist Groups	Low	Medium	High	Critical
Proxy Avoidance	Low	Medium	High	Critical
Plagiarism	Low	Medium	High	Critical
Child Sexual Abuse	Low	Medium	High	Critical
Peer-to-peer File Sharing	Low	Medium	High	Critical
Pornography	Low	Medium	High	Critical
Terrorism	Low	Medium	High	Critical

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 based on their 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. In your firewall policy, which setting must you enable to generate logs on traffic sent through that firewall policy?
 A. Log Allowed Traffic
 B. Event Logging

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

**Log Basics****Local and Remote Logging****Log Settings and Log Search****Protect Log Data**

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 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 allogs [ftp | tftp | usb]
```

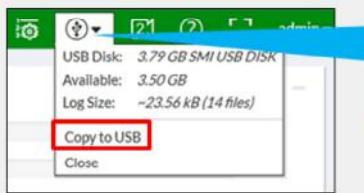
- Export specific log type to **FTP, TFTP, or USB** (stored as LZ4 compressed files)

```
# execute backup disk log [ftp | tftp | usb] <log_type>
```

- 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



Appears as an option on the GUI when you insert a USB drive into the FortiGate USB port

Date/Time	Source	Device
55 seconds ago	1.1.1.1	2.2.2.2
55 seconds ago	1.1.1.1	2.2.2.2
Minute ago	1.1.1.1	2.2.2.2
Minute ago	1.1.1.1	2.2.2.2
Minute ago	test user (172.16.78.32)	1.1.1.32
Minute ago	test user (172.16.78.32)	1.1.1.32
2 minutes ago	test user (172.16.78.32)	1.1.1.32
2 minutes ago	test user (172.16.78.88)	229.118.95.20
3 minutes ago	1.1.1.1	2.2.2.2
3 minutes ago	10.1.1.1	2.2.2.2

You can also protect your log data by performing log backups. A backup operation copies log files from the database to a specified location.

The `execute backup disk allogs` command backs up all logs to **FTP, TFTP, or USB**, while the `execute backup disk log <log type>` command backs up specific log types (such as **web filter** or **IPS**) to **FTP, TFTP, or USB**. These logs are stored in LZ4 format.

You can also use the GUI to back up logs to a USB drive, or to your computer disk. 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 downloads only the logs in the results table—not all logs on disk. As such, you can add log filters if you want to download only a subset of logs. When you download log messages from the GUI, you are downloading log messages in raw format.

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)

```
# config log disk setting
  set max-log-file-size <1-100>
  set roll-schedule [daily | weekly]
  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 uploadaddir [remote FTP dir]
  set uploadtype [log type]
  set upload-delete-files [enable* | disable]
```

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.

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

**Log Basics****Local and Remote Logging****Log Settings and Log Search****Protect Log Data**

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
- ✓ Describe the effect of logging on performance
- ✓ Identify log storage options
- ✓ Configure local and remote logging
- ✓ Understand disk allocation and reserved space
- ✓ 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
Training Institute



FortiGate Security

Certificate Operations

FortiOS 7.2

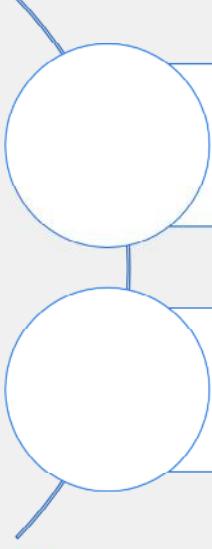
Last Modified: 23 August 2022

In this lesson, you will learn why FortiGate uses digital certificates and how to configure FortiGate to use certificates (including to inspect the contents of encrypted traffic).

DO NOT REPRINT

© FORTINET

Lesson Overview



Authenticate and Secure Data
Using Certificates

Inspect Encrypted Data

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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 be better able to judge 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 services
- **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 certificate authority (CA), can authenticate on FortiGate to access the network or to establish a VPN connection
 - Administrator 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 services, 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 CA can authenticate on FortiGate to access the network or to establish a VPN connection. Administrator 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 ...

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 Bloggs), 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 an 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 the following checks against a certificate before trusting it and using it:
 - Revocation check
 - You must download the relevant certificate revocation lists (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

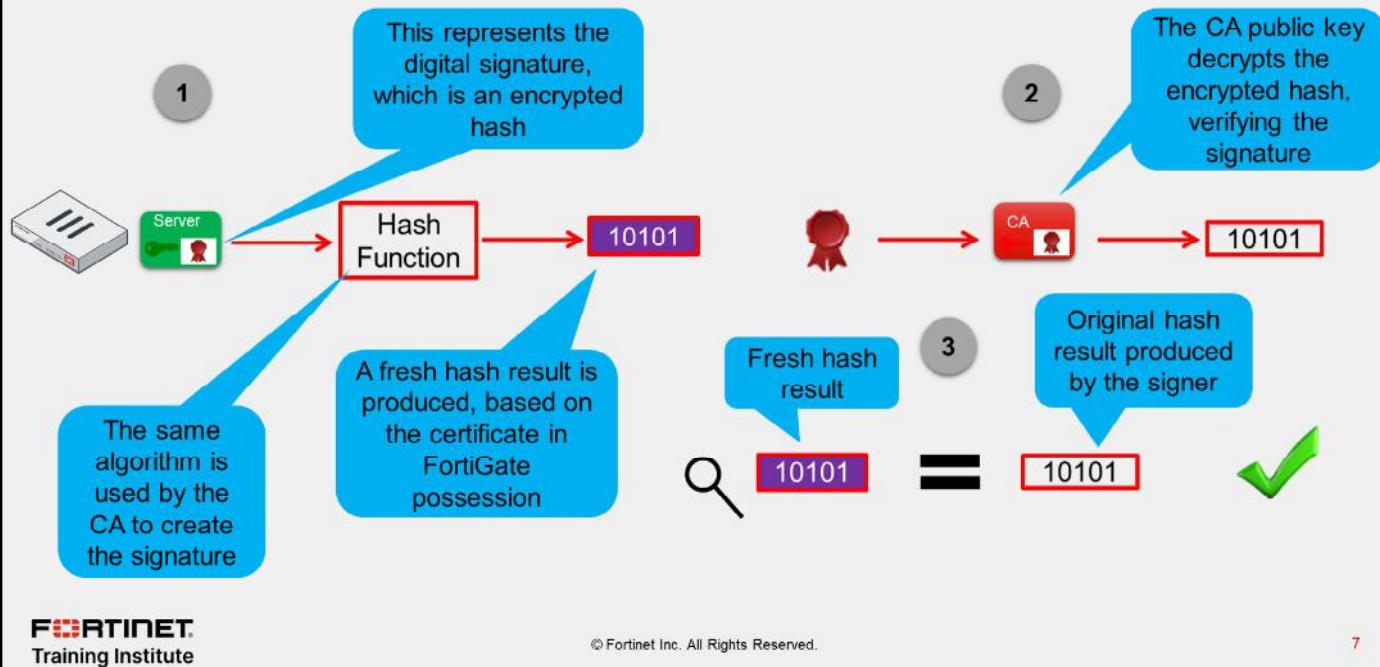
Field	Value
Version	V3
Serial number	7e 9b 8a 8d 00 00 00 00 00 00 6b
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	fortinet-us-FGT-NPS-CA, fort...
Valid from	Tuesday, September 06, 2016...
Valid to	Wednesday, September 06, 2...
Subject	Derrick MacLean, Training, Ottawa, ON, Canada
Public key	RSA (1024 Bits)
Certificate Template Name	EFS
Enhanced Key Usage	Encrypting File System (1.3.6.1.5.2.3.1.1)
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 ...

FortiGate runs the following checks before it trusts the certificate:

- Checks the 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 does 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



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

7

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 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 private key encrypting the hash result of the certificate
 - The user 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 public key, which allows the authentication server to decrypt and validate anything encrypted and signed by the CA private key



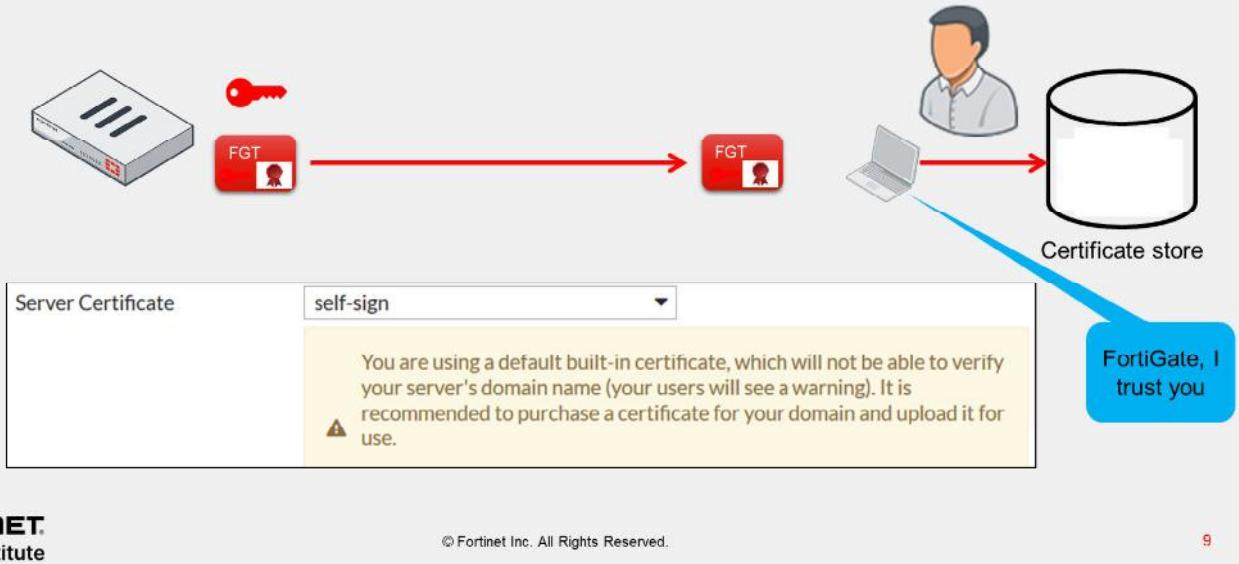
Certificate-based user authentication uses an end-entity certificate to identify the user. This certificate contains the user public key and the signature of the CA that issued the certificate. The authentication server (for example, FortiGate) must have the CA certificate whose private key signed the user certificate. FortiGate verifies that the certificate 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



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.

You can configure self-signed certificates 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 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 device.

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 public key to encrypt a string known as the premaster secret. The web server private key would decrypt the premaster secret

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 FortiGate can use it to identify one or both parties 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.

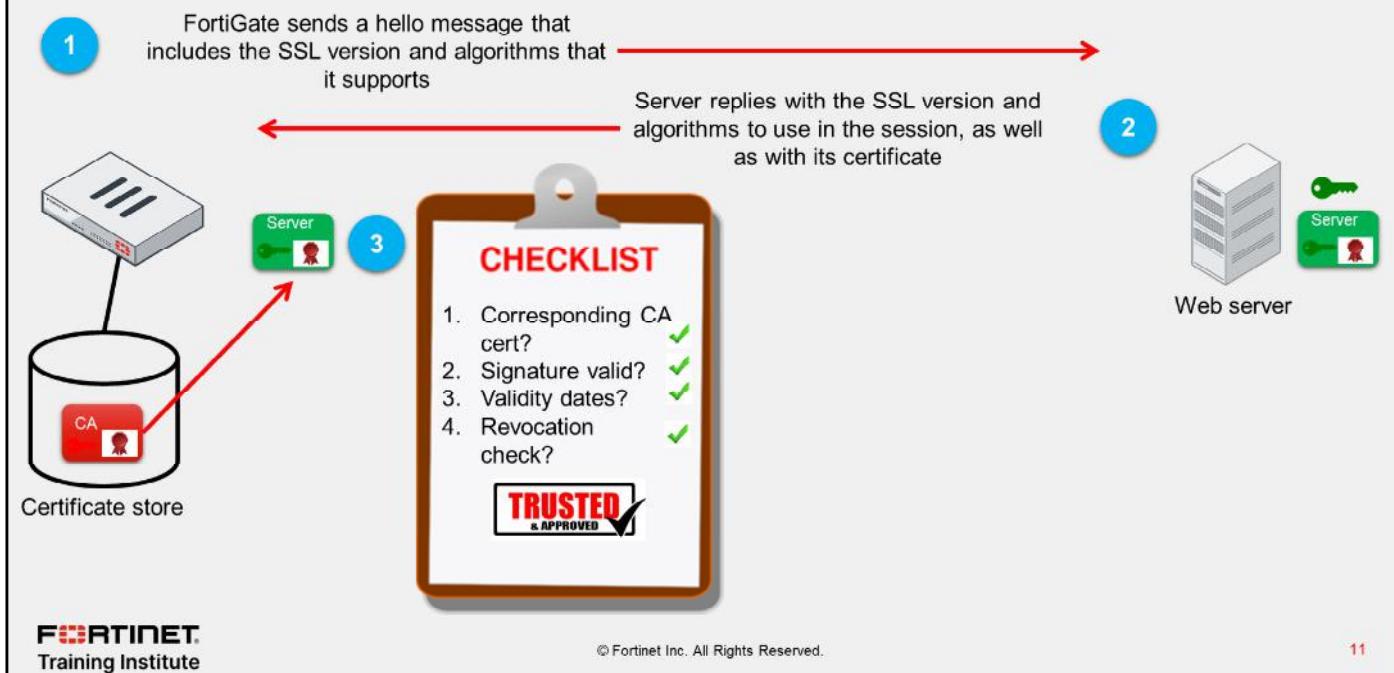
An important attribute of symmetric cryptography is that the same key is used to encrypt and decrypt data. When FortiGate establishes an SSL session between itself and another device it must share, the symmetric key (or rather the value required to produce it), so that data can be encrypted by one side, 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 public key to encrypt a string known as the premaster secret. The web server private key decrypts the premaster secret.

DO NOT REPRINT

© FORTINET

SSL Between FortiGate and a Web Server



Now, you will learn more about the process of establishing an SSL session.

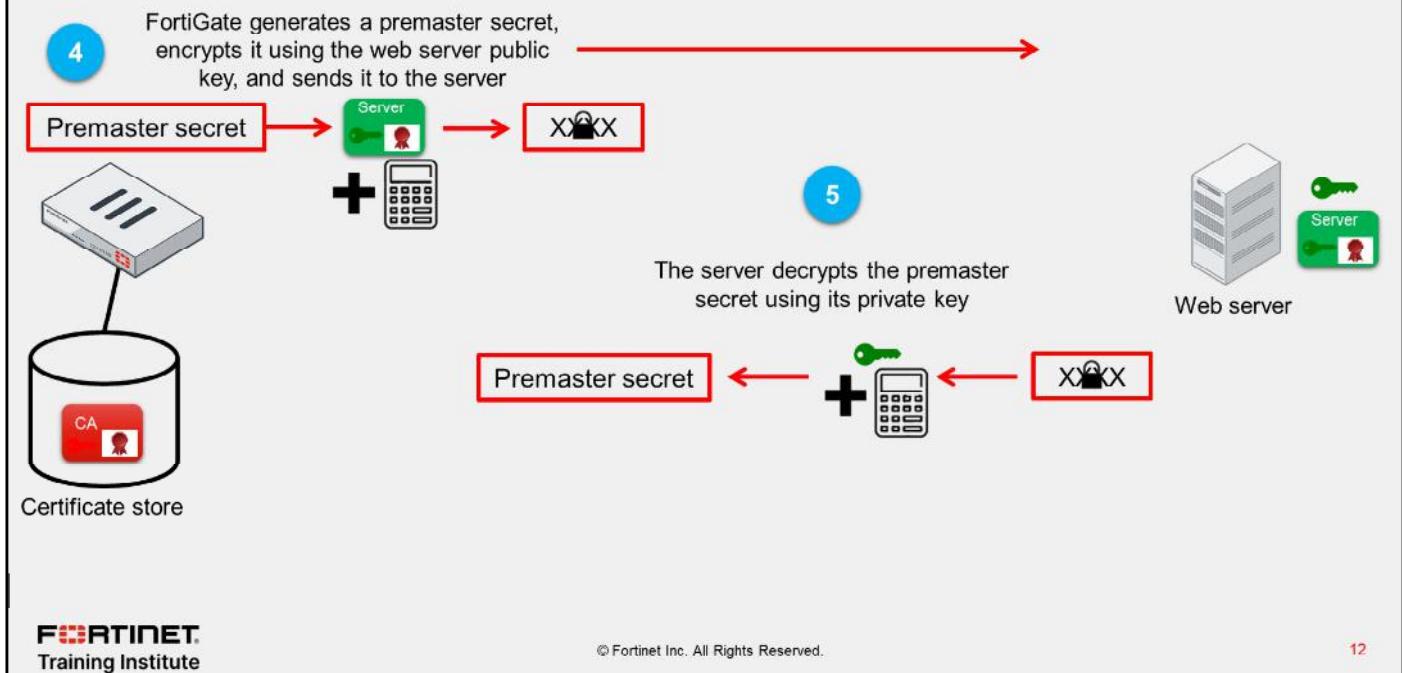
In the first step of the example shown on this slide, FortiGate connects to a web server that is configured for SSL. In the initial hello message, the browser provides critical information that is needed to communicate with the web server. This information includes the SSL version number and the names 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 included in the message, and verifies that it is also supported by the web server. The web server replies with the chosen SSL version and cipher suite, and then sends its certificate to FortiGate. Note that the certificate information is passed as cleartext 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 certificate. The checklist shown on this 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 (Contd)

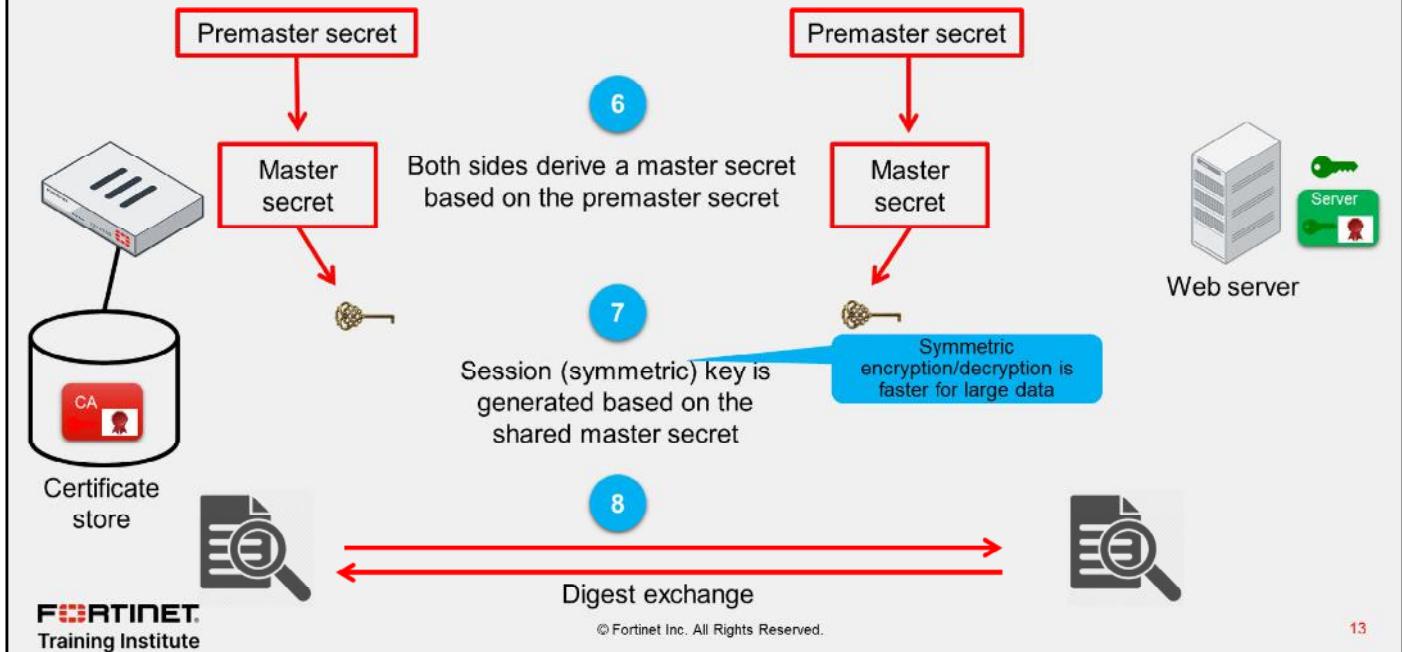


In the fourth step, FortiGate generates a value known as the premaster secret. FortiGate uses the server public key, which is in the certificate, to encrypt the premaster secret. FortiGate then sends the encrypted premaster secret to the web server. If a third-party intercepted the premaster secret, 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 premaster 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 (Contd)



In the sixth step, both FortiGate and the web server derive the master secret based on the premaster 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. The main advantage of symmetric key over asymmetric keys is that it is fast and efficient for large amounts of data. 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. Which attribute or extension identifies the owner of a certificate?
 A. The subject name in the certificate
 B. The unique serial number in the certificate

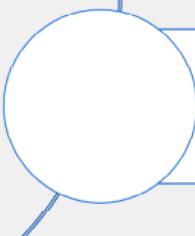
2. How does FortiGate determine if a certificate has been revoked?
 A. It checks the CRL that resides on FortiGate.
 B. It retrieves the CRL from a directory server.

DO NOT REPRINT**© FORTINET**

Lesson Progress



Authenticate and Secure Data Using Certificates



Inspect Encrypted Data

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

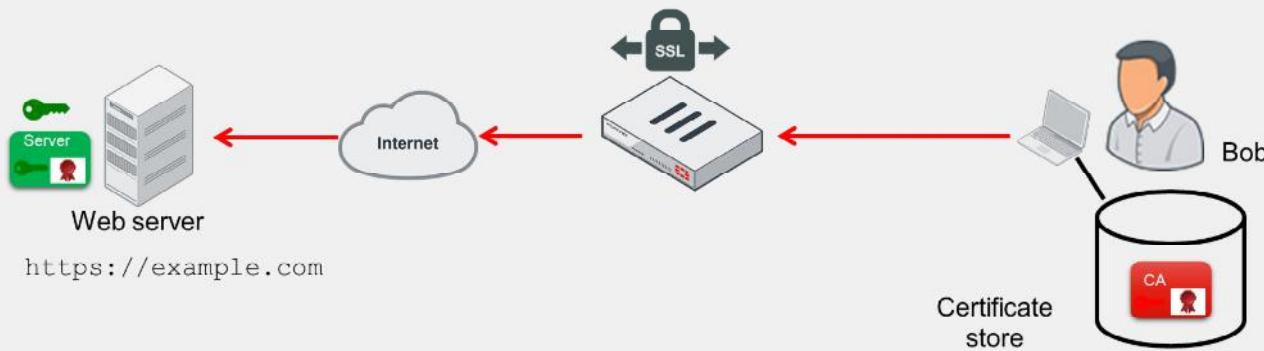
After completing this section, you should be able to achieve the objectives shown on this slide.

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 you enable full SSL inspection

*(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 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 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 you can apply using SSL certificate inspection mode is web filtering and application control
- 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, FortiGate parses server name indication (SNI) from client Hello, which is an extension of 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 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 certificate.

When you use certificate inspection, FortiGate inspects only the header information of the packets. You use certificate inspection to verify the identity of web servers. You can also use it to make sure that the HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

The only security feature that you can apply using SSL certificate inspection mode is web filtering and application control. 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 you use web filtering.

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

Preconfigured SSL certificate inspection profile

Select Multiple Clients Connecting to Multiple Servers

Select SSL Certificate Inspection

New SSL/SSH Inspection Profile

SSL Inspection Options

Protecting SSL Server

SSL Certificate Inspection

Full SSL Inspection

Fortinet_CAs SSL

Allow Block

View Blocked Certificates

Allow Block

View Trusted CAs List

Protocol Port Mapping

Inspect all ports

HTTPS

FORTINET
 Training Institute

© 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 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 performs web proxy and 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 connection with the web server is not delayed.

Although it appears as though the user 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 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 must import the root CA certificate, in order to trust FortiGate and accept an SSL session. You must install the chain of CA certificates 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

- 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

FORTINET
 Training Institute

© 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.

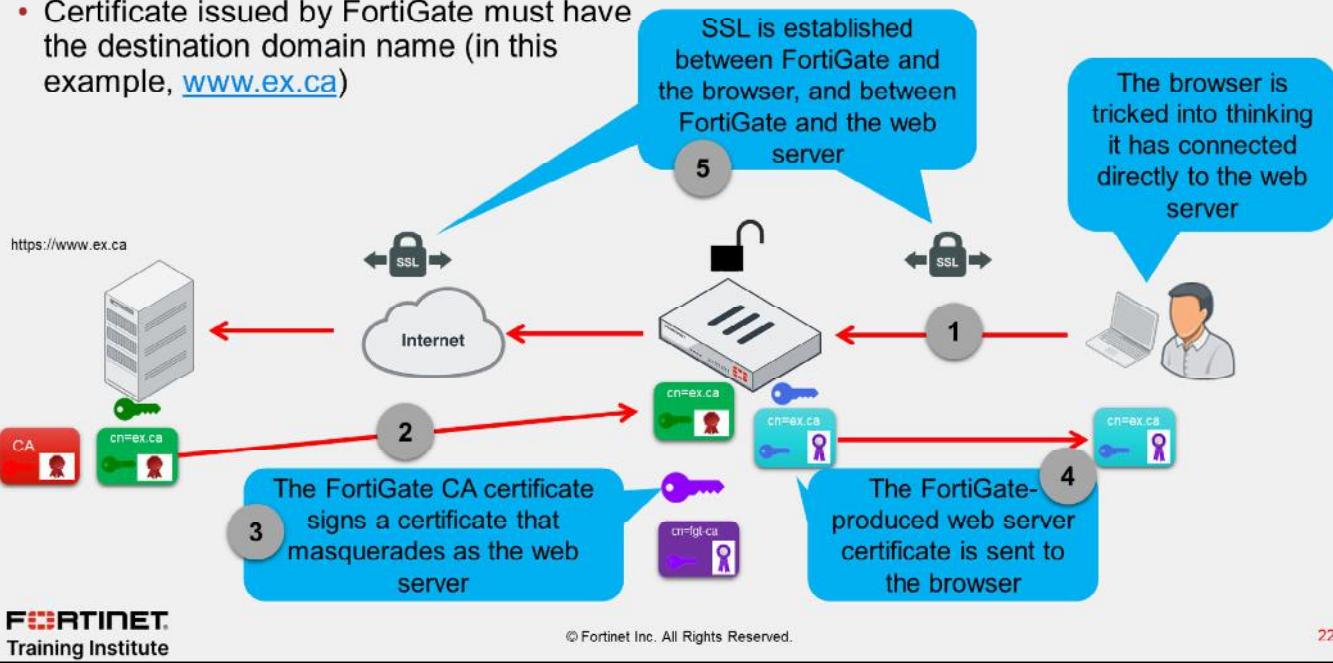
If the connection request is outbound (initiated by an internal client to an external server), you must select the option, **Multiple Clients Connecting to Multiple Servers**. Then, you must select the CA certificate that will be used to sign the new certificates. In the example shown on this slide, 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 (Contd)

- Certificate issued by FortiGate must have the destination domain name (in this example, www.ex.ca)



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, the FortiGate internal CA generates a new key pair and certificate. The new certificate 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 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

Security Profiles > SSL/SSH Inspection

New SSL/SSH Inspection Profile

Name: New Profile
Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL inspection of: **Multiple Clients Connecting to Multiple Servers**

Inspection method: Protecting SSL Server, SSL Certificate Inspection (Full SSL Inspection selected), Fortinet_CA_SSL

CA certificate: Fortinet_CA_SSL

Blocked certificates: **Untrusted SSL certificates** (Allow, Block, Ignore buttons selected)

Server certificate SNI check: Enable, Strict, Disable

Enforce SSL cipher compliance: Off

Enforce SSL negotiation compliance: Off

RPC over HTTPS: Off

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-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.

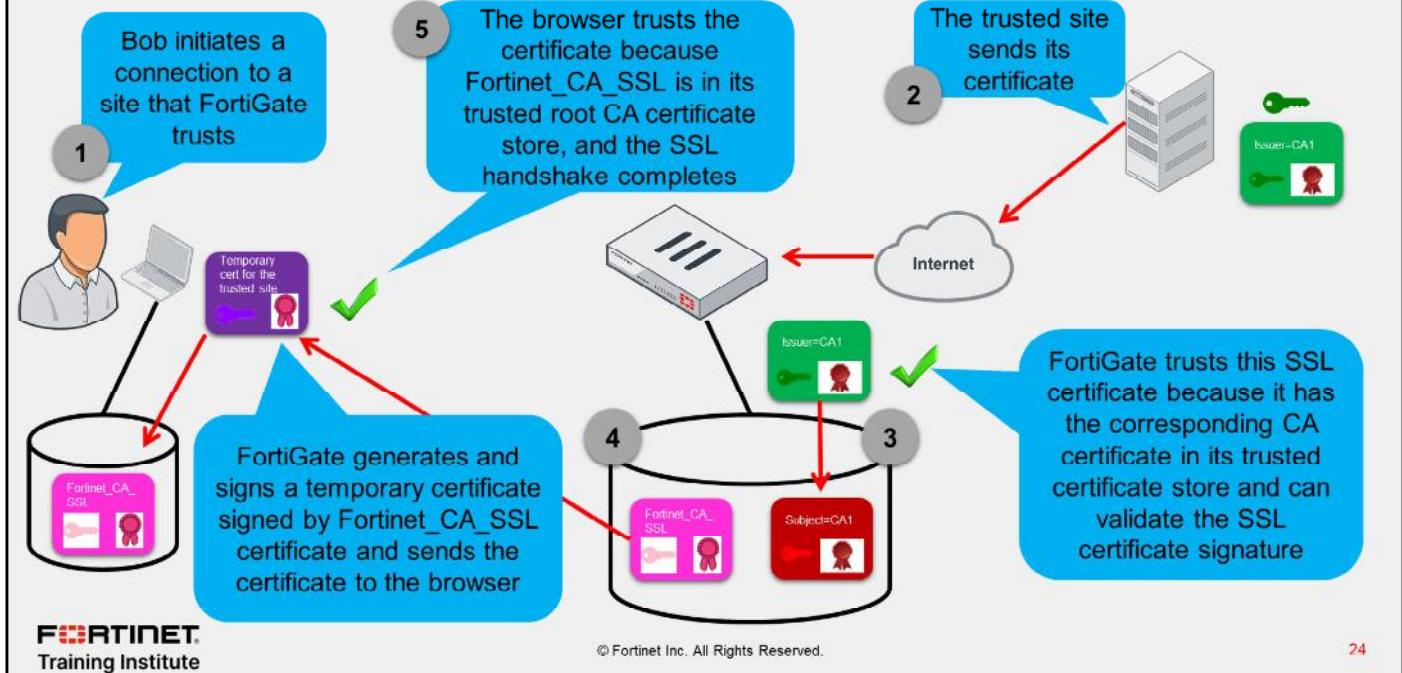
When you set the **Untrusted SSL certificates** setting to **Allow** and FortiGate detects an untrusted SSL certificate, FortiGate generates a temporary certificate signed by the built-in Fortinet_CA_Untrusted certificate. FortiGate then sends the temporary certificate to the browser, which presents 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 completes the SSL handshake. Otherwise, the browser also presents 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 certificate 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 status—trusted or untrusted. FortiGate then proceeds to establish SSL sessions.

DO NOT REPRINT
© FORTINET

Untrusted SSL Certificates—Trusted Site

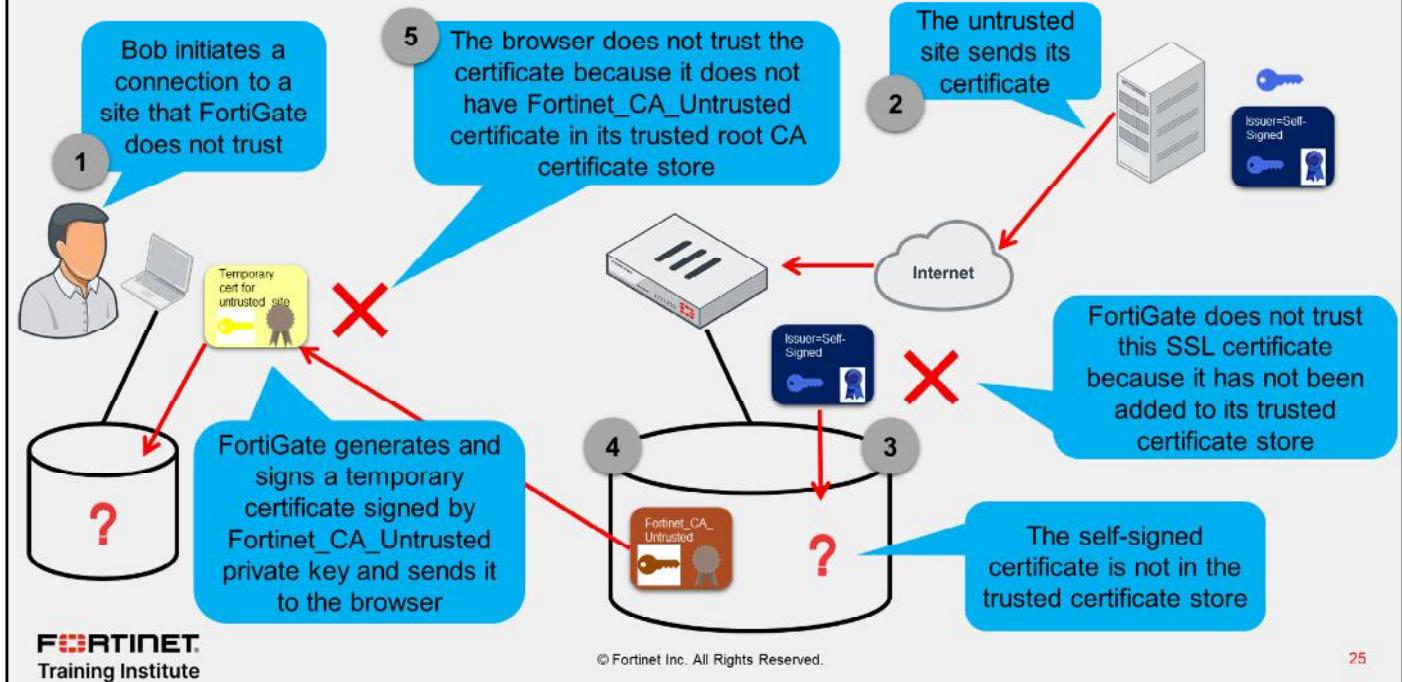


The scenario shown on this slide describes how FortiGate handles a trusted external site regardless of the **Untrusted SSL Certificate** setting.

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 the Fortinet_CA_SSL certificate. FortiGate sends the temporary certificate to the browser. Finally, in step 5, the browser trusts the temporary certificate because the 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



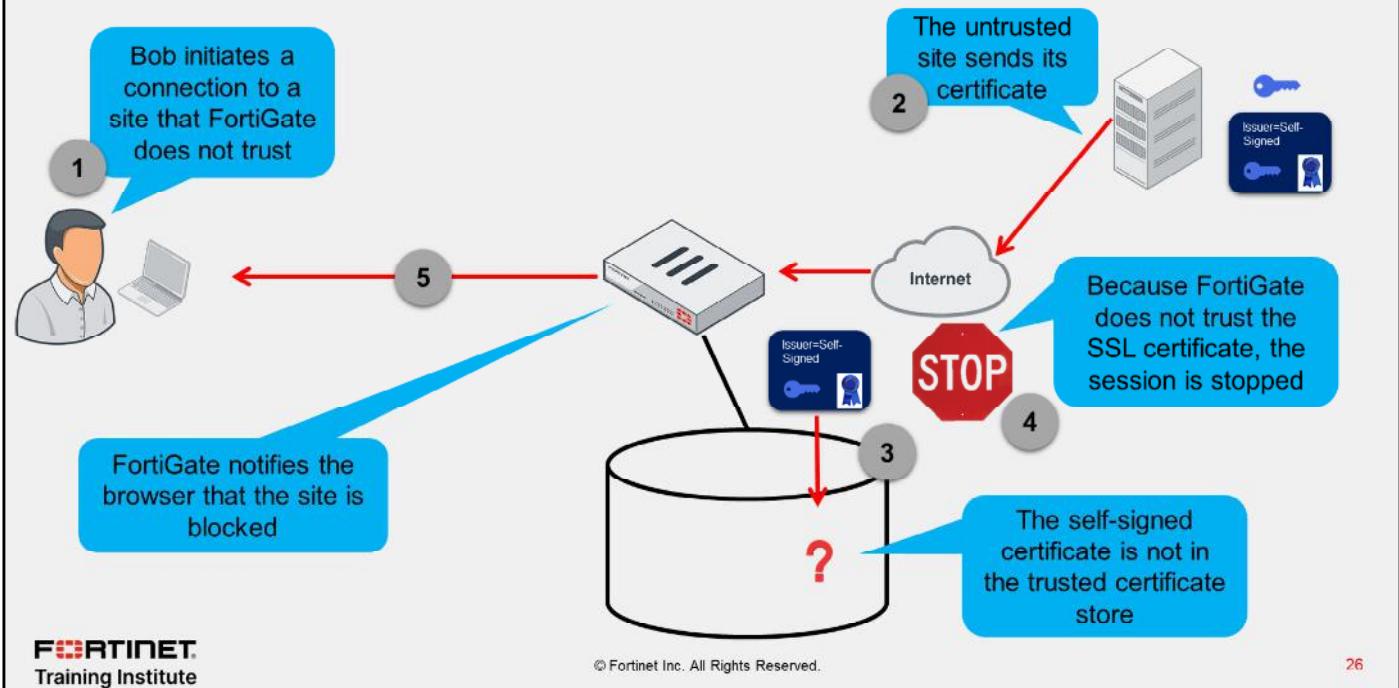
The scenario shown on this slide describes how FortiGate handles an untrusted external site when **Untrusted SSL Certificate** is set to **Allow**.

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 the 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 trusted certificate store. However, this has no impact in the future. The next time the user connects to the same untrusted site, a new temporary certificate is produced for the session.

DO NOT REPRINT
© FORTINET

Untrusted SSL Certificates—Blocked, Untrusted Site

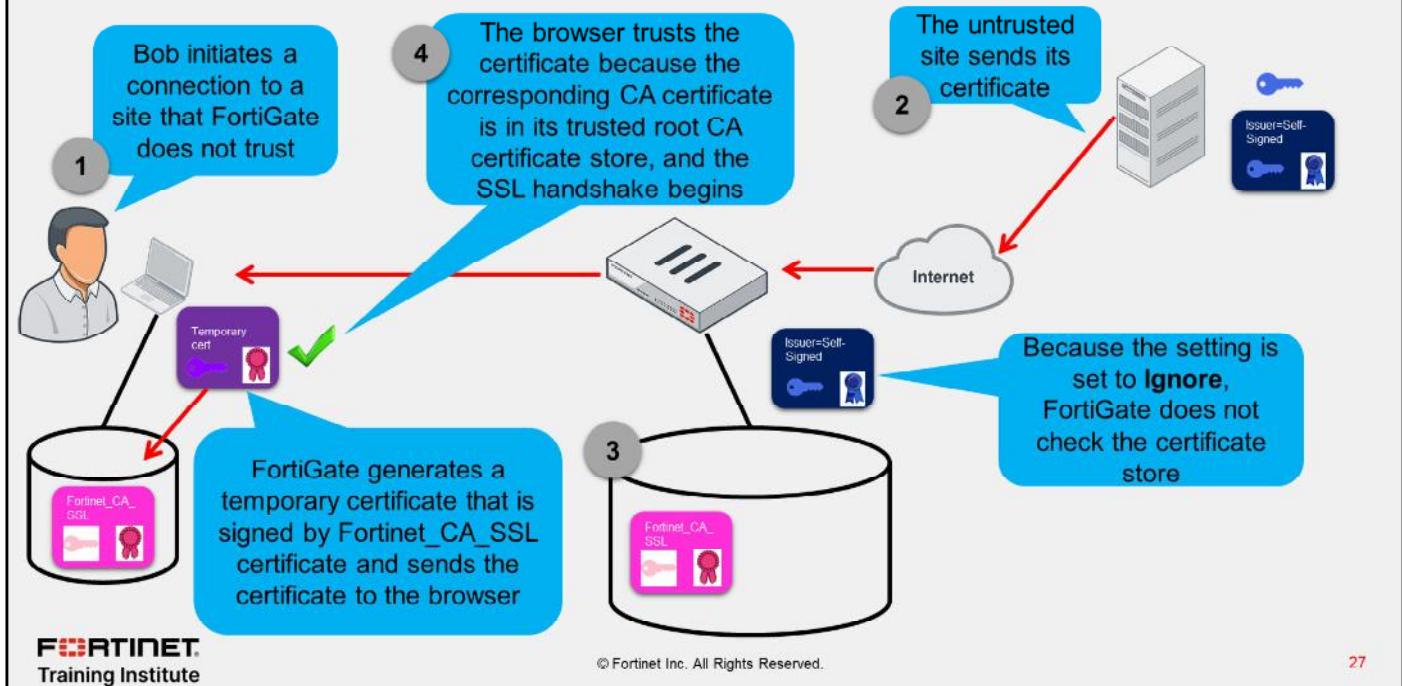


The scenario shown on this slide describes how FortiGate handles an untrusted external site when **Untrusted SSL Certificate** is set to **Block**.

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. After the browser finishes checking the certificate, it completes the SSL handshake with FortiGate. Next, FortiGate continues the SSL handshake with the untrusted 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

Allowlist exemption as rated by
 FortiGuard web filtering

Security Profiles > SSL/SSH Inspection

Exempt from SSL Inspection

Reputable websites

Web categories

Finance and Banking	X
Health and Wellness	X
Personal Privacy	X

Addresses

gmail.com	X
login.microsoft.com	X
login.microsoftonline.com	X

Log SSL events

You can exempt sites by web category or address

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. After FortiGate presents the temporary SSL certificate, browsers that use HPKP refuse to proceed. The SSL inspection profile, therefore, allows you to exempt specific traffic.

Laws protecting privacy might 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 an allowlist 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 **Keep Untrusted & Allow**, **Block**, or **Trust & Allow** invalid certificates
- Selecting **Custom** allows the user to select the action for each reason

Security Profiles > SSL/SSH Inspection

Common Options	
Invalid SSL certificates	Allow Block Custom
Expired certificates	Keep Untrusted & Allow Block Trust & Allow
Revoked certificates	Keep Untrusted & Allow Block Trust & Allow
Validation timed-out certificates	Keep Untrusted & Allow Block Trust & Allow
Validation failed certificates	Keep Untrusted & Allow Block Trust & Allow
Log SSL anomalies	 

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:

- **Keep untrusted & 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.
- **Trust & Allow:** FortiGate allows the website and takes the certificate as *trusted*.

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 presents the certificate as either trusted (signed by Fortinet_CA_SSL) or untrusted (signed by Fortinet_CA_Untrusted), and either allows the content or blocks it. You can also track certificate anomalies by enabling the **Log SSL anomalies** option.

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 certificate, private key, and chain of certificates must be installed on 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 **Multiple Clients Connecting to Multiple Servers** **Protecting SSL Server**

Server certificate **Cert_Webserver**

Protocol Port Mapping

Inspect all ports HTTPS 443

https://www.example.com

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

30

In the example shown on this slide, 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 key pair to FortiGate, and then select the certificate from the **Server Certificate** drop-down list.

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 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.

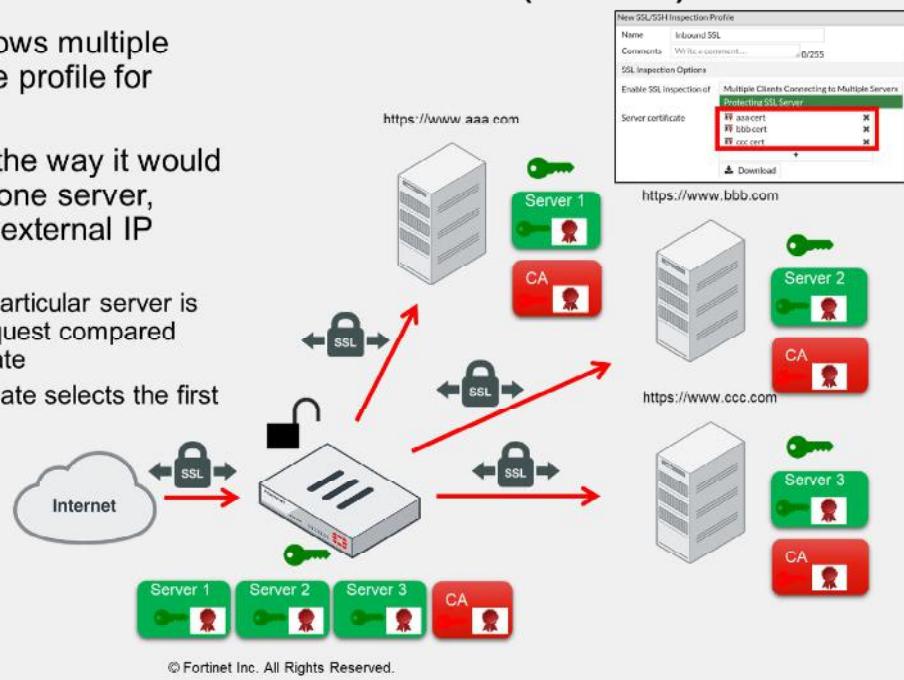
You must install the server certificate and private key plus the chain of certificates required to build the chain of trust. FortiGate sends the chain of certificates to the browser for this purpose.

DO NOT REPRINT
© FORTINET

Full SSL Inspection on Inbound Traffic (Contd)

- The inspection profile allows multiple certificates defined in one profile for multiple servers
- FortiGate acts similar to the way it would if the connection targets one server, however, it hits a shared external IP address:
 - Certificate selection to a particular server is based on SNI on each request compared against CN on the certificate
 - If no matching SNI, FortiGate selects the first certificate on the list

SNI: www.aaa.com
 IP: 172.16.1.1
 SNI: www.bbb.com
 IP: 172.16.1.1
 SNI: www.ccc.com
 IP: 172.16.1.1



FORTINET
 Training Institute

31

By creating a full SSL inspection profile on inbound traffic, you can configure the profile to use multiple web sites if they are approachable by the same external IP address. When FortiGate receives client and server hello messages, it selects the certificate to perform the full SSL inspection based on server name indication (SNI) value against the common name (CN) on the certificate part of the inspection profile. If a certificate CN matches the SNI on the request, FortiGate then selects this certificate to replace the original certificate and uses it to inspect the traffic.

If the SNI does not match the CN in the certificate list in the SSL profile, then FortiGate selects the first server certificate in the list.

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 does not scan SSL and SSH traffic through that firewall policy

Policy & Objects > Firewall Policy

Security Profiles

AntiVirus	AV default
Web Filter	disabled
DNS Filter	DNS default
Application Control	disabled
IPS	IPS default
SSL Inspection	SSL deep-inspection
Decrypted Traffic Mirror	disabled

Logging Options

Unallowed Traffic

Generate Logs when Session Starts

Capture Packets

Search + Create

SSL certificate-inspection

SSL custom-deep-inspection

SSL deep-inspection

SSL my-ssl-inspection-profile

SSL no-inspection

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 usually 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, it only works with flow-based inspection. 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 they can use the feature.

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 on 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.

You must install the SSL certificate on FortiGate and configure the device 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, you do not have to install the intermediate CA certificates on the browsers.

DO NOT REPRINT

© FORTINET

Applications and SSL Inspection

- Any SSL application might 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)

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 reports 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 certificate 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.

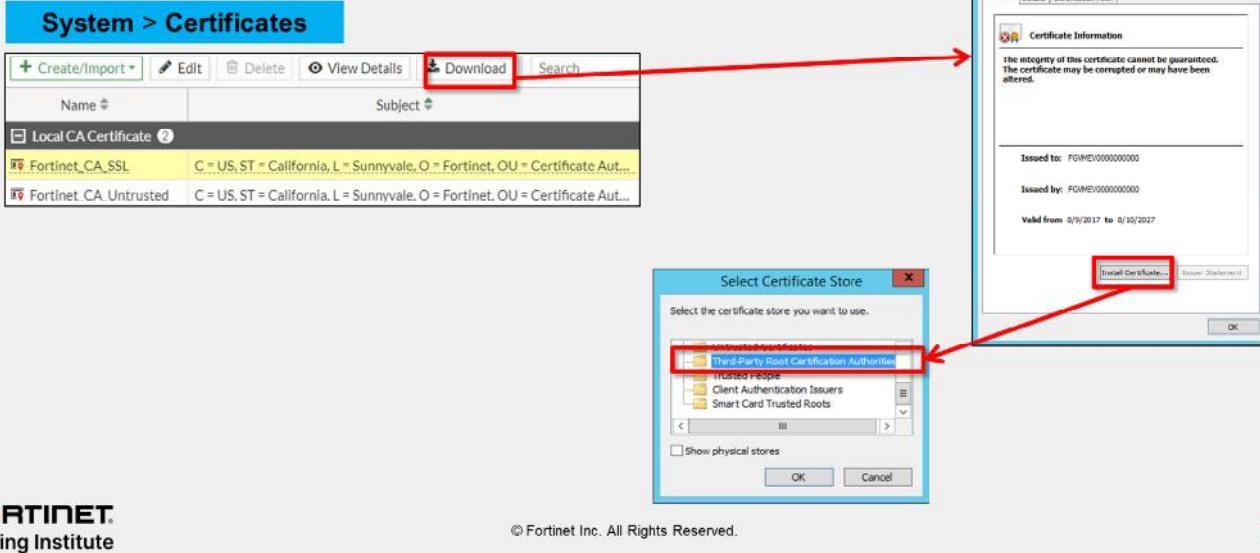
There are other applications that have built-in extra security checks that prevent MITM attacks, such as HPKP or certificate pinning. For example, Dropbox uses certificate pinning to ensure that no SSL inspection is possible on user traffic. As a result, when you enable full SSL inspection on FortiGate, your Dropbox client stops working and reports 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 depends on the security measures adopted by the application.

DO NOT REPRINT
© FORTINET

Installing an SSL Certificate Issued by a Private CA

- You should install private CA certificates used by SSL on endpoints
 - Prevents certificate warnings
 - Strict SSL fails with no override option if CA is untrusted



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 appears in your web browser any time you access an HTTPS website. Encrypted communications might also fail, simply because the CA that issued and signed the certificate is untrusted.

After 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 prevent certificate warnings, you must install the SSL certificate as a trusted root CA.

When you install the certificate, make sure that you save it to the certificate store for root authorities.

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

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
- ✓ Identify what is required to implement full SSL inspection
- ✓ Identify the obstacles to implementing full SSL inspection and possible remedies



© Fortinet Inc. All Rights Reserved.

38

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

By mastering the objectives covered in this lesson, you learned how FortiGate uses certificates, and how to manage and work with certificates in your network.

DO NOT REPRINT

© FORTINET



FORTINET

Training Institute



FortiGate Security

Web Filtering

 FortiOS 7.2

Last Modified: 23 August 2022

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



Video 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

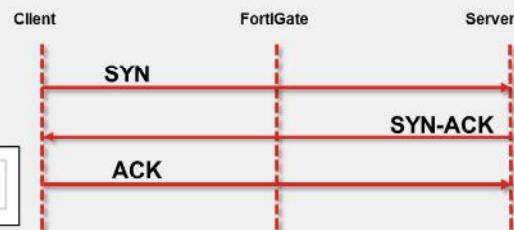
© FORTINET

Flow-Based Inspection

- Per firewall policy setting
- 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

Policy & Objects > Firewall Policy

Inspection Mode **Flow-based** Proxy-based



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:

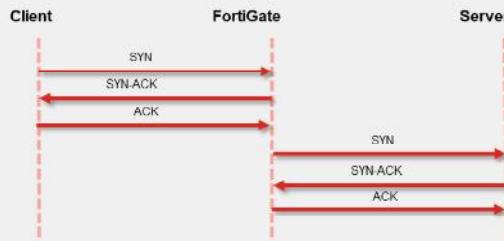
- A number of security features that are available in proxy-based mode are not available in flow-based mode
- Fewer actions are available based on the categorization of the website by FortiGuard services

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
Training Institute

© Fortinet Inc. All Rights Reserved.

5

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 inspection.

In TCP connections, the FortiGate 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 inspection, yielding fewer false positives and negative results.

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



Fortinet
Training Institute

© Fortinet Inc. All Rights Reserved.

6

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, URL categories and groups configured on security policy
 - Inspect traffic with additional security profiles, if enabled, such as AV, IPS, and file filter
 - Can use users and groups if authentication is required
- Available actions in security policy: **ACCEPT** or **DENY**
- SSL inspection profile to be selected in the consolidated policy

Policy & Objects > SSL Inspection & Authentication

Name	Access
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Service	ALL
SSL Inspection	
Comments	W...
Enable this policy	<input checked="" type="checkbox"/> no-inspection <input type="checkbox"/> certificate-inspection <input type="checkbox"/> custom-deep-inspection <input type="checkbox"/> deep-inspection <input type="checkbox"/> no-inspection

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

Policy & Objects > Security Policy

New Policy	ID	0
Name	Full Access	
Policy Mode	Standard	
Incoming Interface	port3	
Outgoing Interface	port1	
Source	all	
Destination	all	
Schedule	always	
Service	App Default	
Application	LinkedIn, Twitter	
URL Category	Business, Information and Computer Security	
Action	<input checked="" type="checkbox"/> ACCEPT, <input type="checkbox"/> DENY	

7

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 policy 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 according to the consolidated policy, FortiGate then processes it based on the security policy to analyze additional criteria, such as URL categories, groups for web filtering, and application control. Also, if enabled, the security policy further inspects traffic using security profiles such as AV, IPS, and file filter.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. 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.

2. Which statement 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



Video 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

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 and use FortiGuard web filter profiles.

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



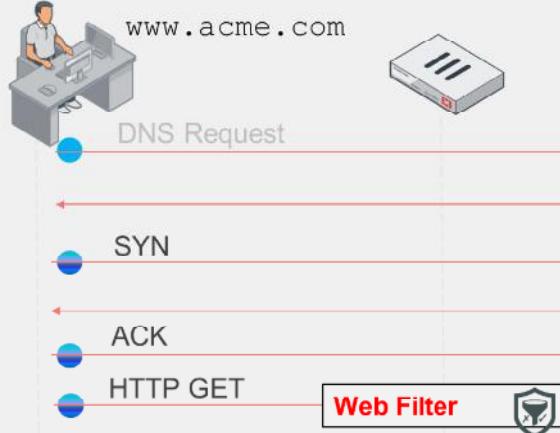
Web filtering helps to control, or track, the websites that people visit. There are many reasons why network administrators apply web filtering, including to:

- 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

(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 the following in the header: Host: www.acme.com, and the URL might look like the following in the header: /index.php?login=true.

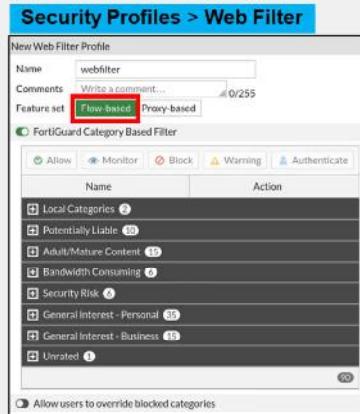
If you filter by domain, sometimes it blocks too much. For example, the blogs on tumblr.com are considered different content, because of all the different authors. In that case, you can be more specific, and block by the URL part, tumblr.com/hacking, for example.

DO NOT REPRINT

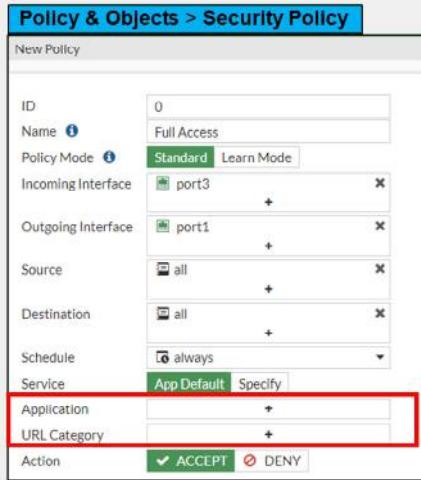
© FORTINET

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

13

Now, you will look at the web filter profile.

You can configure this security profile 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. 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 subcategories by FortiGuard. FortiGate offers two 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

DO NOT REPRINT
© FORTINET

Web Filter Profiles—Proxy Based

- Proxy-based options
 - Configure web filter profile
 - Local categories
 - Remote categories
 - Search engines
 - Proxy options
- 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 checked="" type="checkbox"/> Search Engines	
<input checked="" type="checkbox"/> Static URL Filter	
<input checked="" type="checkbox"/> Rating Options	
<input checked="" type="checkbox"/> Proxy Options	

In the 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:

- **Search Engines**
- **Static URL Filter**
- **Rating Options**
- **Proxy Options**

After you configure 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
- Can use FortiManager instead of FortiGuard

Categories action:

Proxy-Based	Flow-Based (Profile)	Flow-Based (Policy)
Allow	Allow	Accept
Block	Block	Deny
Monitor	Monitor	
Warning	Warning	
Authenticate	Authenticate	

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 reports 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 the **Allow websites when a rating error occurs** setting. You will learn more about this setting in this lesson.

You can configure FortiManager 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.

You can enable the FortiGuard category filtering on the web filter. Categories and subcategories are listed, and you can customize the actions to perform individually.

The actions available 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 (accept or deny)

To review the complete list of categories and subcategories, visit www.fortiguard.com/webfilter/categories.

DO NOT REPRINT
© FORTINET

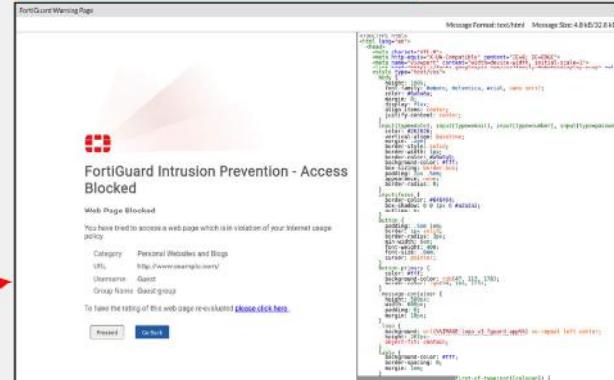
Web Filter FortiGuard Category Action—Warning

- Category Action =



- Exclusive for web filtering
 - Proxy mode
 - Flow mode (profile-based only)
 - Not available in:
 - Static URL filtering feature
- FortiGuard warning page
 - Customizable warning interval

System > Replacement Messages



The warning action informs users that the requested website is not allowed by the internet policies. However, the action gives the user the option to proceed to the requested website, or return to the previous website.

You can customize the warning interval, 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

Bandwidth Consuming (6)	
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

WebFilter_Group



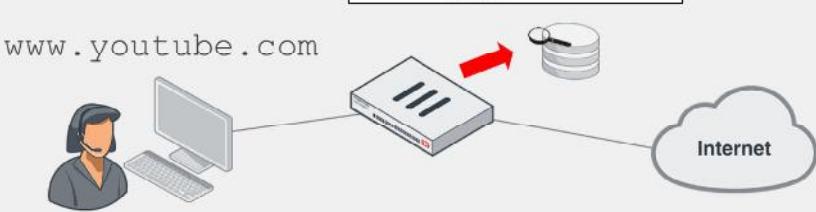
1. Define Users and Group
2. Set Action = Authenticate
3. Select User Group

 FortiGuard Intrusion Prevention - Access Blocked

Web Filter Block Override

Please contact your administrator to gain access to the web page.

Username:
 Password:



17

The authenticate action blocks the requested websites, unless the user enters a successful username and password. Local authentication and remote authentication using LDAP, radius and so on are supported for web filtering authentication.

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 prompts you to define user groups that are allowed to override the block.

FortiGate Security 7.2 Study Guide

267

DO NOT REPRINT
© FORTINET

Web Rating Override—Configuration

- Changes a website category, not the category action
 - Make an exception

Security Profiles > Web Rating Overrides

URL	Status	Comments	Ref.
Finance and Banking 1			
www.bing.com	Enable	0	
Games 1			
www.canamvrl.com	Enable		
Health and Wellness 1			
www.fortinet.com	Enable		

Edit Web Rating Override

URL: www.fortinet.com

Category: General Interest - Business

Sub-Category: Information Technology

Comments: Write a comment... 0/255

Override to

Category: General Interest - Personal

Sub-Category: Health and Wellness

Create New

© Fortinet Inc. All Rights Reserved. 18

If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. 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 depends on the settings within the web filter profile.

DO NOT REPRINT

© FORTINET

URL Filtering

Security Profiles > Web Filter

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
.*\something\{org biz}	Regular Expression	<input type="radio"/> Exempt <input checked="" type="radio"/> Enable	
somewhere.*	Wildcard	<input type="radio"/> Monitor <input checked="" type="radio"/> Enable	
www.somesite.com/someURL	Simple	<input checked="" type="radio"/> Block <input checked="" type="radio"/> Enable	

URL: www.somesite.com/someURL

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

- 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

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, regular expressions, and wildcard.

Take a look at how it works.

When a user visits a website, FortiGate looks at the URL list for a matching entry. In the example shown on this slide, 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**, so FortiGate displays a block page message.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following can act as a local FortiGuard server?

- A. FortiManager
- B. FortiAnalyzer

2. Which action in URL filtering will bypass all security profiles?

- A. Exempt
- B. Allow

DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes



Web Filtering Basics



Additional Proxy-Based Web Filtering Features



Video 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 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 search engine filters, and web content filtering.

DO NOT REPRINT

© FORTINET

Search Engine Filtering

- A proxy-based mode feature
- 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
- Logs all search keywords

Security Profiles > Web Filter

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex

Log all search keywords

```
config webfilter profile
  edit "default"
    config web
      set safe-search url header
      cnd
      next
    cnd
```



© Fortinet Inc. All Rights Reserved.

23

Search engine filtering is available when you configure a web filter profile while setting the feature set to proxy-based.

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 applies safe search to the requests when they pass through. Safe search is supported for Google, Yahoo, Bing, and Yandex.

As a proxy-based web filter feature, search engine filtering is supported only 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

Security Profiles > Web Filter

Pattern Type	Pattern	Language	Action	Status
Wildcard	something*	Western	Exempt	Enable
Regular Expression	.^quelqueque	French	Block	Enable

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 on 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 uses deep SSL inspection because FortiGate requires full access to the packet headers.

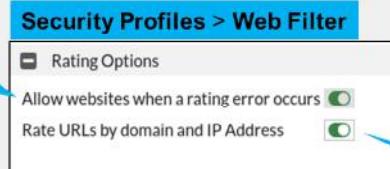
DO NOT REPRINT
© FORTINET

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.

You can use advanced web filtering settings to improve the web filter.

The rating options are as follows:

- Allow websites when a rating error occurs.** If a rating error occurs from the FortiGuard web filter service, users 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.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following is used for matching content in Web Content Filtering ?
 - A. Perl regular expressions
 - B. Boolean operators

2. Which feature can be used for restricting websites or images from search results ?
 - A. Web Content Filtering
 - B. Search Engine Filtering

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Inspection Modes****Web Filtering Basics****Additional Proxy-Based Web Filtering Features****Video Filtering****Best Practices and Troubleshooting**

Good job! You now understand additional proxy-based web filtering features.

Now, you will learn about video filtering.

DO NOT REPRINT**© FORTINET**

Video Filtering

Objectives

- Enable a YouTube API key
- Filter YouTube videos using FortiGuard
- Filter YouTube based on restriction level
- Filter YouTube channels

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

By demonstrating competence in video filtering, you will be able to control access to YouTube using FortiGuard categories and YouTube static IDs.

DO NOT REPRINT

© FORTINET

Video Filter Profile

- Controls YouTube content access:
 - To allow, monitor, or block based on category
 - To allow, monitor, or block access to channels
 - To set restriction levels
- Separate FortiGuard license for video filtering
- Supported only on proxy-based firewall policy
- Requires full SSL inspection
- Requires YouTube API key
- Enables YouTube key on CLI
 - You can add multiple YouTube API keys
- Filters videos using two methods:
 - FortiGuard categories
 - Channel IDs



```
config videofilter youtube-key
  edit 1
    set key "youtube_api_key"
    next
end
```

Video filtering allows you to control access to YouTube content using parameters that are associated with the video channel, video categories, or the video itself. It is part of the FortiGuard service, which requires a separate license bundled with the other FortiGuard security services.

To apply the video filter profile, proxy-based firewall policies currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy.

You must obtain a YouTube API key to use the video filter feature. The API key allows FortiGate to match parameters identified when users access YouTube content, and match the parameters with the local categories defined on the video filter.

DO NOT REPRINT
© FORTINET

Video Filter Profile—FortiGuard Categories

- FortiGuard categories for video filtering are based on universal classification:
 - Combine popular online video provider categories
- FortiGuard video categories:
 - Applicable to videos from YouTube, Vimeo, Dailymotion
 - Require API to determine category and match it on the video filter
 - Security action determines the flow of security checks:
 - If set to allow, bypass the rest of video filter profile
 - If set to monitor, log access and continue
 - If block, log and prevent playing the video

Security Profiles > Video Filter

FortiGuard Category Based Filter

Category	Action
Business	Allow
Entertainment	Allow
Games	Allow
Knowledge	Allow
Lifestyle	Allow
Music	Allow
News	Allow
People	Allow
Society	Allow
Sports	Allow

The video filter can identify videos using universal categories used by major online video content providers, such as YouTube. The generic classification combines multiple categories by these providers into one category. For example, the FortiGuard video category **Entertainment** includes YouTube categories, such as entertainment, comedy, movies, shows, and trailers.

The FortiGuard video categories are universal, to cover the common classifications used in the categories of online video content providers. Currently, it is applicable to content hosted by YouTube, Vimeo, and Dailymotion. Some of these providers offer API queries that enable FortiGate to identify the content and match it to local FortiGuard video categories.

In a video filter profile, if a FortiGuard category is allowed, the video content bypasses the rest of the security checks configured on the video profile, such as channel override and YouTube restriction level. If the action is set to monitor or block, then the video content undergoes further security checks configured on the video filter profile.

DO NOT REPRINT

© FORTINET

Video Filter Profile—YouTube

Security Profiles > Video Filter

Edit Video Filter Profile

Name: YouTube Filter

Comments: Write a comment... 0/255

FortiGuard Category Based Filter

YouTube

Restrict YouTube access: Moderate (selected)

Channel override list:

Channel ID	Comments	Action
UCJHo4AuVomwMRzgkA5DQE0A		Block (selected)

Set Moderate or Strict access to YouTube

You can Allow, Monitor, or Block access to specific YouTube channels IDs

Accessing the channel while on YouTube is blocked as configured in the video filter profile

Attention
Web Page Blocked
The page you have requested has been blocked because the requested video resource is not allowed.
URL: https://www.youtube.com/channel/UCupvZG-Sko_eiXAupb0fxWw
Description: Video channel is blocked, channel-id=UCupvZG-Sko_eiXAupb0fxWw
Username: Group Name

You will see a replacement message if you access a blocked channel directly using the URL

Connect to the internet
You're offline. Check your connection.
RETRY

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

31

You can restrict YouTube access on a video filter by setting the restriction level to **Moderate** or **Strict**. When users access YouTube content using the firewall policy with the video filter profile applied, the users are given only content that is screened according to a filter applied by Google. Moderate restricted access is similar to strict but makes more videos available.

The YouTube channel ID is used to identify YouTube channels. It allows FortiGate to apply actions to access related content on the channel. These actions can allow, monitor, or block access to the channel. If a video filter has a channel override to block a specific YouTube channel, access to this channel is stopped only to this particular channel. If a user attempts to access the channel while surfing YouTube content, an error message appears telling the user that they must connect to the internet. If the user accesses the channel using the URL, a blocked replacement message shows up to confirm the reason why access is blocked.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which is required by FortiGate to configure YouTube video filtering?

- A. YouTube API key
- B. Username

2. Which action in video filtering will prevent the videos from playing?

- A. Deny
- B. Block

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Inspection Modes****Web Filtering Basics****Additional Proxy-Based Web Filtering Features****Video Filtering****Best Practices and Troubleshooting**

Good job! You now understand the video filtering feature.

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

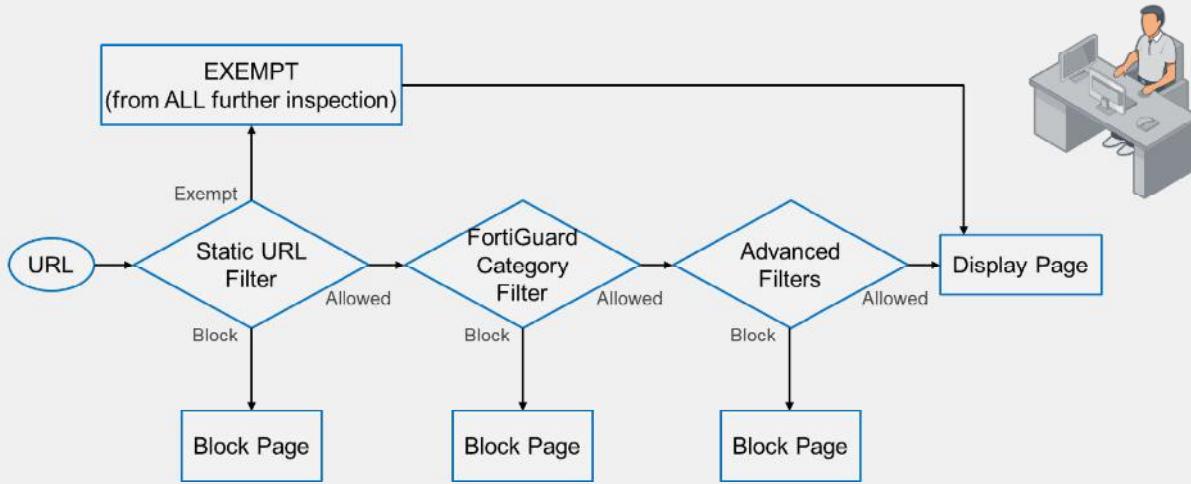
After completing this section, you should be able to achieve the objectives shown on this slide.

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



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 moves 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?

Policy & Objects > Firewall Policy

Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
IPS
File Filter
SSL Inspection

The 'Web Filter' and 'SSL Inspection' rows are highlighted with a red box.

```
config firewall policy
edit 1
set webfilter-profile <profile>
next
end

config firewall profile-group
edit <group name>
set webfilter-profile <profile>
next
end
```

You have configured your security profiles, but they are not performing web 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.

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 FortiGuard requests are lost

```
FortiGate-VM64 # diagnose debug rating
Locale      : english

Service     : Web filter
Status      : Enable
License     : Contract
\

Num. of servers : 1
Protocol      : https
Port          : 443
Anycast      : Enable
Default servers : Included

--- Server List (Wed Apr 21 13:59:43 2021) ---

IP          Weight    RTT Flags  TZ  FortiGuard-requests  Curr Lost Total Lost      Updated Time
173.243.140.16      -72    101 DI      0          36      0      0      0 Wed Apr 21 13:58:13 2021
```



© Fortinet Inc. All Rights Reserved.

37

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 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
- **FortiGuard-requests:** The number of requests sent by FortiGate to FortiGuard
- **Curr Lost:** Current number of consecutive lost FortiGuard requests (in a row, resets to 0 when one packet succeeds)
- **Total Lost:** Total number of lost FortiGuard requests

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

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

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

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

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

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

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 > Security Events

Date/Time	User	Source	Action	URL	Category
20 minutes ago	10.0.1.10	passthrough	https://www.bing.com/		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	https://www.bing.com/		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	http://www.bing.com/rp/hqv4DMgsfI4xwi6kpApki-DF...		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	http://www.bing.com/rp/hqx6FcD0hjfzrON5oLgx2RM...		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	http://www.bing.com/rp/mlKookf6UTEZv7k-d_D59PC...		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	http://www.bing.com/rp/08hWncb4hLQzpDiAvQdqLI...		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	http://www.bing.com/rp/bLULVERLX4vU6bjspboNMw...		Malicious Websites
20 minutes ago	10.0.1.10	passthrough	http://www.bing.com/rp/bLULVERLX4vU6bjspboNMw...		Malicious Websites

```

date=2022-04-03 time=22:10:44 eventtime=1649049044450880096 tz=-0700"
logid="0316013057" type="utm" subtype="webfilter" eventtype="ftgd_blk"
level="warning" vd="root" policyid=1 policytype="policy" sessionid=3425 srcip=10.0.1.10
srcport=54354 srccountry="Reserved" srcintf="port3" srcintfrole="undefined"
dstip=13.107.21.200 dstport=80 dstcountry="United States" dstintf="port1"
dstintfrole="undefined" service="HTTP" hostname="www.bing.com" "profile="default"
action="passthrough" reqtype="direct" url="http://www.bing.com/" sentbyte=342 rcvbyte=0
direction="outgoing" msg="URL belongs to a category with warnings enabled"
  ratemethod="domain" cat=26 catdesc="Malicious Websites" crscore=30 craction=4194304
|

```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

39

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.

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Inspection Modes****Web Filtering Basics****Additional Proxy-Based Web Filtering Features****Video 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
- ✓ Work with web filter categories
- ✓ Configure web filter to support search engines
- ✓ Apply video filter on proxy-based firewall policy
- ✓ Monitor logs for web filtering events



© Fortinet Inc. All Rights Reserved.

42

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
Training Institute



FortiGate Security

Application Control

FortiOS 7.2

Last Modified: 13 June 2022

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



© Fortinet Inc. All Rights Reserved.

2

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



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



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.

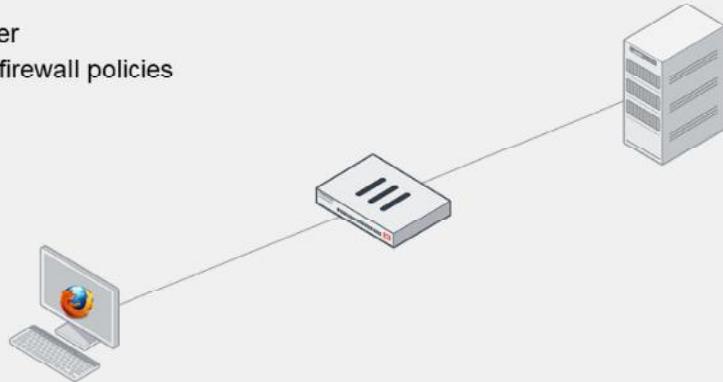
These techniques make P2P applications difficult to block using a firewall policy, and also make them difficult to detect by proxy-based inspection.

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



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.

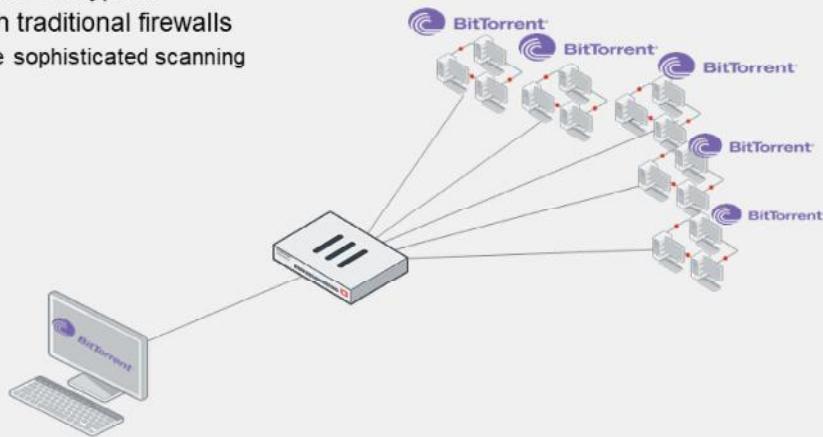
Traditional downloads use a defined protocol over a standard port number. Whether it's from a web or FTP site, the download is from a single IP address, to a single IP address. So, blocking this kind of traffic is easy: you only need one firewall policy.

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 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 for database updates
 - The database of application control signatures is separate from the IPS database.

The screenshot shows two parts of the FortiGate configuration interface. The top part, titled 'System > FortiGuard', displays a table of updates. The 'Application Control Signatures' row is highlighted with a red box and shows 'Version 20.00291'. A blue callout points to this row with the text 'Currently installed application control database version'. To the right of the table is a 'Actions' dropdown with 'Upgrade Database' selected, and a blue callout points to it with the text 'Forcing FortiGate to check for latest updates'. The bottom part, also titled 'System > FortiGuard', shows 'FortiGuard Updates' settings. The 'Scheduled updates' section is highlighted with a red box, showing 'Every Day' selected, '1' in the count field, and 'AM' in the time dropdown. A blue callout points to this section with the text 'Configuring scheduled updates'. Other settings in this section include 'Improve IPS quality', 'Use extended IPS signature package', 'AntiVirus PUP/PUA', and 'Update server location' with options 'Lowest latency locations', 'Restrict to', 'US only', and 'EU only'.

FORTINET
 Training Institute

© 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 updates come as part of the standard FortiCare support contract, but it requires a subscription for database updates. 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.

DO NOT REPRINT

© FORTINET

Application Control Database

- You can view complete list of applications supported by FortiGuard application control on <https://fortiguard.com/>
 - You can review the application category or request a signature for a new application from the same website.

The screenshot shows two main views of the FortiGuard Application Control Database. The left view is a search interface with filters for Risk Level (All, Level 5, Level 4, Level 3, Level 2, Level 1), Popularity (All, 5 stars, 4 stars, 3 stars, 2 stars, 1 star), and Category (All, Proxy). A blue callout box points to the 'Refine search using filters' link. The right view is a detailed application profile for 'Tor' (ID: 13363). It includes a description of Tor as a free proxy software for anonymous communication, its technology (Browser-Based, Network-Protocol, Client-Server, Peer-to-Peer, Cloud-Based, Mobile Device, Tunneling), and its behavior (Frequent, Tunnelling). A red callout box points to the 'Tor (Proxy)' link in the search results.

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 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. The rating can help you decide whether or not to block an application.

On the FortiGuard website, you can read details about each signature's related application.

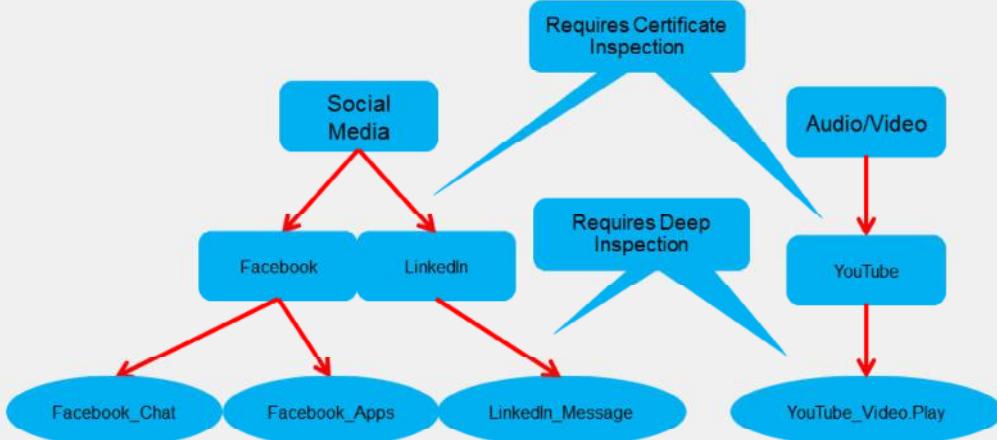
This slide shows an example for an application called Tor. Tor is a web proxy, so it belongs in the proxy category. A best practice is to create test policies that you can use to observe policy behavior.

If the most recent FortiGuard update does not include a definition for an application that you need to control, you can submit a request on the FortiGuard website to have the application 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



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 a hierarchical structure. This gives you the ability to inspect the traffic with more granularity. You can block Facebook applications 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.

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 NGFW policy mode.

DO NOT REPRINT**© FORTINET**

Application Control Profiles

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

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

111 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: wifi-default
Comments: Default configuration for offloading WiFi traffic. 50/255

Categories: All Categories (Applies an action to all categories at once)

- Business (153, △ 6)
- Email (77, △ 12)
- IoT (450)
- P2P (56)
- Social.Media (118, △ 32)
- Video/Audio (155, △ 17)
- Unknown Applications (Matches traffic to unidentified applications)
- Cloud.IT (66, △ 1)
- Game (86)
- Mobile (3)
- Proxy (174)
- Storage.Backup (161, △ 19)
- VoIP (23)
- Collaboration (268, △ 16)
- General.Interest (233, △ 8)
- Network.Service (334)
- Remote.Access (95)
- Update (49)
- Web.Client (24)

Firmware & General Updates License: Licensed (Expiration Date: 2022/12/19)
Application Control Signatures Package: Version 20.00291
Application Signatures: [View Application Signatures](#) (Displays list of application control signatures)

Additional Information: [API Preview](#), [References](#), [Edit in CLI](#), [Documentation](#), [Online Help](#), [Video Tutorials](#)

© 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 must decrypt the traffic in order to perform inspection and control application traffic.

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

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

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

DO NOT REPRINT
© FORTINET

Configuring Additional Options

- Application control profiles include additional options that you can configure

The number to the right of the cloud symbol indicates the number of cloud applications in the category

The number listed to the right of the cloud symbol indicates the number of cloud applications in the category.

Allow and Log DNS Traffic: Enable this option to allow DNS traffic for the application sensor. Depending on the application and how often it queries DNS servers, enabling this setting can use significant system resources.

QUIC: QUIC is a protocol from Google that uses UDP instead of the standard TCP connections for web access. UDP is not scanned by web filtering. Allowing QUIC instructs FortiGate to inspect Google Chrome packets for a QUIC header and to generate logs as QUIC messages. Blocking QUIC forces Google Chrome to use HTTP2/TLS1.2 and FortiGate to log QUIC as blocked. The default action for QUIC is **Block**.

Replacement Messages for HTTP-based Applications: This setting allows you to replace blocked content from HTTP/HTTPS applications with an explanation for the user's benefit. For non-HTTP/HTTPS applications, FortiGate only drops the packets or resets 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 only to 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

- Allows blocking or monitoring of known services on unknown ports

The screenshot shows the FortiGate interface for 'Security Profiles > Application Control'. On the left, a 'Categories' tree includes 'All Categories' and various service groups like Business, Email, Mobile, Proxy, Storage/Backup, VoIP, Cloud/IT, Game, Network Service, P2P, Remote Access, Update, Collaboration, General Interest, Social Media, Video/Audio, and Web Client. Below this is the 'Network Protocol Enforcement' table:

Port #	Enforce Protocols	Violation Action
Port 52	PROT DNS	Monitor
Port 80	PROT HTTP	Block

A red box highlights the 'Create New' button in the table header. A red arrow points from this button to a 'Create New' dialog box on the right. This dialog box has fields for 'Port' (80) and 'Enforce protocols' (PROT HTTP). A red box highlights the 'PROT HTTP' entry in the list. Below this is a 'Violation action' section with 'Monitor' and 'Block' buttons. A red box highlights the 'Block' button. At the bottom are 'OK' and 'Cancel' buttons. To the right of the dialog is a 'Select Entries' sidebar with a 'List of known services' section containing a list of protocols: DNS, FTP, HTTP, HTTPS, IMAP, NNTP, POP3, SMTP, SNMP, SSH, and TELNET. A blue callout box points to this list.

FORTINET
Training Institute

© 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. For example, if port 21 is configured for FTP and IPS Dissector could not decide on the exact service but is sure it is not FTP. If the port of the non-ftp traffic is 21, it will be a violation.

DO NOT REPRINT

© FORTINET

Scanning Order

- The IPS engine identifies the application
- The application control profile scans for matches in this order:
 1. Application and filter overrides
 2. Categories

FORTINET
Training Institute

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:

1. 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.
2. 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)

- Application Overrides:** Battle.Net and Dailymotion applications are set to **Monitor**
- Filter Overrides:** Excessive bandwidth consuming applications are set to **Block**
 - Contains applications from different categories – BitTorrent (P2P), Adobe Update (Update), FaceTime (VOIP), Flickr (Social.Media)
- Categories:** The **Game** and **Video/Audio** categories are set to **Block** and all other categories are set to **Monitor**

Priority	Details	Type	Action
1	BattleNet, Dailymotion	Application	Monitor
2	Excessive-Bandwidth	Filter	Block

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 and Filter 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 are allowed, and generate logs.

Next, the scan checks for **Application and Filter Overrides**. Because a filter override is configured to block applications that use excessive bandwidth, it blocks 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)

- Filter Overrides:** Excessive bandwidth consuming applications are set to **Block**
 - Contains applications from different categories – BitTorrent (P2P), Adobe.Update (Update), FaceTime (VOIP), Flickr (Social.Media)
- Application Overrides:** Battle.Net and Dailymotion applications are set to **Monitor**
- Categories:** The **Game** and **Video/Audio** categories are set to **Block** and all other categories set to **Monitor**

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Battle-Net	Application	Monitor

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**) is blocked and, since **Dailymotion** falls under the excessive bandwidth category, Dailymotion is blocked even though it is set to **Monitor** under the **Application and Filter Overrides** section.

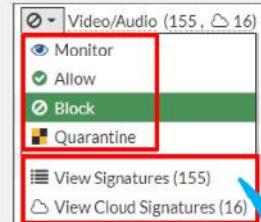
The priority in which application and filter overrides are placed takes precedence.

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

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.

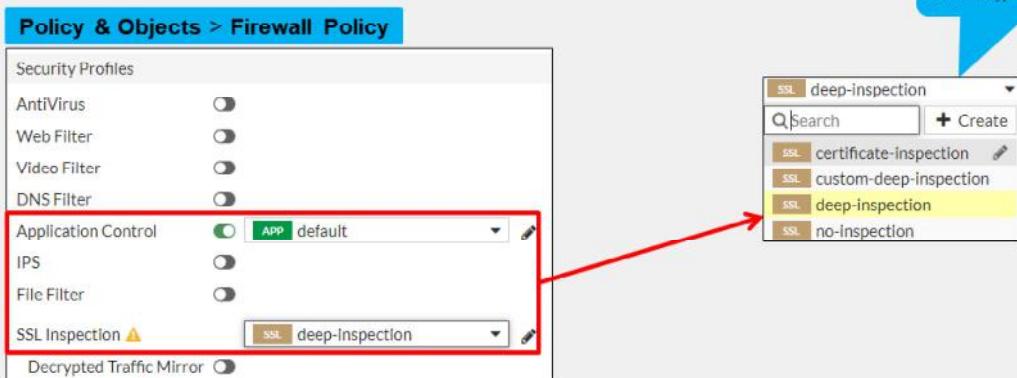
Which is the correct action to choose?

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

- You must apply the **Application Control** profile on a firewall policy to scan the passing traffic
 - You must also select **SSL/SSH Inspection** profile



After you configure an application control profile, you must apply it to a firewall policy. This instructs FortiGate to start scanning application traffic that is subject to the firewall policy.

DO NOT REPRINT

© FORTINET

Block Page

- Application control in profile mode displays 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



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 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
- Must select SSL inspection profile on an SSL Inspection & Authentication (consolidated) policy
- Requires the use of central SNAT policy

The image shows two screenshots of the FortiGate management interface. The left screenshot, titled 'Policy & Objects > Central SNAT', displays a 'New Policy' configuration. It includes fields for Incoming Interface (port3), Outgoing Interface (port1), Source Address (all), Destination Address (all), and NAT (selected). The 'Protocol' dropdown shows 'any' is selected. The right screenshot, titled 'Policy & Objects > SSL Inspection & Authentication', shows an 'Edit Policy' screen for policy ID 1. It lists 'Name' (Default), 'Incoming Interface' (any), 'Outgoing Interface' (any), 'Source' (all), 'Destination' (all), and 'Service' (ALL). A note indicates 'Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied'. The 'SSL Inspection' dropdown is set to 'no-inspection'. Both screenshots include a 'Comments' field and an 'Enable this policy' checkbox. The bottom of the interface shows the Fortinet logo and 'Training Institute'.

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**

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

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

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

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

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

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

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

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

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

DO NOT REPRINT
© FORTINET

Configuring App Control in Policy-Based Mode

Policy & Objects > Security Policy

New Policy

Application (highlighted in red)

Category (highlighted in red)

Group (highlighted in red)

Group Name: High Bandwidth

Type: Application

Members: Dailymotion, YouTube

Comments: Write a comment... 0/255

ACCEPT **DENY**

© Fortinet Inc. All Rights Reserved. **27**

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. For 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

New Policy

Incoming Interface	port3	+	x
Outgoing Interface	port1	+	x
Source Address	all	+	x
Destination Address	all	+	x

NAT

IP Pool Configuration

Protocol

Use Outgoing Interface Address Use Dynamic IP Pool

any TCP UDP SCTP Specify 0

Policy & Objects > SSL Inspection & Authentication

Edit Policy

ID	1
Name	Default
Incoming Interface	any
Outgoing Interface	any
Source	all
IP/MAC Based Access Control	any
Destination	all
Service	ALL

Firewall/Network Options

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

Security Profiles

SSL Inspection: no-inspection

Comments: Write a comment... 0/1023

Enable this policy:

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

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

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

DO NOT REPRINT

© FORTINET

NGFW Policy Matching

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

Policy & Objects > Security Policy

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

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

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



If an application is necessary, but you must 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

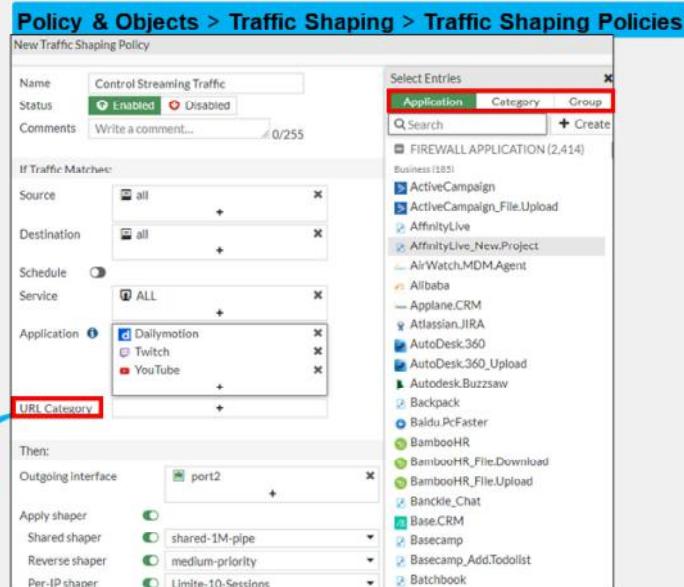
All of these items have separate URLs. If you analyze a site like YouTube, the web pages themselves don't use much bandwidth; it is the video content that uses the most bandwidth. But, since all content is transported using the same protocol (HTTPS), and the URLs contain dynamically generated alphanumeric 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



Fortinet Training Institute

© Fortinet Inc. All Rights Reserved

31

You can limit the bandwidth of an application category, application group, 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), you can set the source in the traffic shaping policy 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 you can configure 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 an 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 configuration.

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

Policy & Objects > Security Policy

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

All attempts to access these applications are blocked and logged

Access to P2P applications are blocked; however attempts are not be logged

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

35

Regardless of which operation mode application control is configured in, you must enable logging on the security or firewall policy. When you enable the logging of security events or all sessions 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.

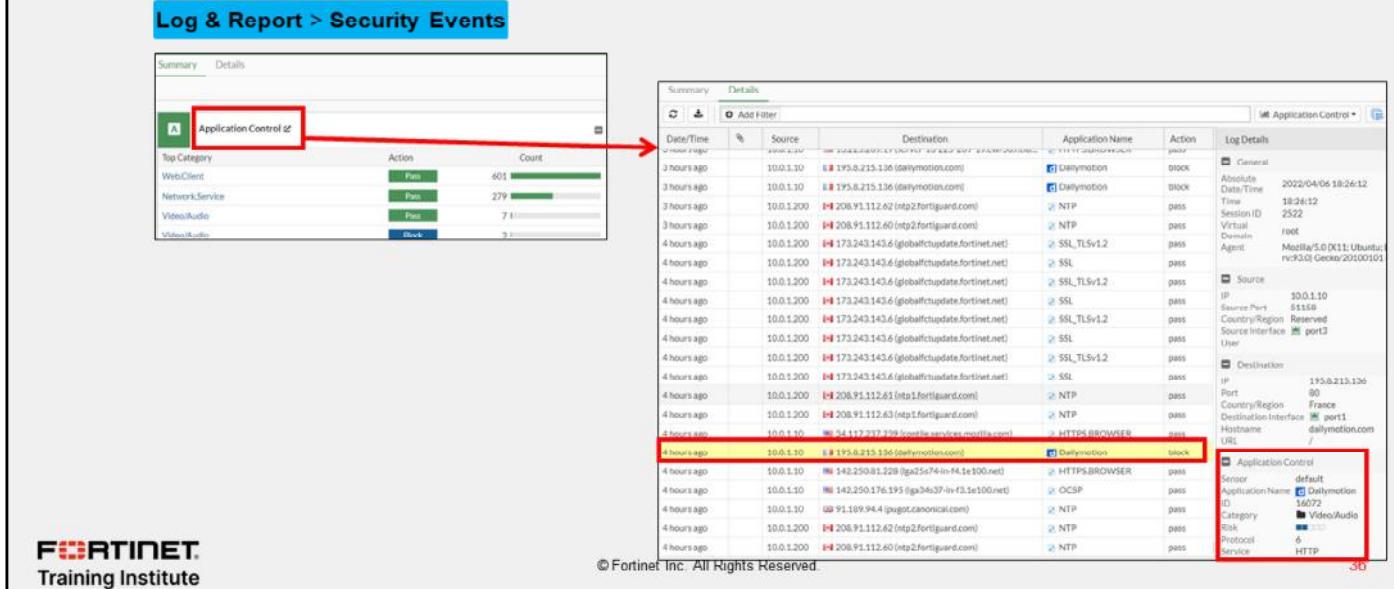
When the **Deny** action is selected on a security or firewall policy, you must enable the **Log Violations** option to generate application control events for blocked traffic.

DO NOT REPRINT

© FORTINET

Logging Application Control Events

- FortiGate logs all application control events on the **Security Events** pane on the **Log & Report** page



The screenshot shows the FortiGate Log & Report interface with the Security Events pane selected. The top navigation bar has a red box around the 'Application Control' link. An arrow points from this link to a detailed log entry in the main pane. The log entry is for a block action on Dailymotion. The log details are as follows:

Date/Time	Source	Destination	Application Name	Action	Log Details
3 hours ago	10.0.1.10	193.8.0.215.136 (dailymotion.com)	Dailymotion	block	General
3 hours ago	10.0.1.10	193.8.0.215.136 (dailymotion.com)	Dailymotion	block	Absolute Date/Time: 2022/04/06 18:26:12
3 hours ago	10.0.1.200	208.91.112.62 (http2.fortiguard.com)	NTP	pass	Session ID: 2522
3 hours ago	10.0.1.200	208.91.112.60 (http2.fortiguard.com)	NTP	pass	Virtual Domain: none
3 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL, TLSv1.2	pass	Agent: Mozilla/5.0 (X11; Ubuntu; rv:3.0) Gecko/20100101
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL	pass	Source IP: 10.0.1.10
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL, TLSv1.2	pass	Source Port: 51558
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL	pass	Country/Region: Reserved
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL	pass	Source Interface: port2
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL, TLSv1.2	pass	User
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL	pass	Destination IP: 193.8.0.215.136
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL, TLSv1.2	pass	Port: 80
4 hours ago	10.0.1.200	173.243.143.6 (globalfctupdate.fortinet.net)	SSL	pass	Country/Region: France
4 hours ago	10.0.1.200	208.91.112.63 (http1.fortiguard.com)	NTP	pass	Destination Interface: port1
4 hours ago	10.0.1.200	208.91.112.63 (http1.fortiguard.com)	NTP	pass	Hostname: dailymotion.com
4 hours ago	10.0.1.10	84.112.217.239 (fontfile.services.mozilla.com)	HTTPS.BROWSER	pass	URL
4 hours ago	10.0.1.10	193.8.0.215.136 (dailymotion.com)	Dailymotion	block	Application Control
4 hours ago	10.0.1.10	142.250.81.228 (tg2a2574-in-f4.1e100.net)	HTTPS.BROWSER	pass	Sensor: default
4 hours ago	10.0.1.10	142.250.176.195 (g4d4637-in-f3.1e100.net)	OCSP	pass	Application Name: Dailymotion
4 hours ago	10.0.1.10	91.189.94.14 (pugit.canonical.com)	NTP	pass	ID: 16072
4 hours ago	10.0.1.200	208.91.112.62 (http2.fortiguard.com)	NTP	pass	Category: Video/Audio
4 hours ago	10.0.1.200	208.91.112.60 (http2.fortiguard.com)	NTP	pass	Rule: 6
4 hours ago	10.0.1.200	208.91.112.60 (http2.fortiguard.com)	NTP	pass	Protocol: HTTP

© Fortinet Inc. All Rights Reserved.

FortiGate logs all application control events on the **Security Events** pane on the **Log & Report** page. You can view the logs by clicking on **Application Control**.

In the example shown on this slide, the default application control profile blocks access to **Dailymotion**. You can view this information in the **Log Details** section, as well as information about the log source, destination, application, and action.

Note that application control generates this log message using a profile-based configuration. The log message for an NGFW policy-based configuration, does not include information that does not apply, such as application sensor name. The remainder of the information and structure of the log message is the same for each log, regardless of which inspection mode FortiGate is using.

You can also view the details on the **Forward Traffic** logs pane, where firewall policies record activity. You can 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.

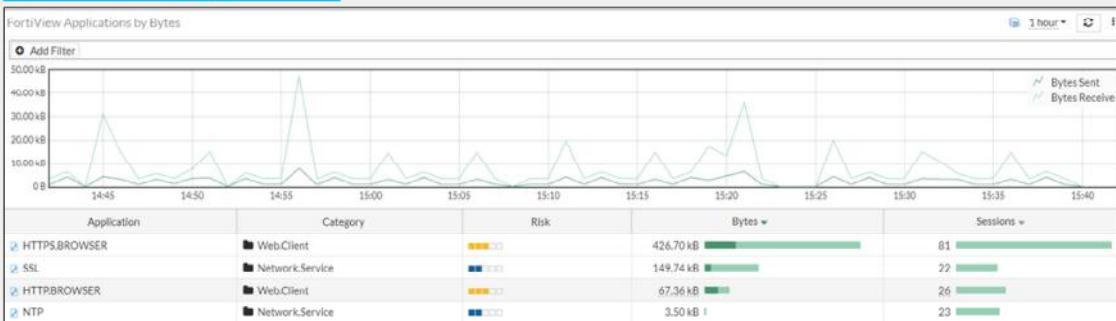
DO NOT REPRINT
© FORTINET

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



FORTINET
Training Institute

© 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

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 reduces resource use, and also helps 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



The screenshot shows the 'System > FortiGuard' page. It displays license information for FortiCare Support, FortiCloud Account, Hardware Version, Enhanced Support, and Virtual Machine. The 'Virtual Machine' section shows a progress bar for Allocated vCPUs at 100% (1/1) and Allocated RAM at 2 GiB. A 'Actions' dropdown is visible for the FortiGate VM License. The bottom of the page includes the Fortinet Training Institute logo and a copyright notice: © Fortinet Inc. All Rights Reserved.

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 FortiManager)
- If the internet connection is stable, check DNS resolution on FortiGate
- If FortiGate is installed behind a network firewall, make sure that port443 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

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



© Fortinet Inc. All Rights Reserved.

45

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
Training Institute



FortiGate Security

Antivirus

FortiOS 7.2

Last Modified: 13 June 2022

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

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

Antivirus Basics

Objectives

- 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**

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
- Machine learning (AI) scan:
 - Enabled by default
 - Machine learning training model
 - Trained by FortiGuard Labs
 - Malware detection model
 - To detect Windows Portable Executables (PEs)
 - Mitigation process for zero-day attacks
 - Files detected by AI scan are identified with the W32/AI.Pallas.Suspicious signature.

Order of scan

1 Antivirus Scan

2 Grayware Scan

3 AI Scan

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.
- Machine learning (AI) scan: These scans are based on probability, so they increase the possibility of false positives, but they also detect zero-day attacks. Zero-day attacks are malwares that are new, unknown, and, therefore, have no existing associated signature. If your network is a frequent target, enabling an AI scan may be worth the performance cost because it can help you to detect a virus before the outbreak begins. Files detected by AI scan are identified with the W32/AI.Pallas.Suspicious signature.

If all antivirus features are enabled, FortiGate applies the following scanning order: antivirus scan, followed by grayware scan, followed by AI scan.

DO NOT REPRINT

© FORTINET

Sandboxing

- FortiSandbox detects zero-day attacks with high certainty:
 - FortiGate uploads files to FortiSandbox Cloud or a FortiSandbox appliance
 - Two type of cloud sandboxing
 - FortiGate cloud: You must activate a FortiCloud account
 - FortiSandbox cloud: You will require an entitlement license embedded to FortiGate
 - 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 a FortiSandbox appliance to supplement the FortiGuard database

Security Fabric > Fabric Connectors

Edit Fabric Connector	
Other Fortinet Products	
 FortiSandbox	
FortiSandbox Settings	
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Server	10.0.1.201
Notifier email	admin@acme.corp
Test Connectivity	

Security Fabric > Fabric Connectors

Edit Fabric Connector	
Core Network Security	
 Cloud Sandbox	
Cloud Sandbox Settings	
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Type	<input checked="" type="radio"/> FortiGate Cloud <input type="radio"/> FortiSandbox Cloud
Region	Global

You need to enable FortiSandbox cloud option on CLI under system global with the command on the CLI set gui-fortigate-cloud-sandbox enable

What if AI 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 either FortiSandbox Cloud or a FortiSandbox appliance. Note you will need to enable cloud sandboxing on the CLI under system global settings for configuration options to appear on GUI. 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.

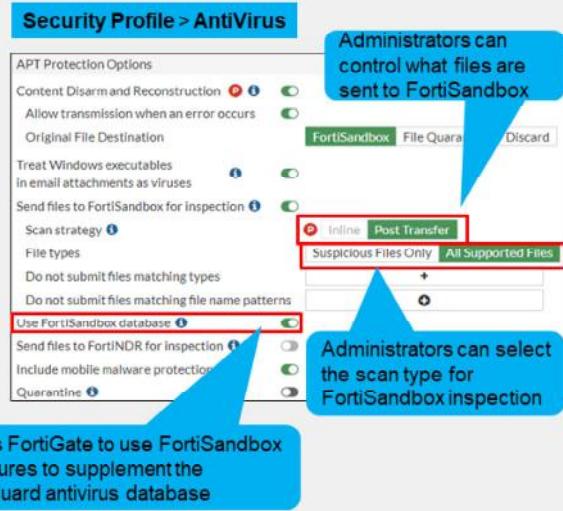
DO NOT REPRINT

© 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
 - Inline scanning is supported only in proxy based inspection and requires a FortiSandbox appliance running version 4.2 or later
 - To enable inline scanning (CLI only)

```
config system fortisandbox
  set inline-scan {enable | disable}
end
```



FortiOS is smart when it comes to determining what files are sent to FortiSandbox. One feature FortiOS uses for this is content disarm and reconstruction (CDR), a proxy-based feature that you will learn more about in this lesson. When CDR processes files, the original documents can be saved 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 antivirus database, to enhance their network security.

FortiSandbox inline scanning is supported only in proxy inspection mode. You will need to enable inline scanning under system fortisandbox settings and then select **Inline** in the antivirus profile. When the setting is enabled, the client's file is held by FortiSandbox for inspection, and an appropriate configured action is applied once a verdict is returned. Inline scanning is not supported on FortiSandbox Cloud or FortiGate Cloud Sandbox.

DO NOT REPRINT

© FORTINET

Antivirus Signature Database

- Requires a subscription to FortiGuard AntiVirus

Product	Version
AntiVirus	Version 85.00712
AV Definitions	Version 6.00258
AV Engine	Version 6.00258
Mobile Malware	Version 85.00712

- 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
```

Scheduled updates allow you to configure scheduled updates at regular intervals, such as hourly, daily, weekly, or automatically within every hour. You can also enable **AntiVirus PUP/PUA**, which allows antivirus grayware checks for potentially unwanted programs and applications.

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
```



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.

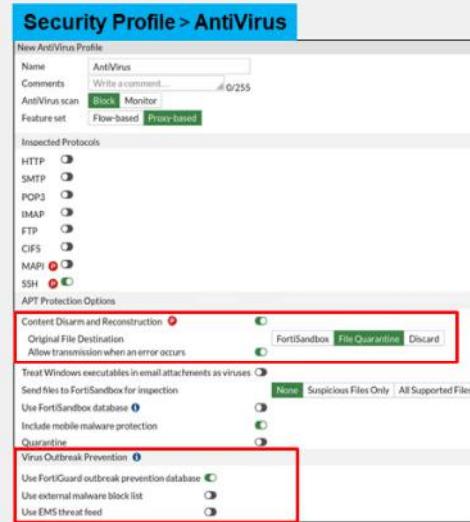
The extreme database is intended for use in high-security environments. The extreme database detects all known viruses, including viruses targeted at legacy operating systems that are no longer widely used. Most FortiGate models support the extreme database.

DO NOT REPRINT

© FORTINET

FortiGuard Protection Services

- CDR
 - 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



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, and then sends the original file to FortiSandbox for inspection. The client can download the original file by logging in to FortiSandbox.

Virus outbreak prevention: This 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 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 hash list can be in the form of MD5, SHA1, and SHA256 hashes, and is 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 AI scans are enabled, in what order are they performed?
 - A. AI scan, followed by grayware scan, followed by antivirus scan
 - B. Antivirus scan, followed by grayware scan, followed by AI scan

2. Which databases can be manually selected for use in antivirus scanning?
 - A. Extended and Extreme
 - B. Quick, Normal, and Extreme

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
 - 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

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: 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 (None, Suspicious Files Only, All Supported Files)

Send files to FortiSandbox for inspection: (None, Suspicious Files Only, All Supported Files)

Use FortiSandbox database: (None, Suspicious Files Only, All Supported Files)

Include mobile malware protection: (None, Suspicious Files Only, All Supported Files)

Quarantine: (None, Suspicious Files Only, All Supported Files)

Virus Outbreak Prevention: (None, Suspicious Files Only, All Supported Files)

Use FortiGuard outbreak prevention database: (None, Suspicious Files Only, All Supported Files)

Use external malware block list: (None, Suspicious Files Only, All Supported Files)

Use EMS threat feed: (None, Suspicious Files Only, All Supported Files)

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).

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.

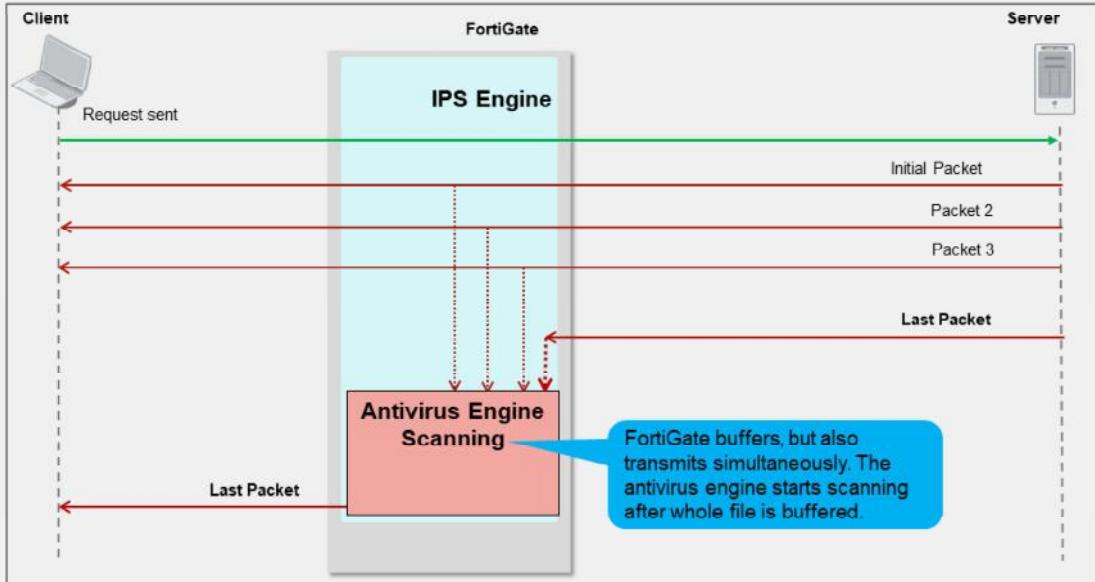
In flow-based inspection mode, the IPS engine reads the payload of each packet, caches a local copy, and forwards the packet to the receiver at the same time. Because the file is transmitted simultaneously, flow-based mode consumes more CPU cycles than proxy-based. However, depending on the FortiGate 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
Training Institute

© Fortinet Inc. All Rights Reserved.

14

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**

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 a block message immediately if a virus is detected
- Stream-based scanning supports FTP, SFTP, and SCP
 - Optimizes memory utilization for large archive files by decompressing and scanning them on the fly
 - Viruses are detected even if they are in the middle or end of the large files



© Fortinet Inc. All Rights Reserved.

15

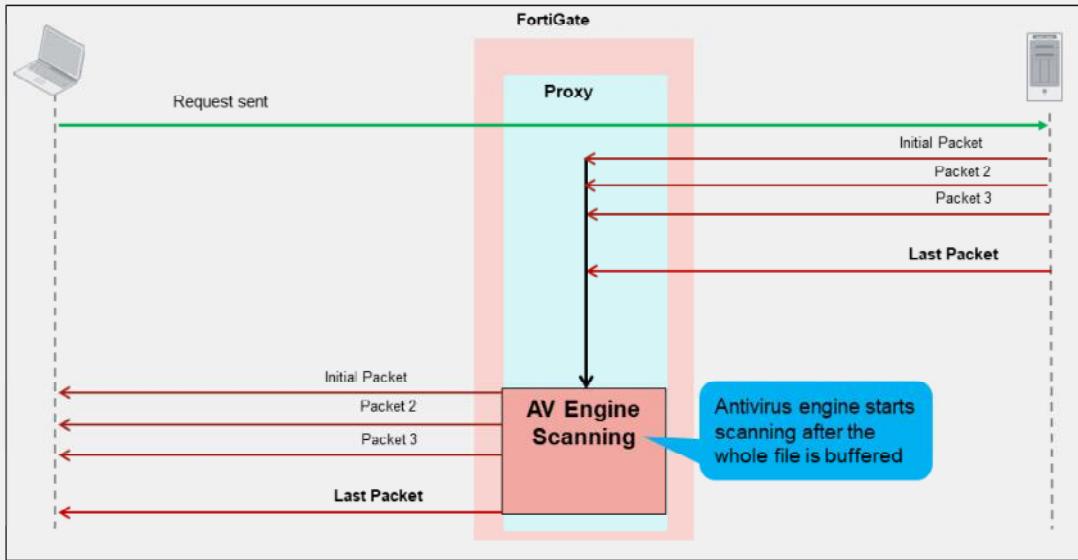
Each protocol's proxy picks up a connection and buffers the entire file first (or waits until the oversize limit is reached) before scanning. The client must wait for the scanning to finish. If a virus is detected, the block replacement page is displayed immediately. Because FortiGate has to buffer the 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.

Using proxy inspection antivirus allow you to use the stream-based scanning, which is enabled by default. Stream-based scanning scans large archive files by decompressing the files and then scanning and extracting them at the same time. This process optimized memory utilization to conserve resources on FortiGate. Viruses are detected even if they are in the middle or towards the end of these large files.

DO NOT REPRINT
© FORTINET

Proxy Inspection Mode Packet Flow



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

16

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 and SSH protocols inspection
 - Content disarm and reconstruction (CDR)



- Proxy-based antivirus profiles
 - Only available if inspection mode is proxy-based
 - Can use flow-based antivirus profiles



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 and SSH protocols 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 to **Proxy-based**, it is only available when the firewall policy inspection mode is set to **Proxy-based**.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What three additional features of an antivirus profile are available in proxy-based inspection mode?
 A. MAPI, SSH, and CDR
 B. Full and quick

2. What antivirus database is limited to specific FortiGate models?
 A. Extended
 B. Extreme

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
- 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

Default inspection mode is flow. Inspection mode is now per policy.

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

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 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 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

New Protocol Options			
Name	protocol_profile		
Comments	0/255		
Log Oversized Files	<input type="checkbox"/>		
RPC over HTTP	<input type="checkbox"/>		
Protocol Port Mapping			
HTTP	<input type="radio"/> Any	<input type="radio"/> Specify	80
SMTP	<input type="radio"/> Any	<input type="radio"/> Specify	25
POP3	<input type="radio"/> Any	<input type="radio"/> Specify	110
IMAP	<input type="radio"/> Any	<input type="radio"/> Specify	143
FTP	<input type="radio"/> Any	<input type="radio"/> Specify	21,22,23
NNTP	<input type="radio"/> Any	<input type="radio"/> Specify	119
MAPI	<input type="checkbox"/> 135		
DNS	<input type="checkbox"/> 53		
CIFS	<input type="checkbox"/> 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 type="checkbox"/>		
Append Signature (SMTP)	<input type="checkbox"/>		

You can specify more than one port number (separated by comma)

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.

You can configure protocol options on the **Protocol 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
```

- You can enable logging of oversize files using CLI

```
config firewall profile-protocol-options
edit <profile_name>
set oversize-log {enable|disable}
end
```

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, LSH, 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!

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

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



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.

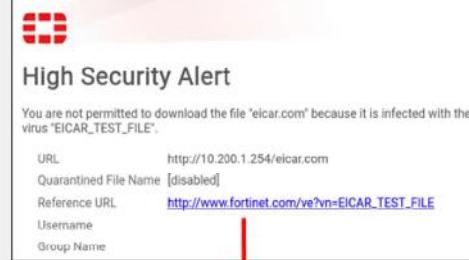
For these reasons, full SSL inspection level is the only choice that allows antivirus to be effective.

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



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:

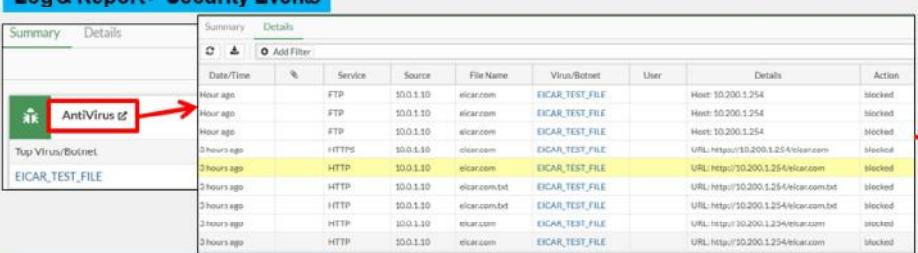
- File name
- Virus name
- Website host and URL
- User name and group (if authentication is enabled)
- Link to FortiGuard Encyclopedia—which provides analysis, recommended actions (if any), and detection availability

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

Antivirus Logs



Log & Report > Security Events

Summary	Details
	Hour ago Hour ago 3 hours ago 3 hours ago 3 hours ago 3 hours ago 3 hours ago 3 hours ago
	FTP 10.0.1.10 elcar.com EICAR_TEST_FILE Host: 10.200.1.254 blocked
	FTP 10.0.1.10 elcar.com EICAR_TEST_FILE Host: 10.200.1.254 blocked
	FTP 10.0.1.10 elcar.com EICAR_TEST_FILE Host: 10.200.1.254 blocked
	HTTPS 10.0.1.10 elcar.com EICAR_TEST_FILE URL: http://10.200.1.254/clean.com blocked
	HTTP 10.0.1.10 elcar.com EICAR_TEST_FILE URL: http://10.200.1.254/elcar.com blocked
	HTTP 10.0.1.10 elcar.com:80 elcar.com EICAR_TEST_FILE URL: http://10.200.1.254/elcar.com blocked
	HTTP 10.0.1.10 elcar.com:80 elcar.com EICAR_TEST_FILE URL: http://10.200.1.254/elcar.com blocked
	HTTP 10.0.1.10 elcar.com EICAR_TEST_FILE URL: http://10.200.1.254/elcar.com blocked
	HTTP 10.0.1.10 elcar.com EICAR_TEST_FILE URL: http://10.200.1.254/elcar.com blocked

Log & Report > Forward Traffic

Dest/Time	Source	Destination	Result	Policy ID	Action	Security Action	Log Details
9 minutes ago	10.0.1.10	10.200.3.1	✓ 1.32 kB/1.22 kB	Full_Access (S)	Accept: session close		
9 minutes ago	10.0.1.10	199.232.37.194 (cloudant-integrations.global.ssl.fastly.net)	✗ 1.32 kB/1.22 kB	Full_Access (S)	Deny: UTM Blocked	Full_Access (S) TCP reset from client	
9 minutes ago	10.0.1.10	89.236.73.97 (secure.elcar.org)	✗ 1.32 kB/1.22 kB	Full_Access (S)	Deny: UTM Blocked	Full_Access (S) TCP reset from server	
9 minutes ago	10.0.1.10	199.232.38.154 (www.vpnfastly.net)	✓ 1.35 kB/1.99 kB	Full_Access (S)	Accept		
9 minutes ago	10.0.1.10	151.501.129.188 (atdecision.com)	✓ 4.65 kB/29.58 kB	Full_Access (S)	Accept		
9 minutes ago	10.0.1.10	104.20.165.49 (privacyportal.elcar.com)	✓ 2.40 kB/3.60 kB	Full_Access (S)	Accept		
9 minutes ago	10.0.1.10	142.250.260.05 (www.gutenberg.org)	✓ 7.44 kB/143.10 kB	Full_Access (S)	Accept: session close		
9 minutes ago	10.0.1.10	10.200.3.1	✓ 1.52 kB/1.22 kB	Full_Access (S)	Accept: session close		
9 minutes ago	10.0.1.10	142.250.185.47 (fonts.googleapis.com)	✓ 3.68 kB/37.45 kB	Full_Access (S)	Accept: session close		
9 minutes ago	10.0.1.10	142.250.386.209 (font.googleapis.com)	✓ 2.02 kB/7.23 kB	Full_Access (S)	Accept		
9 minutes ago	10.0.1.10	142.250.185.47 (fonts.googleapis.com)	✓ 4.31 kB/1.01 kB	Full_Access (S)	Accept		

Log Details

General

Absolute Date/Time: 2022/04/13 19:28:24
Time: 19:28:24
Session ID: 1702
Virtual Domain: root
Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0

Source

IP: 10.0.1.10
Source Port: 56320
Country/Region: Reserved
Source Interface: port3
Source UUID: 703e6f6-791a-51e7-daa0-9859ce6c1d02

User

Destination

IP: 10.200.1.254
Port: 80
Country/Region: Reserved
Destination Interface: port1
Destination UUID: 7bc87d34-7916-51e7-3d5b-71812a61b98e
URL: http://10.200.1.254/elcar.com

Application Control

Protocol: 6
Service: HTTP

Data

File Name: elcar.com
Message: File is Infected.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

27

If you enable logging, you can find details on the **Antivirus** log page under **Security Events**.

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

DO NOT REPRINT

© FORTINET

Lesson Progress



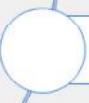
Antivirus Basics



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

The following are some best practices to follow when configuring antivirus scanning for use on FortiOS:

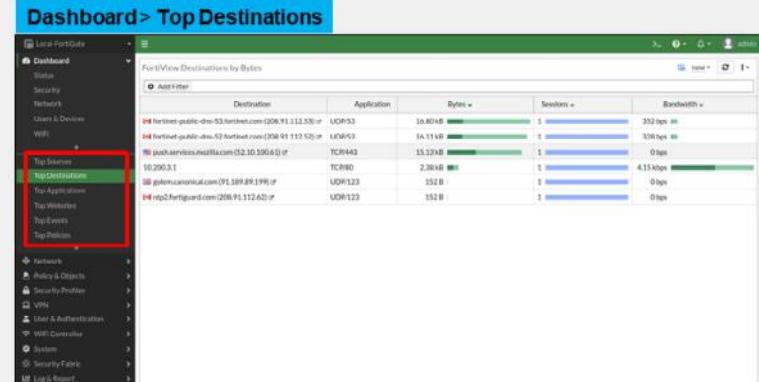
- Enable antivirus scanning on all internet traffic. This includes internal to external firewall policies, and any VIP firewall policies.
- Use *deep-inspection* instead of *certificate-based* inspection, to ensure that full content inspection is performed.
- Use FortiSandbox for protection against new 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

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



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.

33

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

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

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.

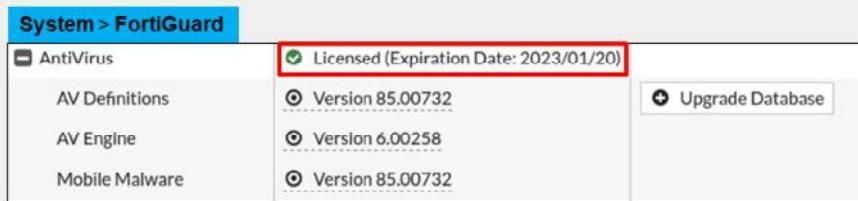
DO NOT REPRINT

© FORTINET

Troubleshooting Common Antivirus Issues

- 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



The screenshot shows the 'System > FortiGuard' interface. On the left, there is a sidebar with options: AntiVirus, AV Definitions, AV Engine, and Mobile Malware. The main panel displays the following information:

- Licensed (Expiration Date: 2023/01/20) (highlighted with a red box)
- Version 85.00732 (radio button selected)
- Version 6.00258 (radio button unselected)
- Version 85.00732 (radio button unselected)

On the right, there is a 'Upgrade Database' button.

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. You can perform the following to handle common antivirus issues:

- Make sure that FortiGate has a stable internet connection and can resolve DNS (update.fortinet.net).
- 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)

- 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
```

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.

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 SSL/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          Displays virus 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 FortiGuard server
```

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. You can verify them as following:

- 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

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

- ✓ 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
- ✓ 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



© Fortinet Inc. All Rights Reserved.

43

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

By mastering the objectives covered in this lesson, you learned how to use FortiGate features and functions to protect your network against viruses.

DO NOT REPRINT**© FORTINET**

FortiGate Security

Intrusion Prevention and Denial of Service



Last Modified: 13 June 2022

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



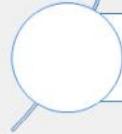
Intrusion Prevention System



Denial of Service



Best Practices



Troubleshooting

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

DO NOT REPRINT**© FORTINET**

Intrusion Prevention System

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 intrusion prevention systems (IPS), you should be able to implement an effective IPS solution to protect your network from intrusion.

DO NOT REPRINT**© FORTINET**

Exploits and Anomalies

Anomaly

- Can be zero-day or DoS attacks
- Detected by behavioral analysis:
 - Rate-based IPS signatures
 - DoS policies
 - Protocol constraints inspection
- Example:
 - Abnormally high rate of traffic (DoS/flood)

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

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.

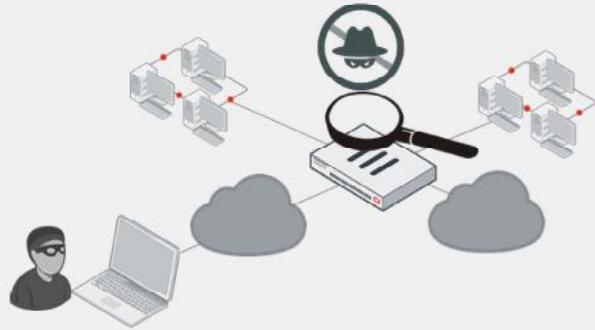
Exploits are known attacks, with known patterns that can be matched by IPS, web application firewall (WAF), or antivirus signatures.

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)



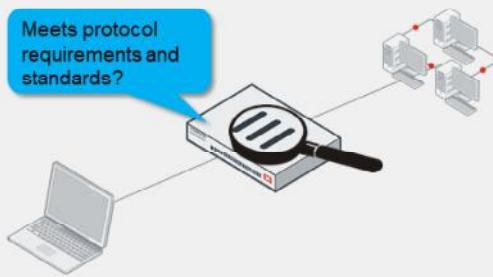
IPS on FortiGate uses signature databases to detect known attacks. Protocol decoders can also detect network errors and protocol anomalies.

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, and email filtering.

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**
Training Institute

© Fortinet Inc. All Rights Reserved.

6

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 on 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
- The default update setting is automatic, and the update interval is calculated based on the model and percentage of valid subscriptions
- The botnet signature subscription is part of a FortiGuard IPS license

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

7

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.

The 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 become increasingly ineffective the longer the signatures are not updated—old signatures won't defend against new attacks.

The default auto-update schedule for FortiGuard packages has been updated. Previously, the frequency was a reoccurring random interval within two hours. Starting in FortiOS 7.0, the frequency is automatic, and the update interval is calculated based on the model and percentage of valid subscriptions. The update interval is within one hour.

For example, an FG-501E has 78% valid contracts. Based on this device model, FortiOS calculates the update schedule to be every 10 minutes. You can verify the system event logs, which are generated approximately every 10 minutes.

IPS is a FortiGuard subscription, and includes a botnet signature database. The botnet IP database is part of the ISDB updates. The botnet domains database is part of the AV updates, and only the botnet signatures require the FortiGuard IPS license subscription.

DO NOT REPRINT**© FORTINET**

Choosing the Signature Database

- Regular
 - Common attacks with fast, certain identification (default action is block)
- Extended
 - Performance intensive



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

Security Profiles > Intrusion Prevention

IPS Signatures

View IPS Signatures

Default action

Active signature database

Name	Severity	Target	OS	Action	CVE-ID
2Wire.Wireless.Router.XSRF.Password.Reset	Server Client	Linux	Block	CVE-2007-4387	
3CX.Phone.System.VAD_Deploy.Arbitrary.File...	Server	Windows	Block	CVE-2005-0277	
3Com.3CDaemon.FTPServer.Buffer.Overflow	Server	Windows	Block	CVE-2005-0277	

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

9

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 wastes 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

The screenshot displays the FortiGate Management UI for configuring IPS Sensors. On the left, the 'New IPS Sensor' configuration page is shown, featuring fields for Name (set to 'IPS profile'), Comments (with placeholder 'Write a comment...'), and a 'Block malicious URLs' toggle. Below these are tabs for 'Details', 'Exempt IPs', 'Action', and 'Packet Logging', with the 'Details' tab currently selected. A red box highlights the '+ Create New' button. On the right, two overlapping windows show 'Add Signatures' lists. The top window, titled 'Signature', lists several signatures with checkboxes for 'Type', 'Action', 'Packet logging', and 'Status'. A red box highlights the 'Signature' button. The bottom window, also titled 'Add Signatures', lists a larger set of signatures with similar configuration options. A red box highlights the 'Signature' button in this window as well. Both windows include search and filter functions.

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

10

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 adds all the signatures that match the filters.

The purpose of the IPS feature is to protect the inside of the network from outside threats.

DO NOT REPRINT
© FORTINET

Configuring IPS Sensors (Contd)

- 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

Security Profiles > Intrusion Prevention

Add Signatures

Type: Signature
Action: Default
Packet logging: Enable
Status: Enable
Rate-based settings: Default
Threshold: 0
Duration (seconds): 60
Track By: Any
Exempt IPs: 0 | Edit IP Exemptions

These parameters are applicable to the signatures selected at the bottom

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 13.995	2Wire.Wireless.Router.XSRF.Password.Reset	Server	Linux	Block	CVE-2007-4387
	3CX.Phone.System.VAD_Deploy.Arbitrary.Fi...	Client		Block	
	3Com.3CDaemon.FTPServer.Buffer.Overflow...	Server	Windows	Block	CVE-2005-0277
	3Com.3CDaemon.FTPServer.Information.D...	Client	Windows	Block	CVE-2005-0278

Add All Results | Search | Selected | All | © Fortinet Inc. All Rights Reserved. | 11

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

Security Profiles > Intrusion Prevention

New IPS Sensor

Name: Server 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
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow 	0	<input checked="" type="radio"/> Monitor <input checked="" type="radio"/> Disabled <input checked="" type="radio"/> Default <input checked="" type="radio"/> Disabled	

© Fortinet Inc. All Rights Reserved. 12

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 allows 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 the FortiGate UI for configuring IP exemptions. The main window is titled "Security Profiles > Intrusion Prevention" and displays a table of IPS signatures. 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" dialog box. The "Edit IP Exemptions" dialog box shows 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".

Details	Exempt IPs	Action	Packet Logging
3Com.3CDaemon.FTP.Server.Information.Disclosure TGT Server SEV SEV OS Windows	1	Monitor Default	Disabled Disabled

Source IP/Netmask	Destination IP/Netmask
10.0.1.10/32	0.0.0.0/0

FORTINET
Training Institute

13

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

Signature	Severity	Target	OS	Action	CVE-ID
2Wire.Wireless.Router.XSRF.Password.Reset	Medium	Server Client	Linux	Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.File...	Medium	Server	Windows	Block	
3Com.3CDaemon.FTP.Server.Buffer.Overflow	Medium	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Dis...	Medium	Client	Windows	Block	CVE-2005-0278

FORTINET.
 Training Institute

© Fortinet Inc. All Rights Reserved.

14

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

IPS Signature Filter Options—CVE Pattern

- IPS signature filter options include CVE pattern
 - Allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard
 - For example, to configure CVE patterns for CVE-2010-0177
- For example, the CVE of the IPS signature Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution is CVE-2010-0177
- This matches the CVE filter in the IPS sensor, so traffic is blocked and logged

```
# config ips sensor
  edit "cve"
    set comment "cve"
    config entries
      edit 1
        set cve "cve-2010-0177"
        set status enable
        set log-packet enable
        set action block
      next
    end
  next
end
```

```
date=2022-04-13 time=15:44:56 logid="0419016384"
type="utm" subtype="ips" eventtype="signature"
level="alert" vd="vd1" eventtime=1594593896666145871
tz="-0700" severity="critical" srcip=10.1.100.22
srccountry="Reserved" dstip=172.16.200.55
srcintf="port2" srcintfrole="undefined"
dstintf="port1" dstintfrole="undefined"
sessionid=1638 action="dropped" proto=6
service="HTTPS" policyid=1
attack="Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution" srcport=58298 dstport=443
hostname="172.16.200.55" url="/Mozilla"
direction="incoming" attackid=20853 profile="sensor-1" ref="http://www.fortinet.com/ids/VID20853"
incidentserialno=124780667 msg="web client:
Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution
," crscore=50 craction=4096 crlevel="critical"
```

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

15

IPS signature filter options include the CVE pattern. The CVE pattern option allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.

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="radio"/> Block	<input type="radio"/> Disabled
SEV (Orange)			
SEV (Red)			
SEV (Grey)		<input checked="" type="radio"/> Default	<input type="radio"/> Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites Disable Block Monitor

FORTINET
 Training Institute

© 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

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Security Profiles' section, 'IPS' is selected and enabled. A tooltip says 'Add IPS sensors as security profiles to firewall policies'. In the 'Logging Options' section, 'Log Allowed Traffic' is set to 'Security Events' and 'Generate Logs when Session Starts' is enabled. A tooltip says 'Enable this option to log all sessions including blocked and allowed traffic'. The Fortinet Training Institute logo is in the bottom left, and the copyright notice '© Fortinet Inc. All Rights Reserved.' is at the bottom center. The page number '17' is in the bottom right.

Add IPS sensors as security profiles to firewall policies

IPS protect_client

Enable this option to log all sessions including blocked and allowed traffic

IPS protect_client

SSL deep-inspection

Security Events All Sessions

© 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 > Security Events

Date/Time	Severity	Source	Protocol	User	Action
2 seconds ago	6	10.200.1.254	6		dropped
2 seconds ago	6	10.200.1.254	6		detected
2 seconds ago	6	10.200.1.254	6		detected
2 seconds ago	6	10.200.1.254	6		detected
12 seconds ago	6	10.200.1.254	6		dropped
22 seconds ago	6	10.200.1.254	6		dropped
32 seconds ago	6	10.200.1.254	6		dropped
42 seconds ago	6	10.200.1.254	6		dropped
53 seconds ago	6	10.200.1.254	6		dropped
Minute ago	6	10.200.1.254	6		dropped

Log Details

General

Absolute Date/Time: 2022/04/21 22:44:13
Time: 22:44:13
Session ID: 10137
Virtual Domain: root
Agent: Mozilla/5.00 (Nikto/2.1.5) (Evasion:None) (Test:004131)

Source

IP: 10.200.1.254
Source Port: 42810
Country/Region: Reserved
Source Interface: port1
User:

If you enabled security events logging in the firewall policies that apply IPS, you can view events are logged on the **Security Events** pane on the **Log & Report** page. You can view the logs by clicking on **Intrusion Prevention**.

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 helps you develop action plans and focus on specific events, for example, patching a critical vulnerability.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which IPS action 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

DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Best Practices



Troubleshooting

Good job! You now understand the IPS on FortiGate.

Now, you will learn about DoS.

DO NOT REPRINT**© FORTINET**

Denial of Service

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.

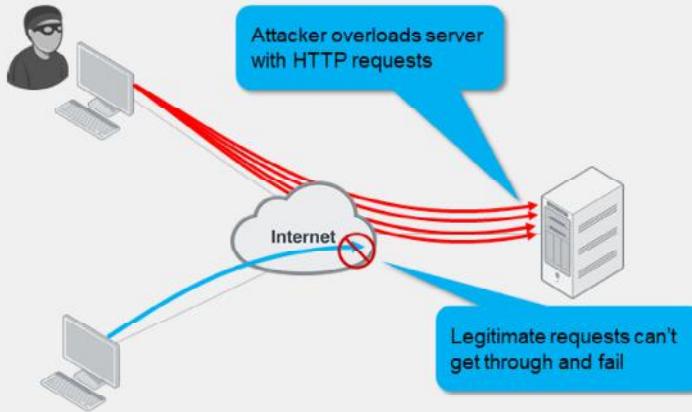
By demonstrating competence in Denial of Service (DoS), you should be able to protect your network from common DoS attacks.

DO NOT REPRINT

© FORTINET

DoS Attacks

- Attacker sessions consume all resources—RAM, CPU, port numbers
- Slows down or disables the target until it can't serve legitimate requests



So far, you have 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?

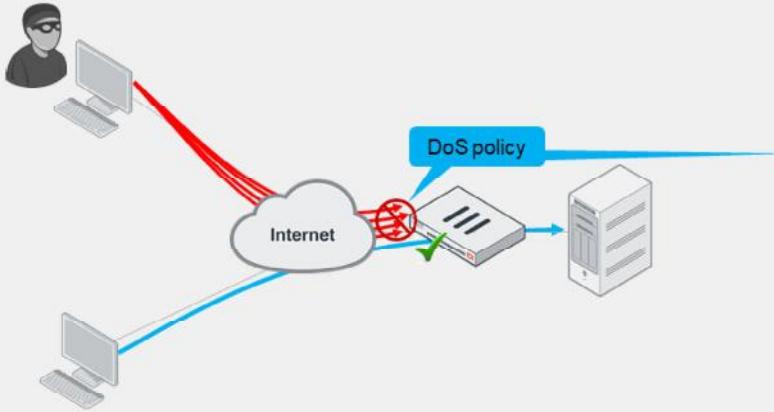
The goal of a DoS attack is to overwhelm the target—to consume resources until the target can't respond to legitimate traffic. There are many ways to accomplish this. High-bandwidth use is only one type of DoS attack. Many sophisticated DoS attacks, such as Slowloris, don't require high bandwidth.

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					
Name	Logging	Action	Disable	Block	Monitor
DoS_Policy		Disable			
Intalling Interface		port1			
Source Address		all	*		
Destination Address		all	*		
Service		ALL	*		

L3 Anomalies					
Name	Logging	Action	Disable	Block	Monitor
ip_src_session		Disable	Block	Monitor	5000
ip_dst_session		Disable	Block	Monitor	5000

L4 Anomalies					
Name	Logging	Action	Disable	Block	Monitor
tcp_syn_flood		Disable	Block	Monitor	2000
tcp_port_scan		Disable	Block	Monitor	1000
tcp_src_session		Disable	Block	Monitor	5000
tcp_dst_session		Disable	Block	Monitor	5000
udp_flood		Disable	Block	Monitor	2000
udp_scan		Disable	Block	Monitor	2000
udp_src_session		Disable	Block	Monitor	5000
udp_dst_session		Disable	Block	Monitor	5000

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

23

To block DoS attacks, apply a DoS policy on a FortiGate 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

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. Legitimate clients 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 is full. Once the server's table is full, it can't accept more connections and begins to ignore all new clients.

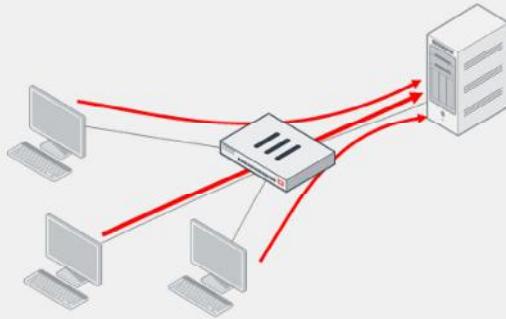
ICMP is used during troubleshooting: devices respond with success or error messages. However, attackers can use ICMP to probe a network for valid routes and responsive hosts. By doing an ICMP sweep, the attacker can gain information about your network before crafting more serious exploits.

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 (Contd)

- **Distributed DoS**
 - Many of the same characteristics of an individual DoS attack
 - However, attack originates from multiple sources



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

Name	Logging	Action	Disable	Block	Monitor	Threshold
ip_src_session	On	Disable	Block	Monitor	5000	
ip_dst_session	On	Disable	Block	Monitor	5000	

Name	Logging	Action	Disable	Block	Monitor	Threshold
tcp_syn_flood	On	Disable	Block	Monitor	2000	
tcp_port_scan	On	Disable	Block	Monitor	1000	
tcp_src_session	On	Disable	Block	Monitor	5000	
tcp_dst_session	On	Disable	Block	Monitor	5000	
udp_flood	On	Disable	Block	Monitor	2000	
udp_scan	On	Disable	Block	Monitor	2000	

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

26

You can apply DoS protection to four protocols: TCP, UDP, ICMP, and SCTP. And, you can apply four different types of anomaly detection protocols:

- 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 ports respond and, therefore, might be vulnerable.
- Source signatures look for large volumes of traffic originating from a single IP address.
- Destination signatures look for large volumes of traffic destined for a single IP address.

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 thresholds 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 DoS anomaly sensor can be used to detect and block the probing attempts of a port scanner?
 - A. `tcp_syn_flood`
 - B. `tcp_port_scan`

2. Which behavior 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

DO NOT REPRINT**© FORTINET**

Lesson Progress



Intrusion Prevention System



Denial of Service



Best Practices



Troubleshooting

Good job! You now understand how to protect your network from DoS attacks 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 is 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.

30

Before you implement IPS, you must analyze the needs of your network. Enabling the default profiles across all policies quickly causes issues, the least of which are false positives. Performing unnecessary inspections on all network traffic can cause high resource utilization, which can hamper the ability of FortiGate 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 makes sure that FortiGate is not scanning traffic with irrelevant signatures.

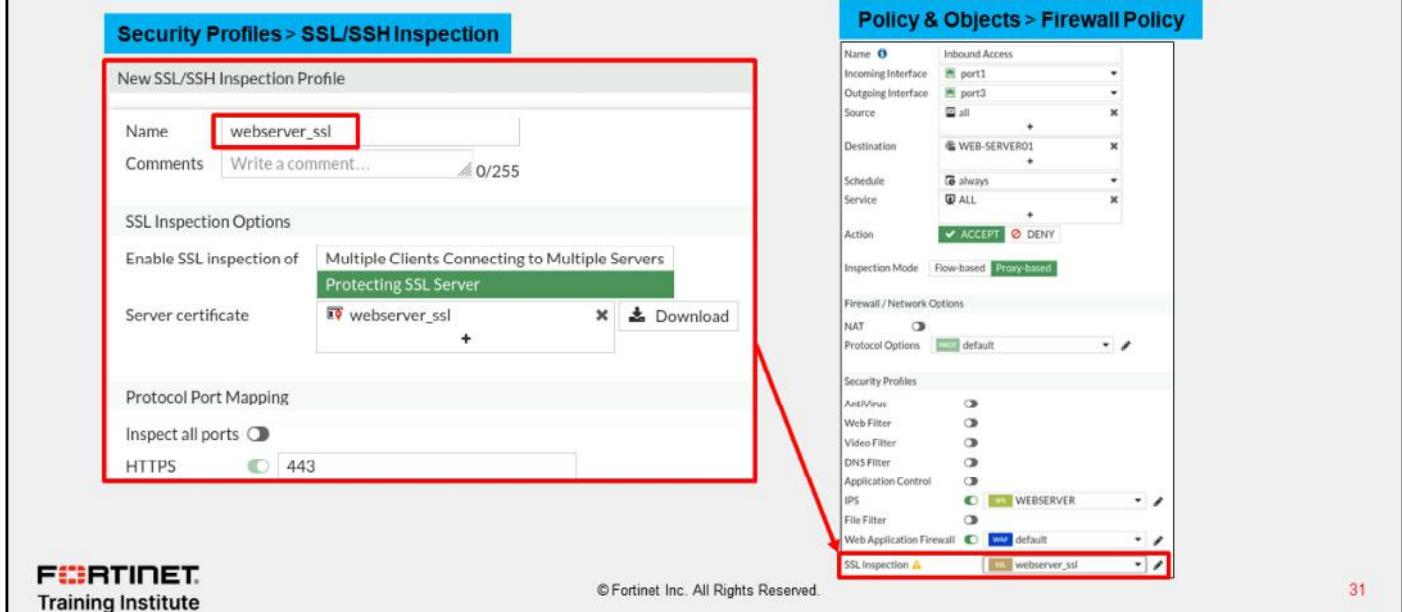
Lastly, IPS is not a *set-and-forget* implementation. You must monitor logs regularly for anomalous traffic patterns, and adjust your IPS profile configuration based on your observations. You should also audit your internal resources regularly to identify if certain vulnerabilities still apply to your organization.

DO NOT REPRINT

© FORTINET

Full SSL Inspection

- Enable a full SSL inspection profile to ensure you're inspecting encrypted traffic



The image shows two screenshots of the FortiGate management interface. The left screenshot is titled 'Security Profiles > SSL/SSH Inspection' and shows the configuration of a new SSL inspection profile named 'webserver_ssl'. It includes fields for 'Name' (webserver_ssl), 'Comments' (Write a comment...), 'SSL Inspection Options' (Enable SSL inspection of 'Multiple Clients Connecting to Multiple Servers' and 'Protecting SSL Server'), 'Server certificate' (selected 'webserver_ssl'), and 'Protocol Port Mapping' (HTTPS port 443). The right screenshot is titled 'Policy & Objects > Firewall Policy' and shows a policy rule. The 'Inbound Access' section lists 'port1', 'port3', and 'all'. The 'Destination' section lists 'WEB-SERVER01'. The 'Action' section shows 'ACCEPT' is selected. In the 'Security Profiles' section, the 'SSL Inspection' profile is assigned to the policy. A red arrow points from the 'SSL Inspection' profile in the left screenshot to the 'SSL Inspection' profile in the right screenshot.

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, can apply IPS and WAF inspection on encrypted traffic reliably, because FortiGate can 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 the 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 with 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 on devices with two or more CP8s or one or more CP9s

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, 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, 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. SoC4

2. Which feature 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



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 on GUI

- Enable real-time debug on CLI

```
# diagnose debug application update -1
# diagnose debug enable
# execute update-now
```

After enabling real-time debugging, force a manual update of all FortiGuard packages

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 on 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 port443. Any intermediary devices performing SSL inspection on this traffic can also cause issues with updates.

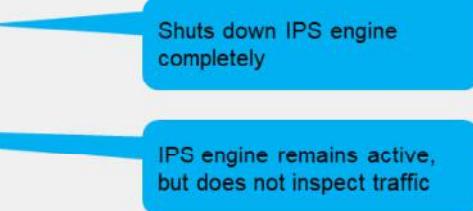
Finally, you can use the FortiGuard update debug to monitor update events in real time.

DO NOT REPRINT**© FORTINET**

IPS and High-CPU Use

```
# diagnose test application ipsmonitor <Integer>

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
```



Short spikes in CPU usage by IPS processes can 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. You can use the command shown on this slide, along with displayed options, 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, which you must report to Fortinet Support. You can disable the IPS engine completely using option 2. If you want 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=2021-04-21 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!

IPS goes into fail-open mode when there is not enough available memory in the IPS socket buffer for new packets. What happens during this 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 are dropped.

Frequent IPS fail open events usually indicate that IPS can't 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**

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 pass through without inspection
 B. New packets are dropped

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Intrusion Prevention System****Denial of Service****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 the IPS implementation methodology
- ✓ Troubleshoot common IPS issues

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

By mastering the objectives covered in this lesson, you gained the skills and knowledge you need to configure, maintain, and troubleshoot the FortiGate IPS solution.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Security

Security Fabric

FortiOS 7.2

Last Modified: 23 August 2022

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.

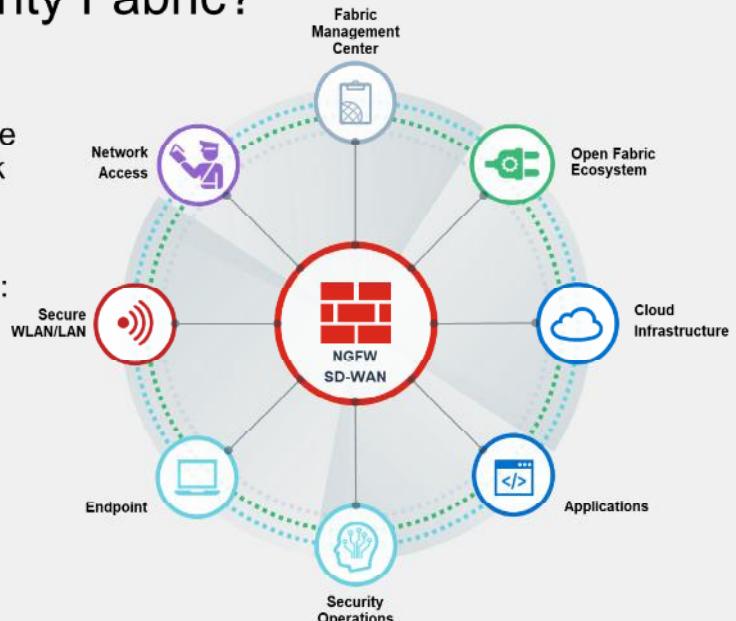
By demonstrating competence in understanding key concepts of the Fortinet Security Fabric, you will better understand the value of the Security Fabric, the servers that comprise it, and how to deploy it.

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



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

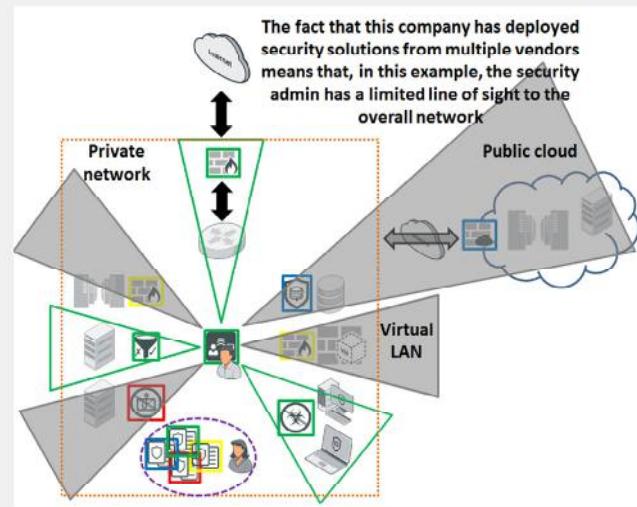
A fourth attribute could be added to this description of the Security Fabric: *open*. The API and protocol are available for other vendors to join and for partner integration. This allows for communication between Fortinet and third-party devices.

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



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. Often, these piecemeal solutions were effective, but deploying products using different standards and protocols 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 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
Training Institute

© Fortinet Inc. All Rights Reserved.

6

As shown on this slide, the Fortinet Security Fabric offers eight solutions: network access, security, 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, SD-WAN. It also offers multi-cloud strategy across public clouds, private clouds, hybrid clouds, and software as a service (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, secure access across distributed enterprises and SD-WAN environments, advanced threat protection, management and analytics, and security information and event management (SIEM).

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

DO NOT REPRINT**© FORTINET**

Devices That Comprise the Security Fabric



- **Core:**
 - Minimum of two FortiGate devices: one root, and one or more downstream
 - At least one of: FortiAnalyzer, FortiAnalyzer Cloud, or FortiGate Cloud
- **Recommended**—Adds significant visibility or control:
 - FortiManager, FortiAP, FortiSwitch, FortiClient, FortiClient EMS, FortiSandbox, FortiMail, FortiWeb, FortiNDR, FortiDeceptor
- **Extended**—Integrates with fabric, but may not apply to everyone:
 - Other Fortinet products and third-party products using the API

You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode.

To add more visibility and control, Fortinet recommends adding FortiManager, FortiAP, FortiClient, FortiClient EMS, FortiSandbox, FortiMail, FortiWeb, FortiNDR, FortiDeceptor, and FortiSwitch.

The solution can be extended by adding other network security devices, including several third-party products.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the Fortinet Security Fabric?

- A. A Fortinet solution that enables communication and visibility among devices of your network
- B. A device that can manage all your firewalls

2. Which 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

DO NOT REPRINT

© FORTINET

Lesson Progress



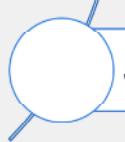
Introduction to the Fortinet Security Fabric



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

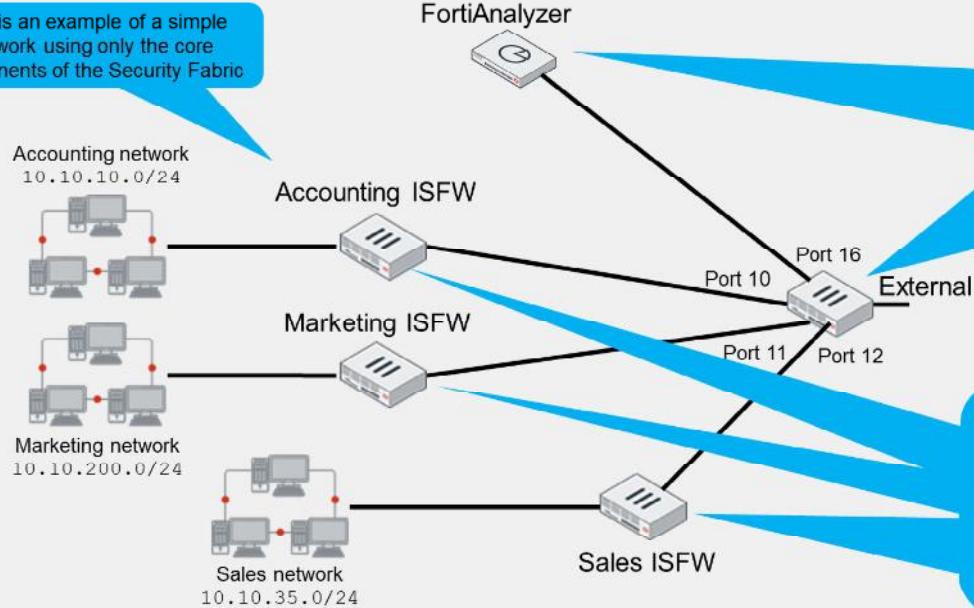
After completing this section, you should be able to achieve the objectives shown on this slide.

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?

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



There is a FortiAnalyzer and one next-generation firewall (NGFW). This FortiGate is 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
 Training Institute

© Fortinet Inc. All Rights Reserved.

11

This simple network that comprises only the core devices of a Security Fabric includes one FortiAnalyzer and four next-generation firewall (NGFW) FortiGate devices.

The FortiGate device named External is acting as the edge firewall and is configured as the *root* firewall within the Security Fabric.

Downstream from the root firewall, three internal segmentation firewalls compartmentalize the WAN in order to contain breaches and to control access to various LANs. This example uses Accounting, Marketing, and Sales LANs.

DO NOT REPRINT**© FORTINET**

General Steps to Configure the Security Fabric

- On the root FortiGate:
 - Enable **Security Fabric Connection** on the required interfaces
 - Enable **Security Fabric** connector and select **Serve as Fabric Root**
 - Configure FortiAnalyzer or cloud logging. You can configure FortiAnalyzer in advance
 - (Optional) Preauthorize downstream devices
- On the downstream devices
 - Enable **Security Fabric Connection** on the required interfaces
 - Enable **Security Fabric Connection** and select **Join Existing Fabric**
 - Specify the IP address of the root device
- On the root FortiGate:
 - Authorize all downstream devices

To configure a new security fabric, follow these general steps:

First, on the root FortiGate, you must enable **Security Fabric Connection** on the interfaces that face any downstream FortiGate. Then, enable the Security Fabric connector, and select **Serve as Fabric Root**. You also need to configure FortiAnalyzer or a cloud logging solution. This logging configuration will be pushed to all the downstream FortiGate devices.

Optionally, you can preauthorize your downstream devices by adding their serial numbers. 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.

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 third step in implementing the Security Fabric is to authorize the downstream FortiGate devices on the root FortiGate.

DO NOT REPRINT
© FORTINET

Synchronizing Objects Across the Security Fabric

- By default, object synchronization is enabled in fabric settings

```
config system csf
set status enable
set configuration-sync default
set fabric-object-unification default
end
```

- If `set fabric-object-unification` is set to `local` on the root FortiGate device, global fabric objects are not synchronized to downstream FortiGate devices

```
config system csf
set status enable
set group-name "fortinet"
set fabric-object-unification local
```

- If `set configuration-sync` is set to `local`, the downstream device does not participate in synchronization

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

- Select per object option to synchronize or not on the root FortiGate

- If this option is disabled (default configuration), objects created on the root FortiGate are kept as local objects that are not synchronized to downstream FortiGate devices



© Fortinet Inc. All Rights Reserved.

13

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

Synchronization always happens from the root FortiGate to downstream FortiGate devices. Any object that can be synced will be available on downstream FortiGate devices after synchronization.

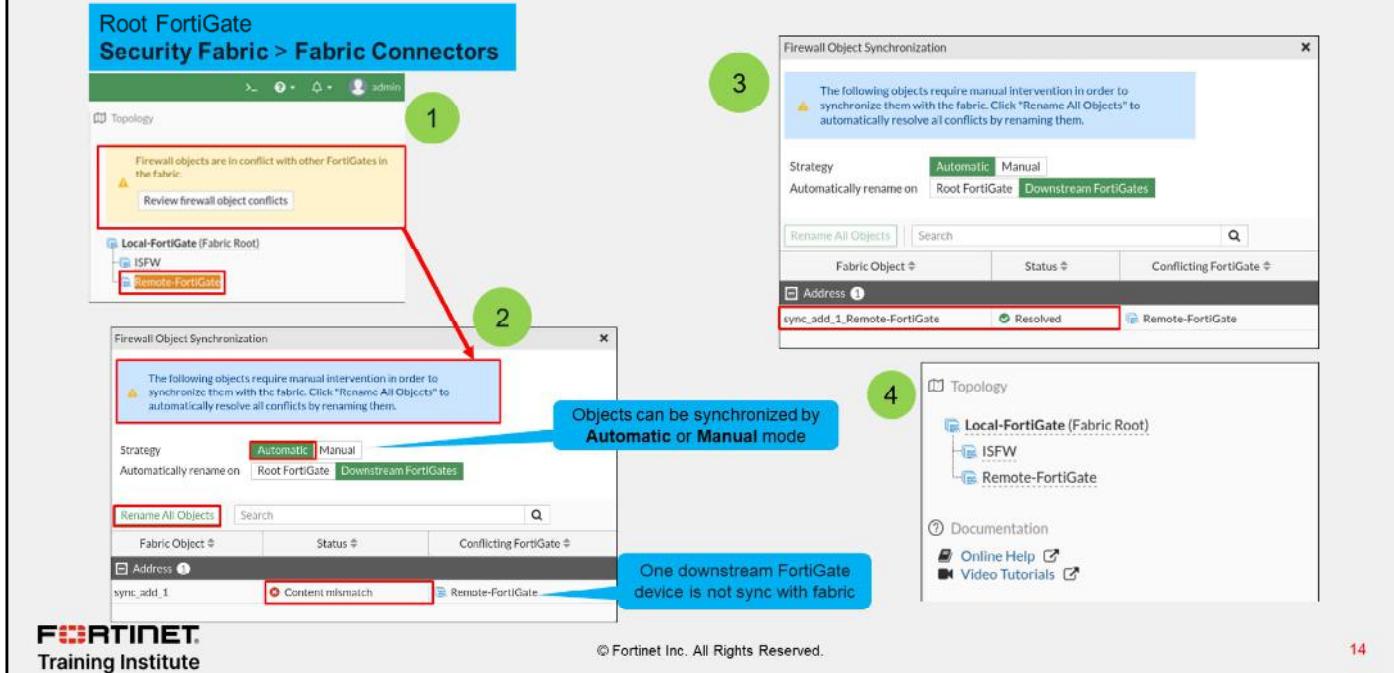
The CLI command `set fabric-object-unification` is only available on the root FortiGate. When set to `local`, global objects will not be synchronized to downstream devices in the Security Fabric. The default value is `default`.

The CLI command `set configuration-sync local` is used when a downstream FortiGate doesn't need to participate in object synchronization. When set to `local` on a downstream FortiGate, the device does not synchronize objects from the root, but will still participate in sending the synchronized object downstream.

You can also enable or disable per object synchronization in the Security Fabric. This option is not available for objects you create on a downstream FortiGate. Fabric synchronization is disabled by default for supported fabric objects, and these fabric objects are kept as locally created objects on all the FortiGate devices in the Security Fabric. If object synchronization is disabled on the root FortiGate, using the command `set fabric-object disable`, firewall addresses and address groups will not be synchronized to downstream FortiGate devices.

DO NOT REPRINT
© FORTINET

Synchronizing Objects Across the Security Fabric (Contd)



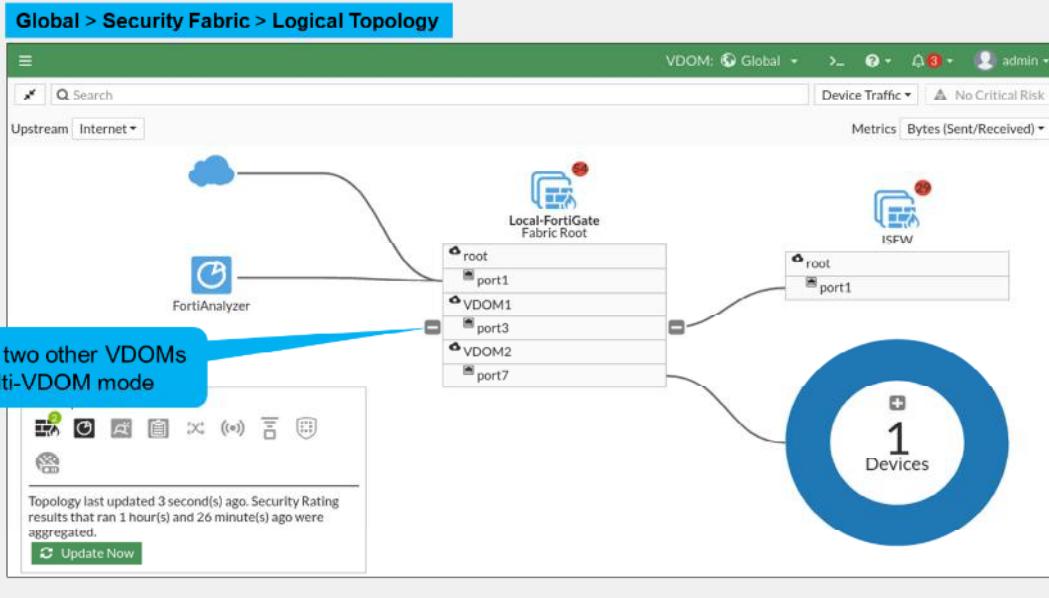
If an object conflict occurs during synchronization, you'll get a notification in the topology tree.

The process to resolve a syncing conflict is as follows:

1. The notification icon displays this message: **Firewall objects are in conflict with other FortiGates in the fabric. Remote-FortiGate** is highlighted in amber. Click **Review firewall object conflicts**.
2. On the **Firewall Object Synchronization** page, you can see that both the root FortiGate and downstream FortiGate devices contain the **syncn_add_1** object (with a different IP address/subnet schema on each device), causing a status of **Content mismatch**. 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**.
3. **Remote-FortiGate** is appended to the name of the downstream FortiGate device **sync_Add_1** address object and the status changes to **Resolved**.
4. In the topology tree, none of the FortiGate devices are highlighted because there is no conflict.

DO NOT REPRINT
© FORTINET

Multi-VDOM in the Security Fabric



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

15

When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. *Only* the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable **Device Detection** on ports you want to have displayed in the **Security Fabric**. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single **Security Fabric**. In the example shown on this slide, the Local-FortiGate is configured in multi-VDOM mode, and has three VDOMs (root, VDOM1, and VDOM2), each with ports that have connected devices.

DO NOT REPRINT

© FORTINET

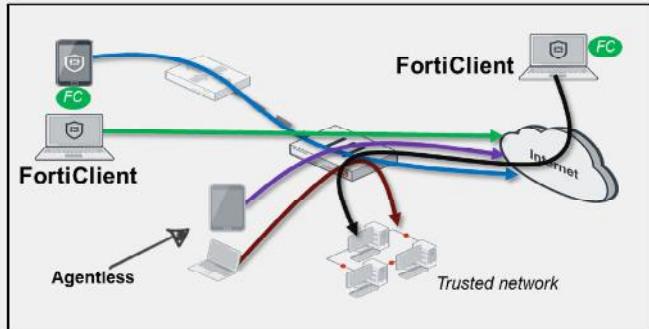
Device Identification—Agentless vs. Agent

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



Device identification is an important component in the Security Fabric. FortiGate detects most of the third-party devices in your network and add 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).

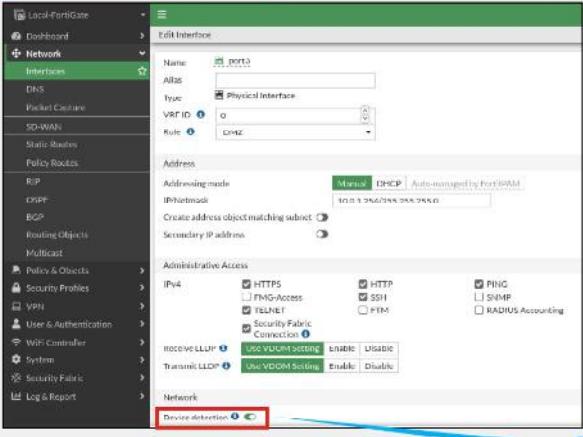
DO NOT REPRINT

© FORTINET

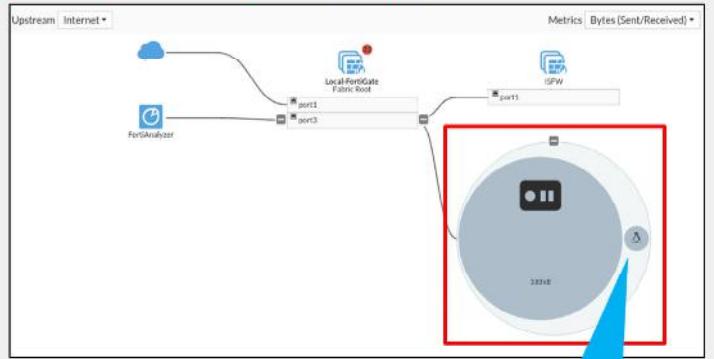
Device Identification

Enable **Device Detection** on interface(s)

Network > Interfaces



Security Fabric > Logical Topology



Enable Device Detection

Ubuntu machine detected upon traffic from the PC to the FortiGate

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

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

FortiGate Security 7.2 Study Guide

438

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

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 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
- 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 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
 - FortiWeb
- FortiClient integration
 - FortiClient
 - FortiClient EMS
- Advanced threat protection integration
 - FortiSandbox
- Access device integration
 - FortiAP
 - FortiSwitch
- AI-driven breach protection
 - FortiNDR
- Advanced Threat Deception
 - FortiDeceptor
- Other optional devices
 - FortiADC
 - FortiDDoS
 - FortiWLC
 - FortiAuthenticator
 - FortiSIEM
 - FortiCache
 - FortiToken



© Fortinet Inc. All Rights Reserved.

21

The slide shows the list of products that Fortinet recommends to extend the Security Fabric.

For example, Fortinet recommends using a FortiManager for centralized management of all FortiGate devices and to access devices in the Security Fabric. You can also extend the Security Fabric down to the access layer by integrating FortiSwitch and FortiAP devices.

DO NOT REPRINT

© FORTINET

Automation Stitches

AUTOMATION STITCHES



- Consist of a trigger and one or more configurable actions
- Can be created only on the root FortiGate in the Security Fabric
- Are available as predefined stitches, or you can create custom ones
- Can run actions sequentially or in parallel
- Some actions include a minimum **Minimum interval** setting to make sure they don't run more often than needed

The screenshot shows the 'Security Fabric > Automation' interface. On the left, a dialog box titled 'Create New Automation Stitch' is open, showing fields for 'Name' (disabled), 'Status' (All FortiGates), 'Action execution' (Sequential), and a 'Stitch' section with 'Add Trigger' and 'Add Action' buttons. To the right is a list of 'Select Entries' with a '+ Create' button, containing items like 'Compromised Host', 'FortiAnalyzer Connection Down', and 'Network Down'. Below the list are three cards: 'Compromised Host', 'FortiAnalyzer Event Handler', and 'Fabric Connector Event'. At the bottom is a 'Security response' section with four cards: 'Access Layer Quarantine', 'FortiClient Quarantine', 'FortINAC Quarantine', and 'IP Ban'.

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

22

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

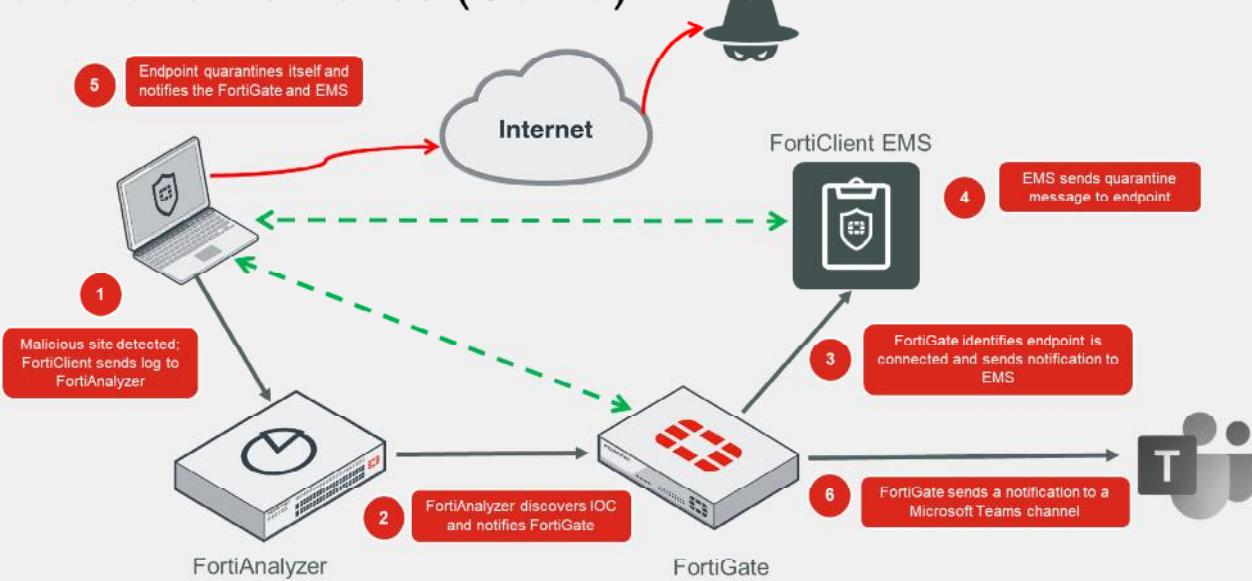
Each automation stitch pairs a trigger and one or more actions. FortiOS has several predefined stitches, triggers and actions. However, you can create custom automation based on the available options.

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 interval (seconds)** setting on some of the available actions to make sure they don't run more often than needed.

DO NOT REPRINT
© FORTINET

Automation Stitches (Contd)



This slide shows an example of how automation stitches can be configured to work in the Security Fabric:

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

DO NOT REPRINT

© FORTINET

External Connectors

- Security Fabric multi-cloud support adds external connectors to the Security Fabric configuration
- Allow you to integrate, among others:
 - Amazon Web Services (AWS)
 - Microsoft Azure
 - Oracle Cloud Infrastructure (OCI)
 - Google Cloud Platform (GCP)

New External Connector

Public SDN

Amazon Web Services (AWS)

Connector Settings

Name: AWS

Status: Enabled

Update interval: Use Default

AWS Connector

Access key ID: AKIxxxxxxxxxxxx

Secret access key: [REDACTED]

Region name: US-East

VPC ID: vpc-e315g651

External connectors allow you to integrate multi-cloud support, such as Microsoft Azure and AWS, among others.

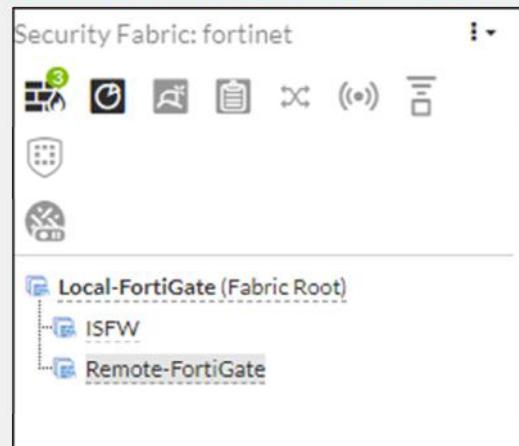
In an application-centric infrastructure (ACI), the SDN connector serves as a gateway bridging SDN controllers and FortiGate devices. For example, the SDN connector can register itself to APIC in the Cisco ACI fabric, polls objects of interest, and translates them into address objects. The translated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

DO NOT REPRINT**© FORTINET**

The Security Fabric Status Widget

- The name of your Security Fabric
- Icons indicating the other devices in the Security Fabric
- The names of the FortiGate devices in the Security Fabric

Dashboard > Status > Security Fabric widget



The **Security Fabric Status** widget shows a visual summary of the devices in the Security Fabric.

You can hover over the icons at the top of the widget to display a quick view of their statuses. From here, 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 not configured, or not detected in your network.
- Devices in red are no longer connected, or not authorized in your network.

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 Fortinet Security rating service
- Understand the differences 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 a report of itemized results and compliance recommendations
- In multi-VDOM mode, reports can be generated in the Global VDOM for all the VDOMs



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

29

Security rating is a subscription service that requires a security rating license. This service 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**, and **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 subcategories. Click a scorecard to drill down to a detailed report of itemized results and compliance recommendations. The point score represents all passed and failed items in that area. The report includes the security controls that were tested, linking them to specific FSBP or PCI compliance policies. You can click **FSBP** and **PCI** to reference the corresponding standard.

In multi-VDOM mode, administrators with read/write access can generate security rating reports in the Global VDOM for all the VDOMs on the device. Administrators with read-only access can view the report, but not generate it.

On the scorecards, the **Scope** column shows the VDOM or VDOMs that the security rating checked. On checks that support **Easy Apply**, you can run the remediation on all the associated VDOMs.

The security rating event log is available on the root VDOM.

DO NOT REPRINT

© FORTINET

Security Posture

The screenshot shows the Fortinet Security Fabric interface with the following details:

- Scorecard:** A circular chart showing a grade of **C** with a score of **-416.04**. A callout text states: "The **Security Rating Score** helps you to identify the security issues in your network and to prioritize your tasks".
- Audit Results:** A table titled "Failed" showing audit findings across various devices and protocols. Key findings include:
 - Unsecure Protocol - HTTP: Interfaces currently in use should not allow HTTP administrative interfaces.
 - Log Capacity Management (Local Device): Local device log settings should be configured to support the.
- Details Panel:** Shows the score of **-416.04**, last run time, endpoints (11), and trends (High: 65, Change: -740.06%).
- Callout Text:** "Security issues that are labelled **EZ** can be resolved immediately".
- Callout Text:** "Identifies critical security gaps".

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

30

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

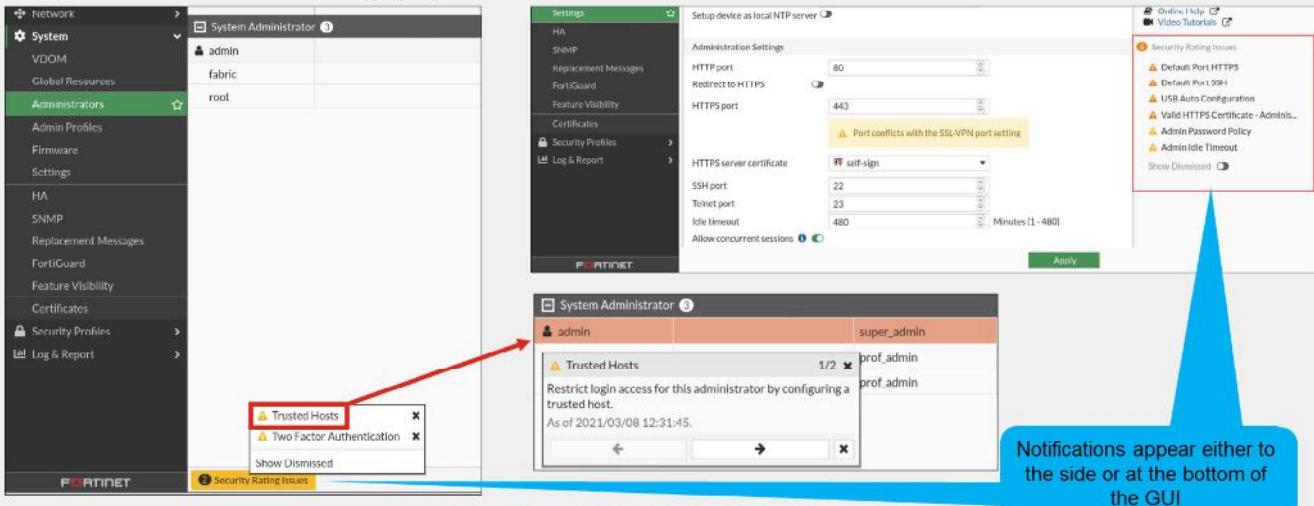
The security posture service now supports the following:

- 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 in to 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

Security Rating Notifications

- Display recommendations determined by security rating
- Appear on various setting pages



Notifications appear either to the side or at the bottom of the GUI

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

31

Security rating provides recommendations and highlights issues with the configuration of the FortiGate settings. These recommendations and issues appear as notifications on the **Settings** page.

Click a notification to display the page where the setting needs to be fixed. This prevents you from having to go back and forth between the **Security Fabric > Security Rating** page and the various settings pages.

Notifications appear either to the side or at the bottom of the GUI. You can also dismiss the notifications.

In the example shown on this slide, some of the issues found are that FortiGate is using the default HTTPS and SSH ports, and that the administrator password policy is not enabled. The security rating check also recommends that you configure trusted hosts and two-factor authentication.

DO NOT REPRINT**© FORTINET**

Security Rating Check Schedule

- Security checks by default are scheduled to run automatically every 4 hours
- Enable or disable security checks using the CLI:

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

- Manually run a rating check using the CLI:

```
#diagnose report-runner trigger
```



© Fortinet Inc. All Rights Reserved.

32

Security rating checks by default are scheduled to run automatically every four hours.

Use the following commands to enable or disable security checks using the CLI:

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

Use the following command to manually run a rating check using the CLI:

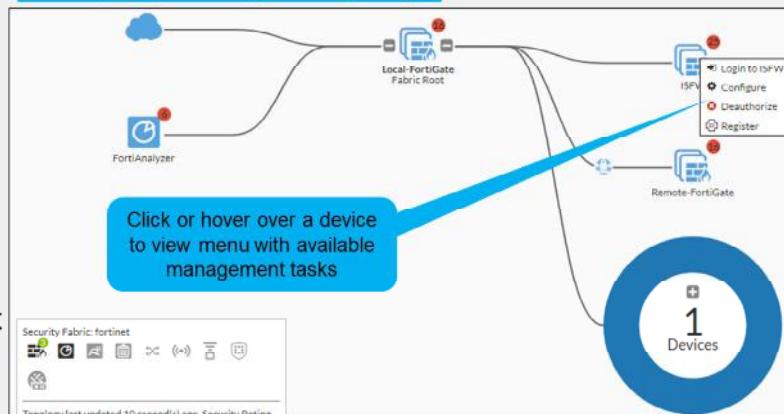
```
#diagnose report-runner trigger
```

DO NOT REPRINT
© FORTINET

Topology Views

- Some device management tasks:
 - Login
 - Configure devices
 - Authorize or deauthorize devices
 - Register devices
 - Ban compromised clients
 - Quarantine hosts
 - Create address objects
- Full view available only at the root FortiGate

Security Fabric > Physical Topology



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.

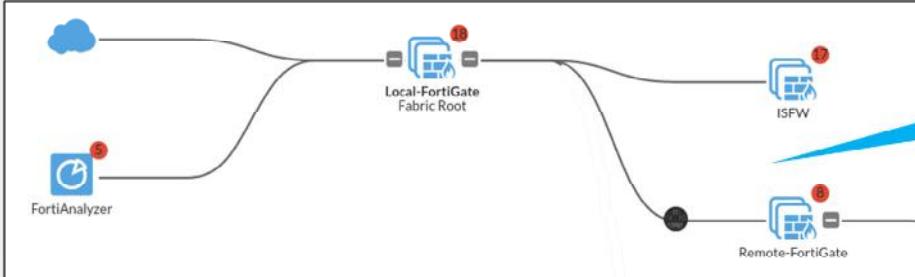
The **Physical Topology** view displays your network as a bubble chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to resize it and view more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

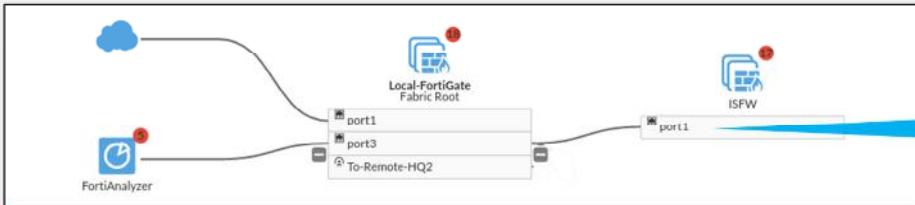
Topology Views (Contd)

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

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

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 the root and downstream FortiGate
- ✓ Understand how device detection works
- ✓ Understand how to extend 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 the Security Fabric Rating service
- ✓ View and run the Security Rating service
- ✓ Understand the differences between the physical and logical topology view



© Fortinet Inc. All Rights Reserved.

37

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

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



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© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

DO NOT REPRINT
© FORTINET



FortiGate Infrastructure Study Guide

for FortiOS 7.2

FORTINET
Training Institute

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

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

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

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

Fortinet | Pearson VUE

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

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

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



TABLE OF CONTENTS

Change Log	4
01 Routing	5
02 Virtual Domains (VDOMs)	68
03 Fortinet Single Sign-On (FSSO)	116
04 ZTNA	162
05 SSL VPN	192
06 IPsec VPN	229
07 High Availability	286
08 Diagnostics	343

Change Log

This table includes updates to the *FortiGate Infrastructure 7.2 Study Guide* dated 6/13/2022 to the updated document version dated 8/30/2022.

Change	Location
Various formatting fixes	Entire Guide
Fixed notes	Lesson 6, slide 50
Updated notes	Lesson 7, slide 19 and 42

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

Routing

FortiOS 7.2

Last Modified: 23 August 2022

In this lesson, you will learn about the routing capabilities and features available on FortiGate.

DO NOT REPRINT

© FORTINET

Lesson Overview



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Link Health Monitor and Route Failover



Diagnostics

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

DO NOT REPRINT

© FORTINET

Routing on FortiGate

Objectives

- Identify the routing capabilities on FortiGate
- Configure static routing
- Implement policy routes
- Route traffic for well-known internet services

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

By demonstrating competence in routing on FortiGate, you should be able to implement static and policy routing. You will also be able to route traffic for well-known internet services.

DO NOT REPRINT

© FORTINET

What Is IP Routing?

- FortiGate acts as an IP router in NAT mode
 - Forwards packets between IP networks
 - Supports IPv4 and IPv6 routing
- IP routing:
 - Performed for firewall traffic and local-out traffic
 - Determines next hop (outgoing interface and gateway) for packet destination address
 - Next hop can be the destination or another router along the path
- Routing table:
 - Contains routes with next hop information for a destination
 - Entries are checked during route lookup (best route selection)
 - *Best route*: most specific route to the destination
 - *Duplicate routes*: multiple routes to the same destination
 - Routes attributes are used as tiebreakers for best route selection
- Routing precedes most security actions
 - Configure your security policies based on routing settings, not the opposite



© Fortinet Inc. All Rights Reserved.

4

When FortiGate operates in NAT mode—the default operation mode—FortiGate behaves as an IP router. An IP router is a device that forwards packets between IP networks. For that, a router performs IP routing, which is the process of determining the next hop to forward a packet to based on the packet destination IP address. FortiGate supports both IPv4 and IPv6 routing.

FortiGate performs routing for both firewall traffic (also known as user traffic) and local-out traffic. Firewall traffic is the traffic that travels through FortiGate. Local-out traffic is the traffic generated by FortiGate, usually for management purposes. For example, when you ping a device from FortiGate, that's local-out traffic. When FortiGate connects to FortiGuard to download the latest definitions, that's also local-out traffic.

Routers maintain a routing table. A routing table contains a series of entries, also known as routes. Each route in the routing table indicates the *next hop* for a particular destination. The next hop refers to the outgoing interface and gateway to use for forwarding the packet. The next hop can be the destination of the packet or another router along the path to the destination. If the next hop isn't the destination, the next router in the path routes the packet to the next hop. The routing process is repeated on each router along the path until the packet reaches its destination.

To route packets, FortiGate performs a route lookup to identify the best route to the destination. The best route is the most specific route to the destination. If FortiGate finds duplicate routes—that is, multiple routes to the same destination—it uses various route attributes as a tiebreak to determine the best route.

Routing takes place before most security features. For example, routing precedes firewall policy evaluation, content inspection, traffic shaping, and source NAT (SNAT). This means that the security actions that FortiGate performs depend on the outgoing interface determined by the routing process. This also means that your security policy configuration must follow your routing configuration, and not the opposite.

DO NOT REPRINT**© FORTINET**

RIB and FIB

- FortiGate maintains two tables containing routing information: RIB and FIB

- RIB
 - Standard routing table containing active (or best) connected, static, and dynamic routes
 - Visible on the GUI and CLI

- FIB
 - Routing table from kernel perspective
 - Composed mostly by RIB entries, plus system-specific entries
 - Used for route lookups
 - Visible on the CLI only:

```
# get router info kernel
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/32 pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.254/32 pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.255/32 pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.200.1.0/32 pref=10.200.1.1 gwy=0.0.0.0 dev=3(port1)
...
```

FortiGate maintains its routing information in two tables: RIB and FIB. The routing table, also known as the routing information base (RIB), is a standard routing table containing active (or the best) connected, static, and dynamic routes. The forwarding information base (FIB) can be described as the routing table from the kernel point of view, and is built mostly out of RIB entries plus some system-specific entries required by FortiOS.

When FortiGate performs a route lookup, it checks the FIB and not the RIB. However, because the FIB is composed mostly by RIB entries, then the route lookup mainly involves checking routes from the RIB. For this reason, the route lookup is often referred to as the routing table lookup process. Nonetheless, a more accurate statement is to refer to it as the FIB lookup process.

You can display the RIB entries on the FortiGate GUI and CLI. However, for the FIB, you can display its entries on the FortiGate CLI only. The output on this slide shows the CLI command that displays the FIB. Note that the output has been cut to fit the slide. You will learn how to display the routing table entries in this lesson.

This lesson focuses on the RIB (or routing table) only, and you will learn more about it, including how to monitor its entries, in this lesson.

DO NOT REPRINT**© FORTINET**

Route Lookup

- For any session, FortiGate performs a route lookup twice:
 - For the first packet sent by the originator
 - For the first reply packet coming from the responder
- Routing information is written to the session table
- All other packets for that session will use the same path
- No more route lookups done unless the session is impacted by a routing change
 - Route information on the session is flushed and new route lookups are performed

For each session, FortiGate performs two route lookups:

- For the first packet sent by the originator
- For the first reply packet coming from the responder

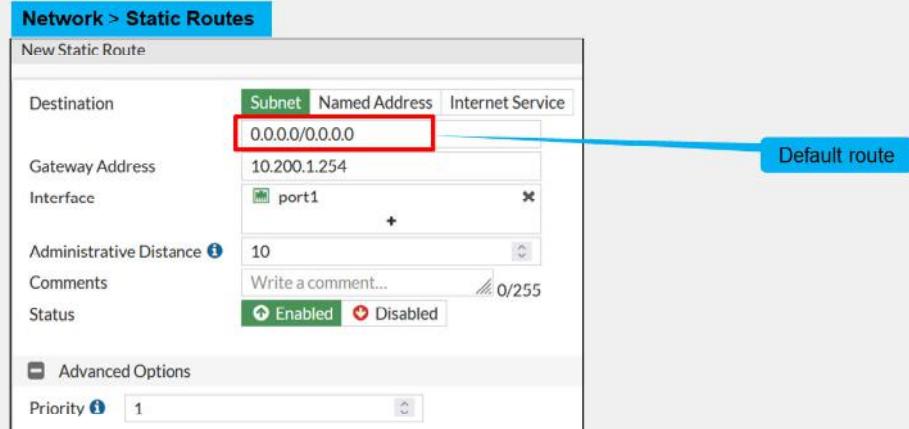
After completing these two lookups, FortiGate writes the routing information to its session table. Subsequent packets are routed according to the *session table*, not the routing table. So, all packets that belong to the same session follow the same path. However, there is an exception to this rule: if there is a change in the routing table that impacts the session, then FortiGate removes the route information for the session table, and then performs additional route lookups to rebuild this information.

DO NOT REPRINT

© FORTINET

Static Routes

- Configured *manually*, by an administrator
- Simple matching of packets to a route, based on the packet destination IP address



One type of manually configured route is called a static route. When you configure a static route, you are telling FortiGate, “When you see a packet whose destination is within a specific range, send it through a specific network interface, towards a specific router.” You can also configure the distance and priority so that FortiGate can identify the best route to any destination matching multiple routes. You will learn about distance and priority in this lesson.

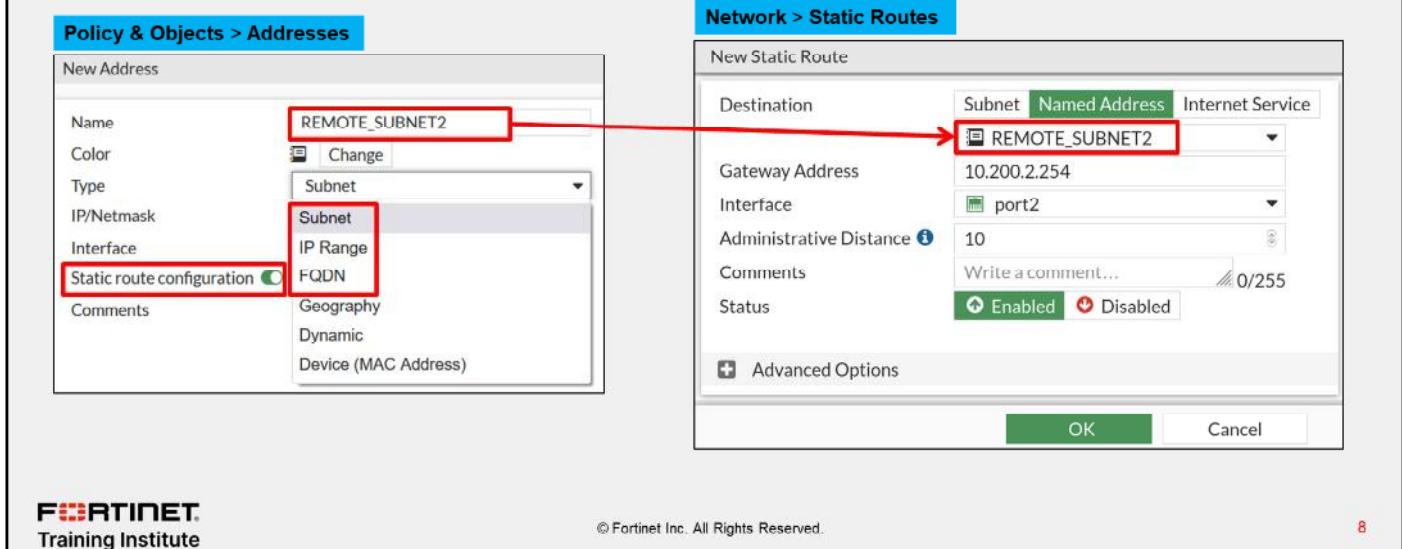
For example, in simple home networks, DHCP automatically retrieves and configures a route. Your modem then sends all outgoing traffic through your ISP internet router, which can relay packets to their destination. This is typically referred to as a default route, because all traffic not matching any other routes will, by default, be routed using this route. The example shown on this slide is a default route. The destination subnet value of $0.0.0.0/0.0.0.0$ matches all addresses within any subnet. Most FortiGate devices deployed at the edge of the network have at least one of these default routes to ensure internet traffic is forwarded to the ISP network.

Static routes are not needed for subnets to which FortiGate has direct Layer 2 connectivity.

DO NOT REPRINT
© FORTINET

Static Routes With Named Addresses

- Firewall addresses set to type **IP/Netmask** or **FQDN** can be used as destinations for static routes



The image shows two screenshots of the FortiGate management interface. The left screenshot is titled 'Policy & Objects > Addresses' and shows the configuration of a new address object named 'REMOTE_SUBNET2'. The 'Type' dropdown is set to 'Subnet', and the 'Static route configuration' checkbox is checked. The right screenshot is titled 'Network > Static Routes' and shows the creation of a new static route. In the 'Destination' field, the 'Named Address' tab is selected, and 'REMOTE_SUBNET2' is chosen from the dropdown. Other route parameters like 'Gateway Address' (10.200.2.254), 'Interface' (port2), and 'Administrative Distance' (10) are also set. A red arrow points from the 'Named Address' dropdown in the left window to the 'Named Address' tab in the right window, indicating the connection between the two configurations.

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

8

If you create a firewall address object with the type **IP/Netmask** or **FQDN**, you can use that firewall address as the destination of one or more static routes. First, enable **Static route configuration** in the firewall address configuration. After you enable it, the firewall address object becomes available for use in the **Destination** drop-down list for static routes with named addresses.

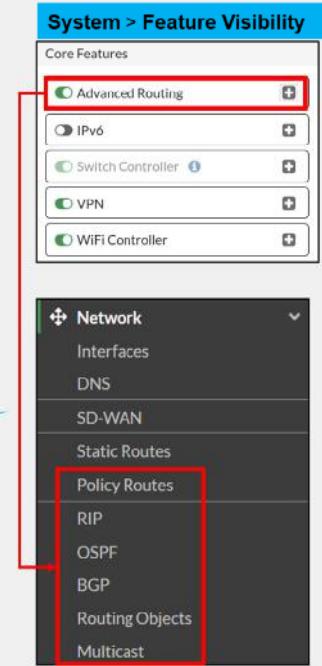
DO NOT REPRINT

© FORTINET

Dynamic Routes

- Routes are automatically learned
 - FortiGate exchanges routes with trusted adjacent routers
 - No need to configure manual routes
 - Useful for large networks with multiple subnets
- Supported dynamic routing protocols:
 - Routing Information Protocol (RIP)
 - Open Shortest Path First (OSPF)
 - Border Gateway Protocol (BGP)
 - Intermediate System to Intermediate System (IS-IS)
 - Must be configured on the FortiGate CLI

Enable **Advanced Routing** to display the GUI configuration pages for policy routes, RIP, OSPF, BGP, routing objects, and multicast



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

9

For large networks, manually configuring hundreds of static routes may not be practical. Your FortiGate can help, by learning routes automatically. FortiGate supports several dynamic routing protocols: RIP, OSPF, BGP, and IS-IS.

In dynamic routing, FortiGate communicates with trusted adjacent routers to exchange routing information about their known networks. Then, FortiGate adds the learned routes into its local routing table and considers them during the route lookup process.

You can configure dynamic routing for RIP, OSPF, and BGP protocols using the FortiGate GUI. You just need to make sure that the **Advanced Routing** option in the **Feature Visibility** page is enabled—it's enabled by default. However, for configuring IS-IS, you must use the FortiGate CLI.

Note that when you enable **Advanced Routing** on the **Feature Visibility** page, you also enable the configuration pages for other advanced routing features such as **Policy Routes**, **Routing Objects**, and **Multicast**. You will learn more about policy routes in this lesson.

Larger networks also may need to balance the routing load among multiple valid paths and detect and avoid routers that are down. You will learn more about that in this lesson.

DO NOT REPRINT

© FORTINET

Policy Routes

- Provide more granular matching than static routes:
 - Protocol
 - Source address
 - Source ports
 - Destination ports
 - ToS marking
 - Destination internet service
- Have precedence over routing table entries
- Separate table: policy route table
- Best practice: narrow down matching criteria

Network > Policy Routes

New Routing Policy

If incoming traffic matches:

Incoming Interface	port5	x			
Source Address	10.0.1.0/24	+			
IP/Netmask		+			
Addresses		+			
Destination Address	10.10.10.10/32	+			
IP/Netmask		+			
Addresses		+			
Internet service		+			
Protocol	TCP	UDP	SCTP	ANY	Specify
Source ports	0	65535			
Destination ports	10444	10444			
Type of service	0x00	Bit Mask	0x00		

Then:

Action	Forward Traffic	Stop Policy Routing
Outgoing Interface	port1	
Gateway address	192.2.0.2	
Comments	Write a comment...	0/255
Status	Enabled	Disabled

Matching criteria

Action

Static routes are simple and are often used in small networks. Policy routes, however, are more flexible because they can match more than just the destination IP address. For example, you can configure as matching criteria the incoming interface, the source and destination subnets, protocol, and port number.

Policy routes are maintained in a separate routing table by FortiGate and have precedence over the entries in the routing table. Because of its precedence, it is a best practice to narrow down the matching criteria of policy routes as much as possible. Otherwise, traffic that is expected to be routed using standard routing, that is, based on the destination address only and the routing table entries, could be handled by policy routes instead.

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

DO NOT REPRINT

© FORTINET

Policy Route—Actions

• Stop Policy Routing

- Skips all policy routes, uses the FIB

• Forward Traffic

- Forwards traffic using the set outgoing interface and gateway
- FIB must have a matching route; otherwise, policy route is considered invalid and skipped

Network > Policy Routes

New Routing Policy

If incoming traffic matches:

Incoming interface: port5

Source Address: 10.0.1.0/24

IP/Netmask: 10.0.1.0/24

Addresses: +

Destination Address: 10.10.10.10/32

IP/Netmask: 10.10.10.10/32

Addresses: +

Internet service: +

Protocol: TCP

Ports: 6

Source ports: 0 - 65535

Destination ports: 10444 - 10444

Type of service: 0x00 Bit Mask: 0x00

Then:

Action: Forward Traffic

Action: Stop Policy Routing

Outgoing interface: port1

Gateway address: 192.2.0.2

Comments: Write a comment... 0/255

Status: Enabled

Action

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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

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

DO NOT REPRINT
© FORTINET

Internet Services Routing

- Route well-known internet services through specific interfaces

Policy & Objects > Internet Service Database

Name	Direction	Number of Entries
Amazon-AWS	Both	14,015
Amazon-AWS.WorkSpaces.Gateway	Destination	27
Amazon-DNS	Destination	41,821
Amazon-FTP	Destination	41,821
Amazon-ICMP	Destination	41,821

Network > Static Routes

New Static Route

Destination:

Gateway Address:

Interface:

Comments:

Status:

Database containing IP addresses, protocols, and port numbers used by most common Internet services

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

12

What happens if you need to route traffic to a public internet service (such as Amazon-AWS or Apple Store) through a specific WAN link? Say you have two ISPs and you want to route Netflix traffic through one ISP and all your other internet traffic through the other ISP. To achieve this goal, you need to know the Netflix IP addresses and configure the static route. After that, you must frequently check that none of the IP addresses have changed. The internet service database (ISDB) helps make this type of routing easier and simpler. ISDB entries are applied to static routes to selectively route traffic through specific WAN interfaces.

Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.

FortiGate Infrastructure 7.2 Study Guide

16

DO NOT REPRINT
© FORTINET

IPv6 Routing

- Enable the IPv6 feature to support IPv6 routing configuration using the GUI
 - Allows static and policy route configuration using IPv6 addresses
 - Enables GUI configuration options of IPv6 versions of dynamic routing protocols

The screenshot shows the FortiGate GUI interface. On the left, the 'System > Feature Visibility' menu is open, with the 'IPv6' option selected and highlighted with a red box. On the right, the 'Network > Static Routes' table is displayed, showing two IPv4 static routes. A red arrow points from the 'IPv6' option in the Feature Visibility menu to the 'IPv6 Static Route' option in the Static Routes table.

IPv4	Gateway IP	Interface	Status
0.0.0.0/0	10.200.1.254	port1	Enabled
0.0.0.0/0	10.200.2.254	port2	Enabled

System > Feature Visibility

Network > Static Routes

© Fortinet Inc. All Rights Reserved. 13

To enable routing configuration for IPv6 addresses using the GUI, you must enable **IPv6** in the **Feature Visibility** menu. Then, you can create static routes and policy routes with IPv6 addresses. Enabling the IPv6 feature also enables GUI configuration options for IPv6 versions of the dynamic routing protocols.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which objects can you use to create static routes?
 A. ISDB objects
 B. Service objects

2. When the **Stop policy routing** action is used in a policy route, which behavior is expected?
 A. FortiGate skips over this policy route and tries to match another in the list.
 B. FortiGate routes the traffic based on the regular routing table.

DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Link Health Monitor and Route Failover



Diagnostics

Good job! You now understand routing on FortiGate.

Now, you will learn about routing monitor and route attributes.

Routing Monitor and Route Attributes

Objectives

- Interpret the routing table on FortiGate
- Identify how FortiGate decides which routes are installed in the routing table
- Identify how FortiGate chooses the best route using route attributes

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

By demonstrating competence in understanding the routing monitor and route attributes, you should be able to interpret the routing table, identify which routes are installed in the routing table, and identify how FortiGate chooses the best route using route attributes.

DO NOT REPRINT

© FORTINET

Routing Monitor

- Routing table (**Static & Dynamic**) view
 - Contains best routes (active routes) of type:
 - Connected, static, and dynamic routes
 - Doesn't contain:
 - Inactive, standby, and policy routes
- Policy route table (**Policy**) view
 - Displays all configured policy routes:
 - Regular policy routes, ISDB routes, and SD-WAN rules

Dashboard > Network > Routing > Static & Dynamic Routing

Dashboard > Network > Routing > Policy

Display connected, static, and dynamic routes

Route type

Regular policy route (top), ISDB route (middle), and SD-WAN rule (bottom)

© Fortinet Inc. All Rights Reserved. 17

The routing monitor widget on the dashboard page enables you to view the routing table and policy route table entries. The routing table contains *the best routes* (or active routes) of the following type:

- Static: manual routes that are configured by the administrator.
- Connected: automatic routes added by FortiOS after an interface is assigned an IP address. A connected route references the interface IP address subnet.
- Dynamic: routes learned using a dynamic routing protocol such as BGP or OSPF. FortiGate installs these routes automatically in the routing table and indicates the dynamic routing protocol used.

To view the routing table entries, select **Static & Dynamic**, as shown on this slide. However, keep in mind that the routing table doesn't contain the following routes:

- Inactive routes: static and connected routes whose interfaces are administratively down or whose links are down. Static routes are also marked inactive when their gateway is detected as dead by the link health monitor.
- Standby routes: These are active routes that are removed from the routing table because they are duplicate and have higher distances. For instance:
 - A second static default route with a higher distance than another static default route.
 - A dynamic route such as BGP or OSPF, to the same destination as another static route. However, the dynamic route is not displayed in the routing table because the static route has a lower distance.
- Policy routes: These include regular policy routes, ISDB routes, and SD-WAN rules. Policy routes are viewed in a separate table—the policy route table. To view the policy route table entries, select **Policy**.

DO NOT REPRINT

© FORTINET

GUI Route Lookup Tool

- Look up route by:
 - Destination address (required)
 - Destination port, source address, protocol, and source interface (optional)
- If all criteria are provided:
 - FortiGate checks both routing table and policy route table entries
 - Otherwise, FortiGate checks routing table entries only
- Matching route is highlighted

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.0.3.0/24	10.0.1.200	port3	200	BGP

Route Lookup	View	Create Address	Search
FortiGate			
Destination	8.8.8.8		
Destination Port	1-65535		
Source	IP or FQDN		
Protocol	TCP		
Source Interface			

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected

Matching route

You are redirected to the policy page if you enter all attributes

© Fortinet Inc. All Rights Reserved. 18

You can perform a route lookup on the routing monitor widget by clicking **Route Lookup**. Then, you must indicate at least the destination address to look up for, and optionally, the destination port, source address, protocol, and source interface.

The way the route lookup works is as follows:

- If you don't provide all lookup criteria, FortiGate considers only the routing table entries. FortiGate then highlights the matching route, if any.
- If you provide all lookup criteria, FortiGate considers both routing table and policy table entries. If the lookup matches a policy route, the GUI redirects you to the policy route page, and then highlights the corresponding matching policy route.

The example on this slide shows a route lookup tool for 8.8.8.8 and TCP as destination address and protocol, respectively. Because the administrator doesn't provide all criteria, FortiGate considers the routing table entries only. Then, the route lookup highlights the static default route as the matching route.

DO NOT REPRINT

© FORTINET

Route Attributes

- Each route in the routing table has the following attributes:

- Network
- Gateway IP
- Interfaces
- Distance
- Metric
- Priority

Dashboard > Network > Routing > Static & Dynamic Routing

Network	Gateway IP	Interface	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
10.200.1.0/24	0.0.0.0	port1	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0

Best Fit All Columns
Reset Table
Select Columns

Network
 Gateway IP
 Interfaces
 Distance
 Type
 Metric
Priority
Up Since
VRF

get router info routing-table all

...

```
Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [10/0]
C 10.0.1.0/24 is directly connected, port3
R 10.0.3.0/24 [200/0] via 10.0.1.200 (recursive is directly connected, port3), 23:21:46, [1,0]
O 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 17:29:25, [1,0]
R 10.0.5.0/24 [120/2] via 10.0.1.200, port3, 00:05:29, [1,0]
C 10.200.1.0/24 is directly connected, port1
C 10.200.2.0/24 is directly connected, port2
C 172.16.100.0/24 is directly connected, port8
```

Display routing table entries on the CLI

Each of the routes listed in the routing table includes several attributes with associated values.

The **Network** column lists the destination IP address and subnet mask to match. The **Interfaces** column lists the interface to use to deliver the packet.

The **Distance**, **Metric**, and **Priority** attributes are used by FortiGate to make various route selection decisions. You will learn about each of these in this lesson.

This slide also shows the command you can run to display the routing table on the FortiGate CLI. The `get router info routing-table all` command displays the same route entries as the routing monitor widget on the FortiGate GUI.

DO NOT REPRINT

© FORTINET

Distance

- First tiebreaker for duplicate routes (best route selection)
 - The lower the distance, the higher the preference
 - Set by the administrator (except connected routes)
- Best route selection:**
 - Route with lowest distance is installed in the RIB
 - Standby routes (higher distance) are not installed in the RIB
 - They are installed in the routing table database
 - Multiple equal-distance duplicate routes but different protocol:
 - FortiGate keeps the route that was learned last (avoid)
- Default distance per route type:

Connected*	Static (SD-WAN zone)	Static (DHCP)	Static (Manual)	Static (IKE)	EBGP	OSPF	IS-IS*	RIP	IBGP
0	1	5	10	15	20	110	115	120	200

* Hardcoded

Network	Gateway IP	Interface	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
10.200.1.0/24	0.0.0.0	port1	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0

Distance, or administrative distance, is the first tiebreaker that routers use to determine the best route for a particular destination. If there are two or more routes to the same destination (duplicate routes), the lowest-distance route is considered the best route and, as a result, is installed in the routing table. Other lower-distance routes to the same destination are standby routes and, as a result, are not installed in the routing table. Instead, they are installed in the routing table database. You will learn more about the routing table database in this lesson.

You can set the distance for all route types except connected and IS-IS routes. This slide shows the default values per type of route.

In case FortiGate learns two equal-distance routes to the same destination but that are sourced from different protocols, then FortiGate installs in the routing table the route that was learned *last*. For example, if you set the distance of BGP routes to 110, and there is another OSPF route to the same destination using the default administrative distance (110), then FortiGate keeps whichever route was learned last in the routing table. Because this behavior can lead to different results based on the timing of events, then it's not recommended to configure different-protocol routes with the same distance.

DO NOT REPRINT

© FORTINET

Metric

- Tiebreaker for same-protocol duplicate dynamic routes
 - The lower the metric, the higher the preference
- Best route is installed in the routing table and other duplicate routes in the routing table database
- The calculation method differs among routing protocols

Dashboard > Network > Routing > Static & Dynamic

Network	Gateway IP	Interface	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
10.200.1.0/24	0.0.0.0	port1	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

21

When a dynamic route protocol learns two or more routes to the same destination, it uses the metric as a tiebreaker to identify the best route. The lower the metric, the higher the preference. The dynamic routing protocol then installs the best route in the routing table and the higher-metric routes in the routing table database. Note that the metric is used as tiebreaker for same-protocol dynamic routes, and *not* between different-protocol dynamic routes.

The metric calculation differs among routing protocols, and the details are not covered in this course. For example, RIP uses the hop count, which is the number of routers the packet must pass through to reach the destination. OSPF uses cost, which is determined by the link bandwidth.

DO NOT REPRINT

© FORTINET

Priority

- Tiebreaker for ECMP static routes
 - ECMP static routes:
 - Equal-distance, equal-priority duplicate routes
 - All ECMP routes are installed in the routing table
 - The lower the priority, the higher the preference
- Best route is used during route lookup
- Applies to all routes except connected
 - Default value: 1
 - Hardcoded on all routes except static and BGP



Dashboard > Network > Routing > Static & Dynamic

Network	Gateway IP	Interfaces	Distance	Type	Metric	Priority
0.0.0.0/0	10.200.1.254	port1	10	Static	0	10
10.0.1.0/24	0.0.0.0	port3	0	Connected	0	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0	1
10.0.4.0/24	10.0.1.200	port3	120	OSPF	11	1
10.0.5.0/24	10.0.1.200	port3	120	RIP	2	1
10.200.1.0/24	0.0.0.0	port1	0	Connected	0	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0	0

New in FortiOS 7.2; useful for advanced routing deployments

© Fortinet Inc. All Rights Reserved.

22

FORTINET
Training Institute

When there are two or more duplicate static routes that have the same distance, FortiGate installs all of them in the routing table. If they also have the same priority, then the routes are known as ECMP static routes, and you will learn more about them in this lesson.

The priority setting enables administrators to break the tie among ECMP static routes. The result is that, during the route lookup process, FortiGate selects as the best route the static route with the lowest priority among all the equal-distance duplicate static routes. The lower the priority value, the higher the preference.

Starting FortiOS 7.2, the priority attribute applies to all routes except connected routes and is set to 1 by default. Before FortiOS 7.2, the attribute applied to static routes only and was set to 0 by default. When you upgrade to FortiOS 7.2, FortiOS automatically increases the priority of static routes by 1, and a value of 0 is no longer valid.

For dynamic routes, you can change the priority of BGP routes only. The priority of other dynamic routes is hardcoded to 1. The use of the priority value in dynamic routes is useful for advanced routing deployments involving SD-WAN and multiple virtual routing and forwarding (VRF) IDs. The details on how the priority attribute is beneficial for such cases is outside the scope of this course.

For static routes, you can configure the priority setting under the **Advanced Options** on the FortiGate GUI, as shown on this slide.

To view the priority in the routing monitor widget, you must enable the priority column (disabled by default). You can also view the priority on the routing table on the FortiGate CLI, which you will learn about later in this lesson.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. The priority attribute applies to which type of routes?
 A. Static
 B. Connected

2. Which attribute does FortiGate use to determine the *best* route for same-protocol duplicate dynamic routes?
 A. Priority
 B. Metric

3. Which routes are installed in the routing table?
 A. Best active routes
 B. Policy routes

DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Link Health Monitor and Route Failover



Diagnostics

Good job! You now understand the routing monitor and route attributes.

Now, you will learn about ECMP routing.

DO NOT REPRINT

© FORTINET

ECMP Routing

Objectives

- Identify the requirements for ECMP routing
- Implement route redundancy and load balancing

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

By demonstrating competence in ECMP, you should be able to identify the requirements for implementing ECMP and ECMP load balancing.

DO NOT REPRINT

© FORTINET

ECMP

- Same-protocol routes with equal:
 - Destination subnet
 - Distance
 - Metric
 - Priority
- ECMP routes are installed in the RIB
 - Traffic is load balanced among routes

Dashboard > Network > Routing > Static & Dynamic

Network #	Gateway IP #	Interfaces #	Distance #	Type #	Metric #	Priority #
0.0.0.0/0	10.200.1.254	port1	10	Static	0	5
0.0.0.0/0	10.200.2.254	port2	10	Static	0	5
10.0.1.0/24	0.0.0.0	port3	0	Connected	0	0
10.0.2.0/24	0.0.0.0	port4	0	Connected	0	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0	1
10.0.3.0/24	10.0.2.200	port4	200	BGP	0	1
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2	1
10.0.4.0/24	10.0.2.200	port4	110	OSPF	2	1
10.200.1.0/24	0.0.0.0	port1	0	Connected	0	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0	0

```
# get router info routing-table all
...
Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [5/0]
    [10/0] via 10.200.2.254, port2, [5/0]
C 10.0.1.0/24 is directly connected, port3
C 10.0.2.0/24 is directly connected, port4
B 10.0.3.0/24 [200/0] via 10.0.1.200 (recursive is directly connected, port3), 00:07:04, [1/0]
    [200/0] via 10.0.2.200 (recursive is directly connected, port4), 00:07:04, [1/0]
O 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:15:12, [1/0]
    [110/2] via 10.0.2.200, port4, 00:15:12, [1/0]
C 10.200.1.0/24 is directly connected, port1
C 10.200.2.0/24 is directly connected, port2
```

Two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes (same destination, distance, metric, and priority)

So far, you've learned about the different route attributes that FortiGate looks at to identify the best route to a destination.

But what happens when two or more routes of the same type have the same destination, distance, metric, and priority? These routes are called equal cost multipath (ECMP) routes, and FortiGate installs all of them in the routing table. FortiGate also load balances the traffic among the ECMP routes.

The example on this slide shows two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes. For each ECMP group, the destination subnet, distance, metric, and priority are the same.

The result is that FortiGate installs both routes of each ECMP group in the routing table. This lesson, however, focuses on ECMP static routes only.

DO NOT REPRINT**© FORTINET**

ECMP Load Balancing Algorithms

- Source IP (default)
 - Sessions sourced from the same address use the same route
- Source-destination IP
 - Sessions with the same source *and* destination address pair use the same route
- Weighted
 - Applies to static routes only
 - Sessions are distributed based on route, or interface weights
 - The higher the weight, the more sessions are routed through the selected route
- Usage (spillover)
 - One route is used until the bandwidth threshold is reached, then the next route is used

ECMP can load balance sessions using one of the following four algorithms:

- Source IP: This is the default algorithm. FortiGate uses the same ECMP route to route sessions sourced from the same address.
- Source-destination IP: FortiGate uses the same ECMP route to route sessions with the same source-destination IP address pair.
- Weighted: Applies to static routes only. FortiGate load balances sessions based on the route weight or the respective interface weight. The higher the weight, the more sessions FortiGate routes through the selected route.
- Usage (spillover): FortiGate sends sessions to the interface of the first ECMP route until the bandwidth of the interface reaches the configured spillover limit. After the spillover limit is reached, FortiGate uses the interface of the next ECMP route.

DO NOT REPRINT

© FORTINET

Configuring ECMP

- If SD-WAN is disabled, the ECMP algorithm is set on the CLI:

```
config system settings
  set v4-ecmp-mode [source-ip-based | weight-based | usage-based | source-dest-ip-based]
end
```

- Configure weight values on the CLI on the interface level (left) and route level (right):

```
config system interface
  edit <interface name>
    set weight <0-255>
  next
end
```

```
config router static
  edit <id>
    set weight <0-255>
  next
end
```

- Configure spillover thresholds on the CLI (kbps):

```
config system interface
  edit <interface name>
    set spillover-threshold <0-16776000>
    set ingress-spillover-threshold <0-16776000>
  next
end
```

If SD-WAN is disabled, you can change the ECMP load balancing algorithm on the FortiGate CLI using the commands shown on this slide.

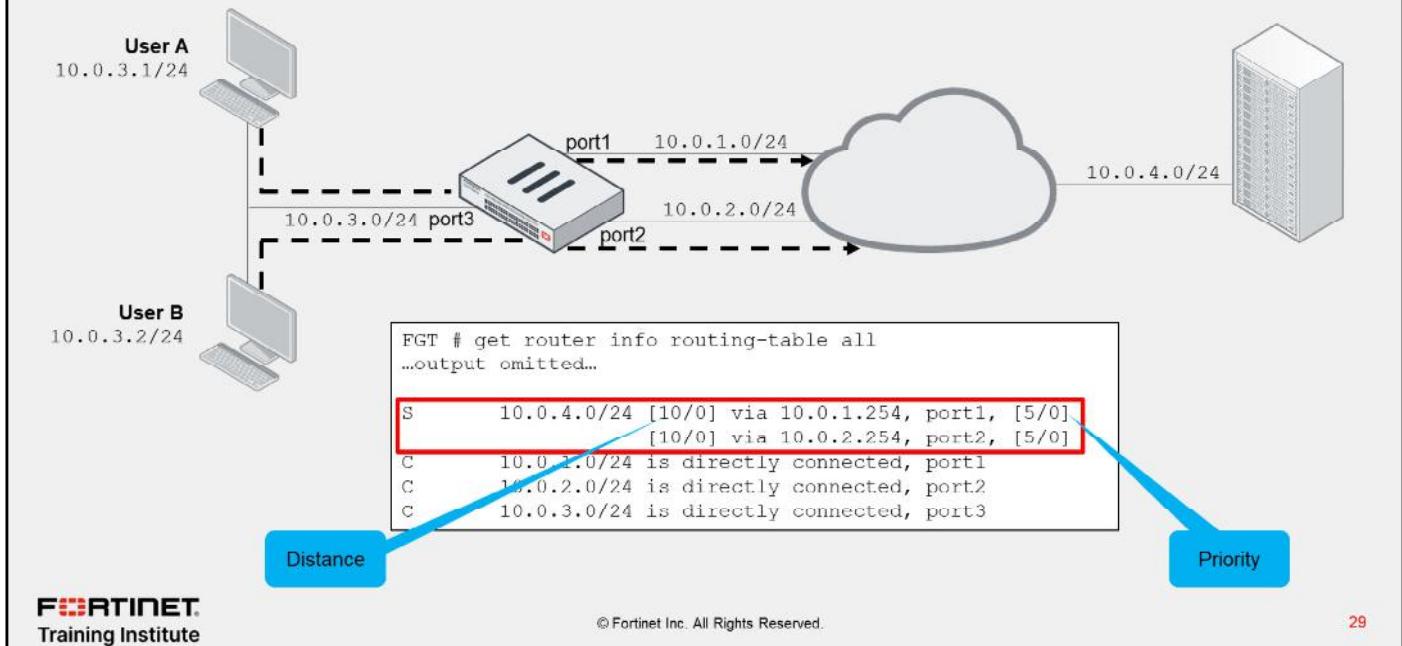
When SD-WAN is enabled, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, when you enable SD-WAN, you control the ECMP algorithm with the `load-balance-mode` setting.

For spillover to work, you must also configure the egress and ingress spillover thresholds, as shown on this slide. The thresholds are set to 0 by default, which disables spillover check. For weighted algorithm, you must configure the weights on the interface level or route level, as shown on this slide.

DO NOT REPRINT

© FORTINET

ECMP Example



In the scenario shown on this slide, FortiGate has ECMP routes for the 10.0.4.0/24 subnet on port1 and port2. Using the default ECMP algorithm (source IP based), FortiGate may use any of the two routes to route traffic from user A and user B.

In the example shown on this slide, FortiGate selects the route over port1 for user A, and the route over port2 for user B. FortiGate continues to use the same selected routes for the same traffic. In the route over port1 is removed from the routing table, FortiGate automatically starts to forward the traffic sourced from both users and destined to 10.0.4.0/24 through port2.

ECMP enables you to use multiple paths for the same destination, as well as provide built-in failover. Usually, you want to use ECMP for mission-critical services that require high availability. Another reason to use ECMP is for bandwidth aggregation. That is, you can leverage the bandwidth of multiple links by load balancing sessions across them.

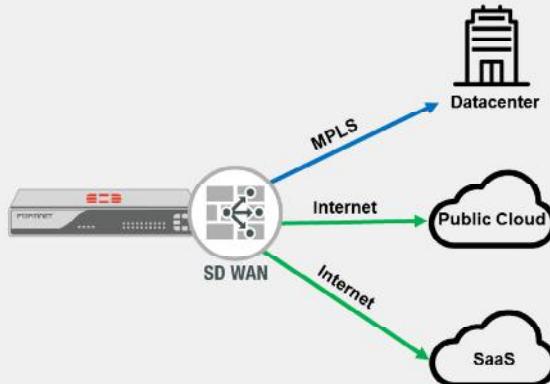
While ECMP enables you to leverage multiple WAN links on FortiGate, you may want to use SD-WAN because of the additional benefits.

DO NOT REPRINT

© FORTINET

What Is SD-WAN?

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



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

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

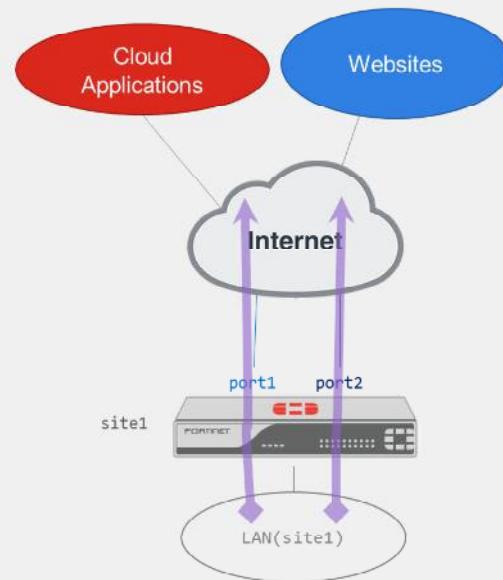
One benefit of SD-WAN is effective WAN usage. That is, you can use public (for example, broadband, LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of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

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

DO NOT REPRINT
© FORTINET

Direct Internet Access With SD-WAN

- Traffic steered across multiple internet links
- Typical operation:
 - Critical/sensitive traffic expedited and steered over best performing links
 - Costly links used for critical traffic or failover
 - Static default routing



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

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

For routing, a typical configuration makes use of static default routes. However, in some cases, BGP is used between the ISP and FortiGate, especially if the site must advertise a public IP prefix.

The example on this slide shows a basic DIA deployment. FortiGate has two internet links. One link is connected to port1 and the other to port2. FortiGate uses both links to steer traffic sourced from the LAN and destined to cloud applications and websites on the internet.

DO NOT REPRINT

© FORTINET

SD-WAN Rules

- Define steering rules based on:
 - Matching traffic criteria
 - Member preference
 - Member performance
- Evaluated from top to bottom:
 - Rules are used to steer traffic
 - Firewall policy required
 - Implicit rule
 - Used if user-defined rules are not matched
 - Usually, traffic is load balanced
- SD-WAN rules are policy routes
 - Route lookup order:
 1. Regular policy routes
 2. ISDB routes
 3. SD-WAN rules
 4. FIB entries

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	Critical-DIA	all	GoToMeeting, Microsoft.Office.365.Portal, Salesforce	Latency	port1, port2	0
2	Non-Critical-DIA	all	Facebook, Twitter		port2	0
	Implicit	sd-wan	all	Source IP	any	

SD-WAN rules represent the intelligence of the SD-WAN solution and the software-defined aspect of it. When you configure an SD-WAN rule, you first define the application or traffic pattern to match. After that, you indicate the preferred members and/or zones to steer the matching traffic to, and in some cases, the performing metrics that the member must meet to be eligible for steering traffic.

SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom, using the first match. However, unlike firewall policies, they are used to steer traffic, and *not* to allow traffic. That is, you must configure corresponding firewall policies to allow the SD-WAN traffic. If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. The implicit rule instructs FortiGate to perform standard routing on traffic. Because SD-WAN deployments usually have multiple routes to the same destination—that is, ECMP routes—then traffic that matches the implicit rule is usually load balanced across multiple SD-WAN members.

SD-WAN rules are essentially policy routes. Like regular policy routes, SD-WAN rules route traffic based on multiple criteria. That is, when you configure an SD-WAN rule, the kernel installs a corresponding policy route that reflects the source, destination, service, and outgoing interfaces configured in the SD-WAN rule. When FortiGate performs a route lookup, it checks the routes in the order of sequence shown on this slide. For example, SD-WAN rules have precedence over FIB entries, but not over regular policy routes.

The example on this slide shows two user-defined rules named **Critical-DIA** and **Non-Critical-DIA**, which are used to steer traffic in our basic DIA setup. The **Critical-DIA** steers **GoToMeeting**, **Microsoft.Office.365.Portal**, and **Salesforce** traffic to the member with the lowest latency, between **port1** and **port2**. The example shows that **port1** is selected because it is the member with the check mark beside it. The **Non-Critical-DIA** rule steers Facebook and Twitter traffic to **port2**. The implicit rule, located at the bottom of the list, is used if none of the two user-defined rules are matched.

DO NOT REPRINT**© FORTINET**

System Settings Algorithm vs. Implicit Rule Algorithm

- Both v4-ecmp-mode and load-balance-mode control the ECMP algorithm
 - load-balance-mode replaces v4-ecmp-mode when SD-WAN is enabled
- Differences:
 - load-balance-mode supports the volume algorithm, v4-ecmp-mode does not
 - load-balance-mode uses the weight defined under the SD-WAN member configuration, v4-ecmp-mode the weight defined in the static route
 - load-balance-mode uses the spillover thresholds defined under the SD-WAN member configuration, v4-ecmp-mode the spillover thresholds defined in the interface settings
- Volume algorithm:
 - FortiGate tracks the cumulative number of bytes of the member
 - The higher the member weight, the higher the target volume, the more traffic is sent to it



© Fortinet Inc. All Rights Reserved.

33

When you enable SD-WAN, FortiOS hides the v4-ecmp-mode setting and replaces it with the load-balance-mode setting under config system sdwan. That is, after you enable SD-WAN, you now control the ECMP algorithm with the load-balance-mode setting.

There are some differences between the two settings. The main difference is that load-balance-mode supports the volume algorithm, and v4-ecmp-mode does not. In addition, the related settings such as weight and spillover thresholds are configured differently. That is, when you enable SD-WAN, the weight and spillover thresholds are defined on the SD-WAN member configuration. When you disable SD-WAN, the weight and spillover thresholds are defined on the static route and interface settings, respectively.

When you set the ECMP algorithm to volume, FortiGate load balances sessions across members based on the measured interface volume and the member weight. That is, the volume algorithm instructs FortiGate to track the cumulative number of bytes of each member and to distribute sessions based on the weight. The higher the weight, the higher the target volume of the interface and, as a result, the more traffic FortiGate sends to it.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the default ECMP algorithm on FortiGate?
 - A. Weighted
 - B. Source IP

2. How does FortiGate load balance traffic when using the spillover algorithm in ECMP routing?
 - A. Sessions are distributed based on interface threshold.
 - B. Sessions are distributed based on route weight.

DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Link Health Monitor and Route Failover



Diagnostics

Good job! You now understand ECMP routing.

Now, you will learn about reverse path forwarding.

DO NOT REPRINT

© FORTINET

RPF

Objectives

- Identify how FortiGate detects IP spoofing
- Block traffic from spoofed IP addresses
- Differentiate between and implement the different RPF check methods

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

By demonstrating competence in RPF, you should be able to identify and block IP spoofing attacks in your network.

DO NOT REPRINT

© FORTINET

RPF

- IP anti-spoofing protection
- Source IP is checked for a return path
- RPF check is only carried out on:
 - The first packet in the session, not on a reply
- Two modes:
 - Feasible path (default; formerly loose)
 - Return path doesn't have to be the best route
 - Strict
 - Return path must be the best route
- If RPF check fails, debug flow shows:
 - reverse path check fail, drop

- Set RPF mode (default = disable):

```
config system settings
  set strict-src-check [disable | enable]
end
```

Strict mode

- Disable RPF (default = enable):

```
config system interface
  edit <interface>
    set src-check disable
  next
end
```

The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table.

The premise behind the RPF check is that if FortiGate receives a packet on an interface, and FortiGate doesn't have a route to the packet source address through the incoming interface, then the source address of the packet could have been forged, or the packet was routed incorrectly. In either case, you want to drop that unexpected packet, so it doesn't enter your network.

FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session.

There are two RPF check modes:

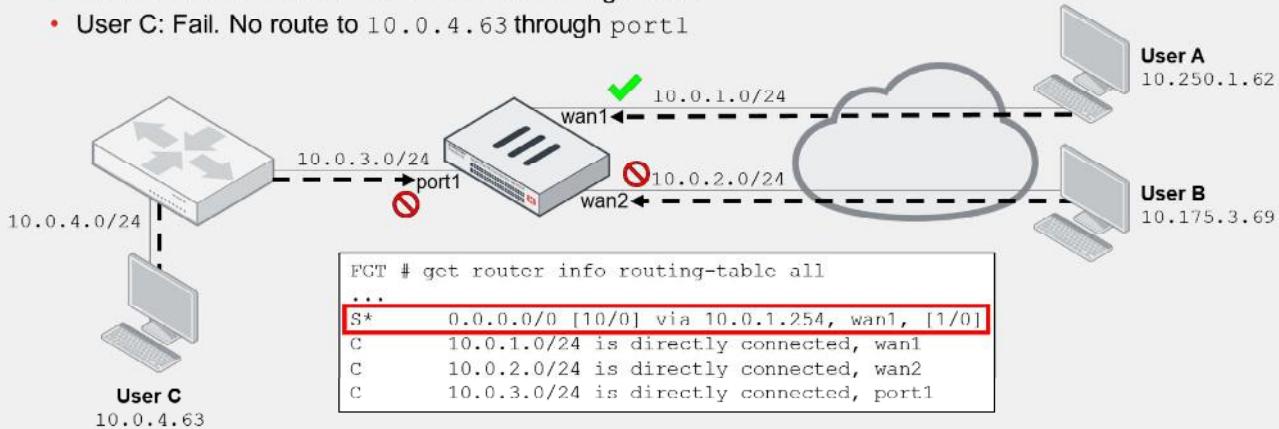
- Feasible path: Formerly known as loose, it's the default mode. In this mode, FortiGate verifies that the routing table contains a route that matches the source address of the packet and the incoming interface. The matching route doesn't have to be the best route in the routing table for that source address. It just has to match the source address and the incoming interface of the packet.
- Strict: In this mode, FortiGate also verifies that the matching route is the best route in the routing table. That is, if the routing table contains a matching route for the source address and incoming interface, but there is a better route for the source address through another interface, then, the RPF check fails.

This slide also shows how to change the RPF check mode on the FortiGate CLI, as well as how to disable the RPF check on the interface level.

DO NOT REPRINT
© FORTINET

RPF—Feasible Path Example

- FortiGate checks for a route matching source address and incoming interface
- RPF check results:
 - User A: Pass. Default route through wan1
 - User B: Fail. No route to 10.175.3.69 through wan2
 - User C: Fail. No route to 10.0.4.63 through port1



The example on this slide shows a FortiGate device using the feasible path RPF check mode. When FortiGate performs RPF check, it checks in the routing table for a route that matches the source address and the incoming interface of the first original packet.

Based on the topology and routing table shown on this slide, the RPF check results for traffic sourced from each user are:

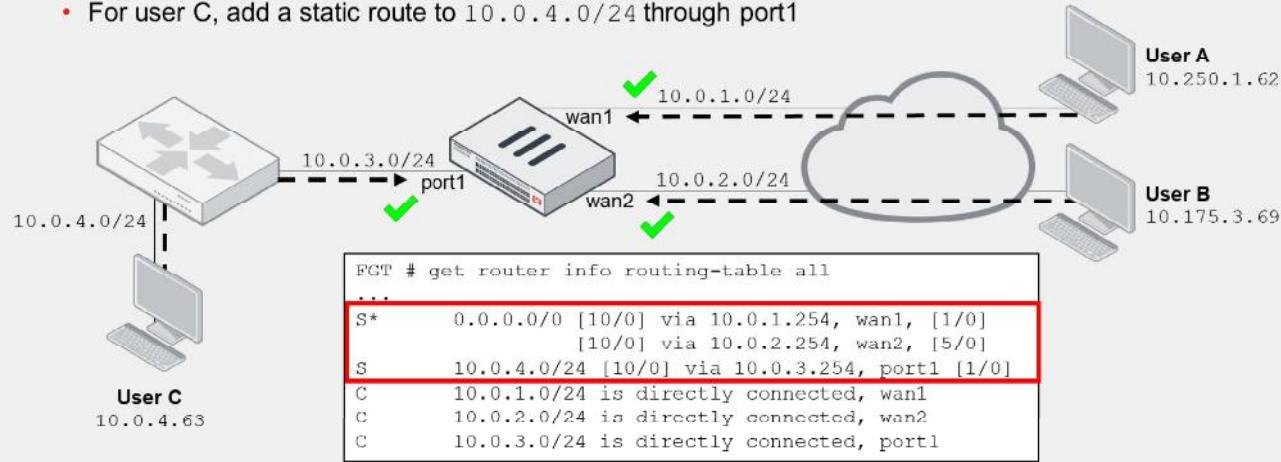
- User A: Pass. There is a default route through wan1. This means that, all packets received at wan1 pass the RPF check regardless of the source address.
- User B: Fail. FortiGate doesn't have a route to 10.175.3.69 through wan2 in its routing table.
- User C: Fail. Like the user B case, FortiGate doesn't have a route to 10.0.4.63 through port1 in its routing table.

DO NOT REPRINT
© FORTINET

RPF—Feasible Path Example (Contd)

- Solution:**

- For user B, add a second static default route, with the same distance, through wan2
 - Use different priority values if you don't want ECMP
- For user C, add a static route to 10.0.4.0/24 through port1



If you consider the packets from user B and user C to be legit packets, you can solve the RPC check fail issue by making sure the routing table contains routes for the return path.

In the example shown on this slide, the administrator adds two new static routes. The static route through wan2 is a duplicate default route of wan1, but has a lower priority. The two default routes are not ECMP routes because of the priority difference, but FortiGate keeps both routes in the routing table. The result is that packets from user B now pass the RPF check.

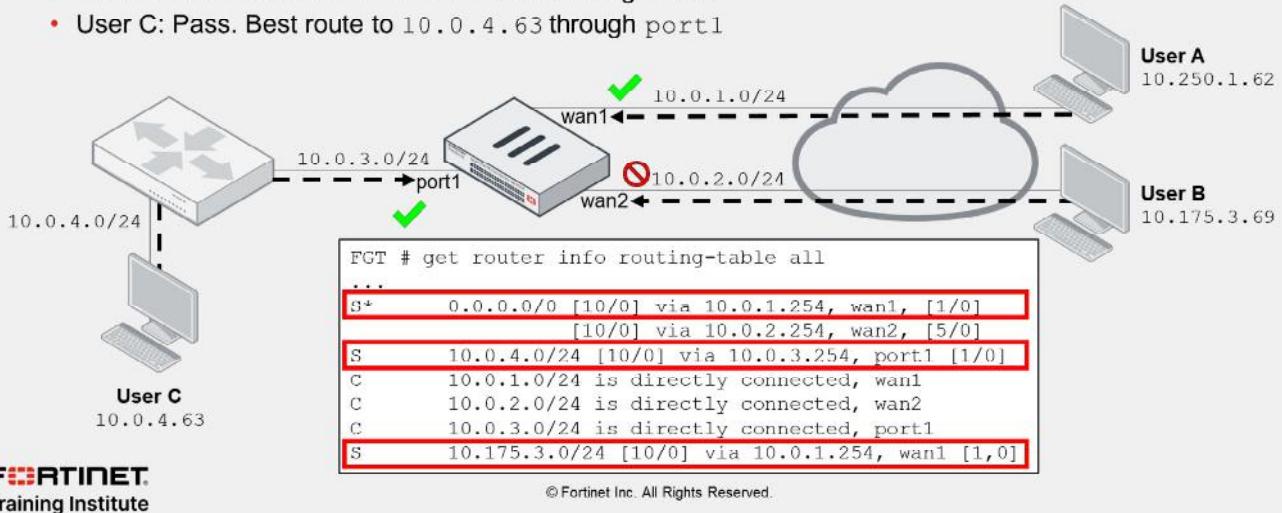
The static route through port1 references the 10.0.4.0/24 subnet. The subnet includes user C address (10.0.4.63), and as result, packets from user C also pass the RPF check.

DO NOT REPRINT

© FORTINET

RPF—Strict Example

- FortiGate also checks if the return path is the best route
- RPF check results:
 - User A: Pass. Best route to 10.250.1.62 through wan1 (default route)
 - User B: Fail. Best route to 10.175.3.69 through wan1
 - User C: Pass. Best route to 10.0.4.63 through port1



The example on this slide shows a FortiGate device using the strict RPF check mode. In strict mode, FortiGate also checks if the matching route is the best route to the source.

Based on the topology and routing table shown on this slide, the RPF check results for traffic sourced from each user are:

- User A: Pass. There is a default route through wan1. The route is also the best (and only) route to 10.250.1.62.
- User B: Fail. There is a default route through wan2. However, there is better (more specific) static route to 10.175.3.69 through wan1.
- User C: Pass. FortiGate has a route to 10.0.4.63 through port1 in its routing table. Although the default routes through wan1 and wan2 are also valid routes for 10.0.4.63, the best route to user C is the route through port1.

Like the feasible path example, you can solve the RPF fail issue for user B by making the respective changes in the routing table so the best route to user B is through wan2.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the default RPF check method on FortiGate?
 A. Feasible path
 B. Strict

2. Which route lookup scenario satisfies the RPF check for a packet?
 A. Routing table has a route to the destination IP of the packet through the incoming interface.
 B. Routing table has a route for the source IP of the packet through the incoming interface.

DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Link Health Monitor and Route Failover



Diagnostics

Good job! You now understand RPF.

Now, you will learn about the link health monitor and route failover.

DO NOT REPRINT

© FORTINET

Link Health Monitor and Route Failover

Objectives

- Configure the link health monitor
- Implement route failover
- Use the forward traffic logs

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

By demonstrating competence in configuring link health monitor and implementing route failover, you should be able to monitor the health of your interfaces and then, when a link is detected as dead, configure FortiGate to fail over the traffic to healthy links to minimize service disruption.

DO NOT REPRINT**© FORTINET**

Link Health Monitor

- Detect dead links when failure is beyond local physical connection
- Periodically send probes to up to four servers (beacons)
 - Choose at least two reliable servers to guard against server failure
 - Supported protocols: ping, TCP echo, UDP echo, HTTP, and TWAMP
- FortiGate operates as follows:
 - Initially, links are marked alive
 - Marks a link as dead after five consecutive failed probes from all configured servers
 - Performs any of the following actions: update static route, update policy route, and update cascade interface
 - Marks a link alive again after five consecutive successful probes from at least one server
 - Reverts any of the previous actions taken
 - The number of failed and successful probes can be adjusted (default = 5)

Static routes are kept in the routing table unless the associated interface is administratively down, its link goes down, or there is a duplicate route with a lower distance. Because it is possible that the link circuit is dead somewhere along the path to the destination, even though the interface link is up, then it is also possible that FortiGate continues to route traffic through a dead link, which would result in service impact. A common example is the Ethernet connection provided by your ISP modem. The Ethernet connection remains physically up even though the upstream ISP network is down. The devices behind your modem will continue to use the internet connection but they won't receive any replies.

Link health monitor enables FortiGate to detect dead links when the failure is beyond the local physical connection. FortiGate periodically sends probes through the configured gateway and interface to up to four servers that act as beacons. A server can be any host that is normally reachable through that path. It's best practice to configure at least two reliable servers to guard against false positives caused by the server being at fault, and not the link. For probes, you should also use a protocol that the server normally responds to.

Initially, FortiGate considers a link as alive. However, if FortiGate detects five consecutive failed probes from each of the configured servers, FortiGate marks the link as dead. FortiGate considers a failed probe a probe for which it does not receive a reply, or whose reply isn't valid. After FortiGate detects the link as dead, it performs any of the actions shown on this slide. The goal of these actions is to redirect the impacted traffic to other healthy links.

After FortiGate detects the link as dead, it continues to monitor the link. As soon as FortiGate receives five successful replies from at least one of the configured servers, it marks the link as alive again, and then reverts any of the previous actions taken on that link.

The number of failed and successful probes is set to five by default, but can be changed if required.

DO NOT REPRINT**© FORTINET**

Link Health Monitor Protocols

- Ping:
 - Most deployed
 - Sends ICMP echo requests and waits for ICMP echo replies
- TCP echo and UDP echo:
 - Sends TCP/UDP requests on port 7
 - Any data received by the server is sent back
- TWAMP:
 - Client-side implementation
 - Most accurate protocol
 - Two sessions:
 - Control: TCP 862 by default (if authentication is enabled)
 - Test: UDP 862 by default
- HTTP:
 - Sends an HTTP GET request and waits for response
 - Optionally, checks if the response contains the configured string



© Fortinet Inc. All Rights Reserved.

45

This slide describes the probe protocols supported by link health monitor.

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

When you use TCP echo and UDP echo, FortiGate sends periodic packets to the configured target servers, which are listening for connections on port 7 for both TCP and UDP. Upon reception of the packets, the server sends back an identical copy of the data it received from FortiGate.

Two-Way Active Measurement Protocol (TWAMP) is the most accurate protocol among the five. Link health monitor uses the client-side implementation of TWAMP. There are two sessions used in TWAMP: control and test. The former is used to authenticate the endpoints, and the latter to exchange packets used to measure the performance. Note that if authentication is disabled—it is disabled by default—FortiGate generates the test session only. FortiGate uses port 862 as default port for both control and test sessions, but you can configure a different port.

When you configure HTTP as the protocol, FortiGate sends periodic HTTP GET requests to the target server, and then waits for a response. Optionally, you can configure FortiGate to check if the response contains a specific string in the HTML content.

DO NOT REPRINT**© FORTINET**

Link Health Monitor Actions

Action	Dead	Alive	Effect during dead state
Update static route*	Flag associated static routes as inactive	Flag associate static routes as active	Static routes are removed from routing table
Update policy route**	Disable associated policy routes	Re-enable associated policy routes	Policy routes are skipped
Update cascade interface***	Bring down alert interfaces	Bring back up alert interfaces	Route LAN-originated traffic to a different device

* Associated static routes match the configured gateway and interface in the link health monitor settings

** Associated policy routes match the configured gateway and Interface in the link health monitor settings

*** Require the configuration of alert interfaces (usually, your LAN-facing interfaces)

This slide describes the actions taken by link health monitor when the state of an interface changes from alive to dead, and vice-versa. All three actions are enabled by default.

When you enable update static route and link health monitor detects an interface as dead, FortiGate marks the associated static routes—those matching the configured gateway and interface—as inactive. The result is that the inactive static routes are removed from the routing table. The absence of such routes can then force FortiGate to redirect the traffic to other valid routes, if any. Note that this action applies to static routes only.

The update policy route action works the same as the update static route action, except that instead of marking the associated static routes as inactive after an interface is detected as dead, FortiGate disables the associated policy routes. For that, FortiGate checks the policy route table and disables the policy routes whose outgoing interface and gateway match the configured interface and gateway in the link health monitor settings. Like the update static route action, the goal is for FortiGate to skip the disabled policy route during the route lookup process, so the traffic matches another policy route or FIB route in the system.

The update cascade interface action requires you to configure one or more alert interfaces. FortiGate then brings down the alert interfaces after the monitoring interface is detected dead. The goal is to force the traffic from networks behind the alert interfaces to be routed through a different device after an important interface, such as the internet-facing interface, is dead, which could mean that FortiGate is unable to forward traffic to the WAN. For example, if you are using dynamic routing or Virtual Router Redundancy Protocol (VRRP) on your LAN interface, which is configured as an alert interface, then bringing down the interface can trigger a routing failover to a backup gateway.

If FortiGate detects the interface as alive again, it reverts any action taken so far for the link. That is, FortiGate restores static routes, re-enables policy routes, and brings back up alert interfaces.

Link Health Monitor Configuration Example

- Configure link health monitor on the FortiGate CLI:

```
config system link-monitor
  edit port1-health
    set srcintf port1
    set server 4.2.2.1 4.2.2.2 8.8.8.8 8.8.4.4
    set gateway-ip 10.200.1.254
    set protocol ping
    set update-cascade-interface enable
    set update-static-route enable
    set update-policy-route enable
  next
end
```

- Configure port3 as alert interface if port1 is detected dead:

```
config system interface
  edit port1
    set fail-detect enable
    set fail-detect-option detectserver
    set fail-alert-method link-down
    set fail-alert-interfaces "port3"
  next
end
```

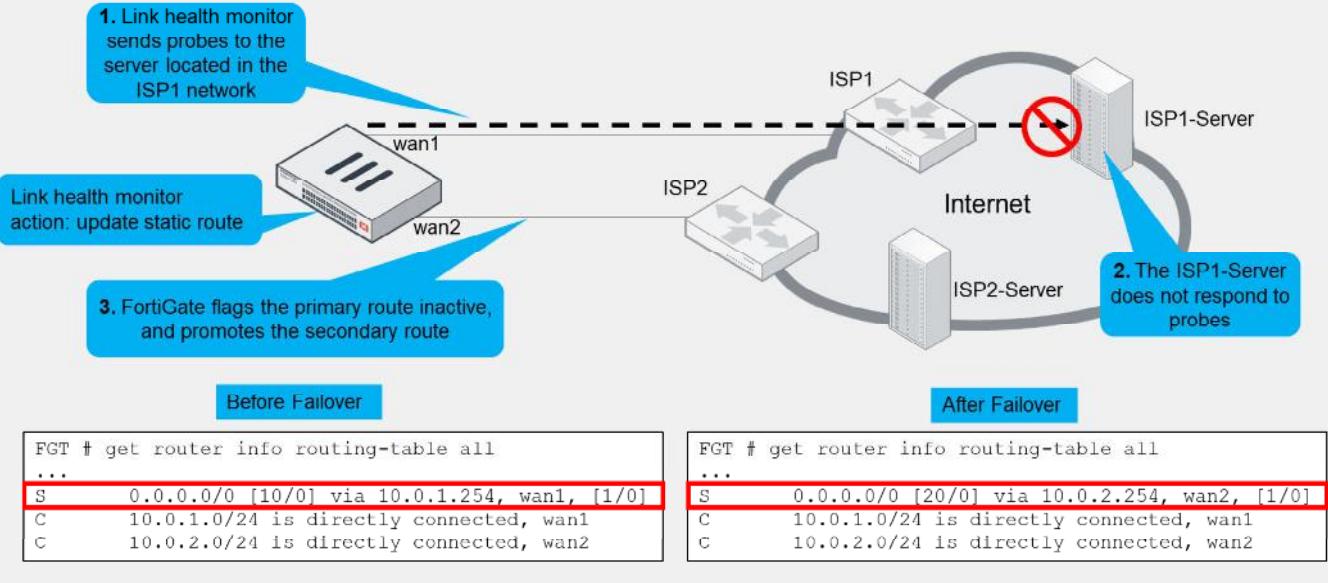
This slide shows a configuration example for link health monitor. FortiGate monitors the health of port1 against Level3 and Google DNS servers (four in total). For sending the probes, FortiGate uses 10.200.1.254 as gateway and ping as protocol.

When the state of port1 changes, FortiGate updates cascade interfaces, static routes, and policy routes. For the update cascade interface action to work, you must configure the alert interfaces. This slide also shows an example of the alert interface configuration required on the monitoring interface (port1). The configuration instructs FortiGate to bring down port3 if port1 is detected dead by the link health monitor feature.

DO NOT REPRINT

© FORTINET

Route Failover Example



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

48

In the example shown on this slide, FortiGate has two internet connections. wan1 is connected to ISP1, and wan2 to ISP2. Within each ISP network, there is a server that FortiGate sends probes to for link health monitoring purposes. For link health monitor, the update static route action is enabled. The administrator configured two static default routes, one through wan1 and the other wan2. The static default routes are assigned a distance of 10 and 20, respectively.

Before failover, the default route over wan1 is installed in the routing table because it has a lower distance, and the default route through wan2 is present in the routing table database as a standby route. The link health monitor sends probes to ISP1-Server located within the ISP1 network through wan1. When FortiGate detects five consecutive failed probes for ISP1-Server, FortiGate flags the default route over wan1 as inactive, which results in the route being removed from the routing table. This also results in the standby default route through wan2 to be installed in the routing table. Then, FortiGate starts using the new default route to route traffic to the internet.

The example shown on this slide makes use of different distance values to control the primary and standby routes. The result is that one default route only is installed in the routing table at any time. In case you always need to have both routes installed in the routing table, you can configure the same distance on both routes, but different priorities. You assign a lower priority number to your primary route, and a higher priority number to your standby route. Having both routes in the routing table is required if you use the interfaces to terminate IPsec VPN tunnels and you want to speed up failover by ensuring the tunnel over the secondary ISP link is already up before failover.

DO NOT REPRINT

© FORTINET

Best Practices—Forward Traffic Logs

- Use the **Destination Interface** column in the **Forward Traffic** logs to determine the egress interface for all traffic

Log & Report > Forward Traffic

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
11 seconds ago	10.0.1.200		208.91.112.52 (fortinet-public-dns-52.fortinet.com)		✓ 3.07 kB / 13.12 kB	Full_Access (1)	port1
13 seconds ago	10.0.1.200		208.91.112.53 (fortinet-public-dns-53.fortinet.com)		✓ 3.48 kB / 14.79 kB	Backup_Access (2)	port2
29 seconds ago	10.0.1.200		208.91.112.63 (ntp1.fortiguard.com)		✓ 76 B / 76 B	Backup_Access (2)	port2
30 seconds ago	10.0.1.200		208.91.112.61 (ntp1.fortiguard.com)		✓ 76 B / 76 B	Full_Access (1)	port1
39 seconds ago	10.0.1.200		208.91.112.62 (ntp2.fortiguard.com)		✓ 76 B / 76 B	Full_Access (1)	port1
45 seconds ago	10.0.1.200		208.91.112.60 (ntp2.fortiguard.com)		✓ 76 B / 76 B	Full_Access (1)	port1
Minute ago	10.0.1.10		54.186.52.97 (autopush.prod.mozaws.net)		✓ 6.01 kB / 9.76 kB	Full_Access (1)	port1
2 minutes ago	10.0.1.10		8.8.8.8 (dns.google)		✓ 92 B / 120 B	Backup_Access (2)	port2
2 minutes ago	10.0.1.10		8.8.8.8 (dns.google)		✓ 92 B / 108 B	Backup_Access (2)	port2

If you enable the **Destination Interface** column in the **Forward Traffic** logs, you can view the egress interface for traffic passing through your FortiGate device. You can use this information to determine which route is applied to which traffic stream, as well as identify any routing configuration issues.

If your firewall policies do not have any security profiles applied, you should enable logging for all sessions in your policies; otherwise, FortiGate does not generate any **Forward Traffic** logs. Use this feature with some caution, since enabling all sessions logging can generate a lot of logs if the firewall policy is handling a high volume of traffic. You should enable it when necessary, and disable it immediately afterwards.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the purpose of the link health monitor setting `update-static-route`?
 - A. It creates a new static route for the backup interface.
 - B. It removes all static routes associated with an interface detected as dead by the link health monitor.

2. When using link health monitoring, which route attribute can you configure to achieve route failover protection?
 - A. Distance
 - B. Metric

DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Link Health Monitor and Route Failover



Diagnostics

Good job! You now understand the link health monitor and route failover.

Now, you will learn about routing diagnostics.

DO NOT REPRINT

© FORTINET

Diagnostics

Objectives

- View active, standby, and inactive routes
- View policy routes on the CLI
- Use the built-in packet capture tool

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

By demonstrating competence in routing diagnostics, you should be able to view the entries in the routing table and routing table database, as well as to identify how packets flow across FortiGate.

DO NOT REPRINT

© FORTINET

Routing Table

```

# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      V - BGP VPNv4
      * - candidate default
      ? - best route

Routing table for VRF-0
S* 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [10/2]
C 10.0.1.0/24 is directly connected, port3
B 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 23:21:46, [1,0]
O 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 17:29:25, [1,0]
R 10.0.5.0/24 [120/2] via 10.0.1.200, port3, 00:05:29, [1,0]
C 10.200.1.0/24 is directly connected, port1
C 10.200.2.0/24 is directly connected, port2
C 172.16.100.0/24 is directly connected, port0
  
```

The CLI command shown on this slide displays all entries in the routing table. The routing table displays the routes that make it to the FIB. That is, the best active routes to a destination.

The left-most column indicates the route source. Route attributes are shown inside square brackets. The first number, in the first pair of attributes, is distance, which applies to both dynamic and static routes. The second number is metric, which applies to dynamic routes only.

Static routes and dynamic routes also have priority and weight attributes, which are shown as the last pair of attributes for the respective route. In the case of dynamic routes, the weight is always zero.

This command doesn't show standby or inactive routes, which are present in the routing table database only. For example, when two static routes to the same destination subnet have different distances, the one with the lower distance is installed in the routing table, and the one with the higher distance in the routing table database.

DO NOT REPRINT
© FORTINET

Routing Table Database

```

# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      V - BGP VPNv4
      > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S  *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10] Active route
S  0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0] Inactive route
S  8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0] Standby route
O  10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C  *> 10.0.1.0/24 is directly connected, port3
O  10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C  *> 10.0.2.0/24 is directly connected, port4
B  *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O  *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0] Active route
B  10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C  *> 10.200.1.0/24 is directly connected, port1
C  *> 10.200.2.0/24 is directly connected, port2

```

If you want to view active, standby, and inactive routes, use the CLI command shown on this slide to display the routing table database entries.

In the example on this slide, the command shows two standby routes, one static and the other BGP. Both standby routes are standby because there are better routes—lower distance—to the same destination. The better routes show an asterisk next to the route source to indicate they are FIB entries, and therefore, are used for routing traffic.

The output also shows one inactive route. Routes are marked as inactive where the corresponding interface is administratively down, has its link down, or when the interface is detected dead by link health monitor and the update static route action is enabled.

DO NOT REPRINT

© FORTINET

Policy Route Table

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

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=7 dport=0-65535
path(1) oif=21(T_MPLS_0)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=18 last_used=2022-02-23 05:47:21
This is a regular policy route (ID ≤ 65535)

id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0
iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
This is an ISDB route (ID > 65535 and no vwl_service field)

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr seq=1 2 dscp_tag=0xff 0xff flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2) oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
This is an SD-WAN rule (ID > 65535 and the vwl_service field is present)
```



© Fortinet Inc. All Rights Reserved.

55

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

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

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

Note that although IDs for regular policy routes are in the 1 to 65535 range, the maximum number of regular policy routes that you can configure are much lower and varies among models. For example, you can configure up to 512 regular policy routes in a FortiGate 300D device. For more information about the maximum supported values per model, refer to the FortiOS Maximum Values Table on docs.fortinet.com. Alternatively, you can run the `print tablesizes` command on the FortiGate CLI to get the maximum values for your device.

DO NOT REPRINT

© FORTINET

Packet Capture

- Can be used to verify the ingress and egress interface of packets

```
# diagnose sniffer packet <interface> '<filter>' <verbosity> <count> <timestamp> <frame size>
  • <interface> can be any or a specific interface (that is port1 or internal)
  • <filter> follows tcpdump format
  • <verbosity> specifies how much information to capture
  • <count> number of packets to capture
  • <timestamp> print time stamp information
    • a – prints absolute timestamp
    • l – prints local timestamp
  • <frame size> specify length of up to a maximum size of 65K
```

Packet captures, or *sniffers*, are one of the most useful sources of information for debugging routing problems. FortiGate includes a built-in traffic sniffer tool. You can use it to verify the ingress and egress interfaces of packets as they pass through. You can run the built-in sniffer from either the GUI or the CLI. The syntax of the CLI command is shown on this slide.

The `<interface>` option is the name of the physical or logical interface to run the sniffer on. Most of the times, you want to indicate `any` to capture packets on all interfaces. This enables you to see how packets flow across the different interfaces. Another option is to indicate the name of the interface, which is useful when you want to narrow down the packet capture to that interface. Indicating the name of the interface is also required if you want the tool to capture the MAC address information. That is, when you use `any`, the sniffer doesn't capture the real MAC addresses used by the packet.

The filter follows the Berkeley Packet Filter (BPF) syntax used by the well-known `tcpdump` tool. You should configure specific filters to ensure you're only capturing what you need. You can also specify a `<count>` value to automatically stop the sniffer after capturing a specific number of packets. Otherwise, the sniffer continues capturing packets until you manually stop it using `Ctrl + C`. You can use the `<time stamp>` option to print the time stamp information. Use `a` to print the absolute time stamp, or `l` (lowercase L) to print the local time-zone based time stamp. Time stamp information is particularly useful when correlating sniffer output to debug flow messages. You will learn more about debug flow in another lesson.

By default, the sniffer uses the MTU configured on the interface to limit the packet length during the capture. Using the `<frame size>` argument, you can specify a length larger or smaller than the interface MTU. Note that if you use the `any` interface, the sniffer will default to 1600 bytes.

DO NOT REPRINT**© FORTINET**

Packet Capture Verbosity Level

Level	IP Headers	Packet Payload	Ethernet Headers	Interface Name
1	•			
2	•	•		
3	•	•	•	
4	•			•
5	•	•		•
6	•	•	•	•

- The most common levels are:
 - 4 – Prints the ingress and egress interfaces
 - You can verify how traffic is being routed, or if FortiGate is dropping packets
 - 3 or 6 – Prints the packet payload
 - You can convert this output to a packet capture (pcap) file that can be opened with a packet analyzer
 - If you don't specify a level, the sniffer uses level 1 by default

The verbosity level specifies how much information you want to display. There are six different levels and this table shows which ones display the IP headers, packet payload, Ethernet headers, and interface names.

Use verbosity level 4 to take a quick look at how the traffic is flowing through FortiGate (if packets are arriving and how FortiGate is routing them out). You can also use level 4 to check if FortiGate is dropping packets.

Verbosity levels 3 and 6 provide the most output. Both show the IP payloads and Ethernet headers. You can save the output and export it to a packet capture (pcap) file using a Perl script. The pcap file can then be opened with a packet analyzer, such as Wireshark, for further investigation. You can locate the Perl script that converts the sniffer output to pcap on the Fortinet Knowledge Base website (kb.fortinet.com).

DO NOT REPRINT
© FORTINET

Packet Capture Examples

```
# diagnose sniffer packet any "port 443" 4
```

All traffic to or from port 443 with verbosity 4

```
...
5.455914 port3 in 10.1.10.1.59785 -> 100.64.3.1.443: syn 457459
5.455930 port1 out 100.64.1.1.59785 -> 100.64.3.1.443: syn 457459
5.455979 port1 in 100.64.3.1.443 -> 100.64.1.1.59785: syn 163440 ack 457460
5.455991 port3 out 100.64.3.1.443 -> 10.1.10.1.59785: syn 163440 ack 457460
5.456012 port3 in 10.1.10.1.59785 -> 100.64.3.1.443: ack 725411
5.456025 port1 out 100.64.1.1.59785 -> 100.64.3.1.443: ack 725411
```

```
# diagnose sniffer packet Students "icmp and host 10.0.10.254" 6 0 1
```

All ICMP traffic to or from 10.0.10.254 with verbosity 6, no packet count (0), and with local timestamps (1)

```
...
2021-05-26 07:43:28.653443 Students -- 10.0.10.2 -> 10.0.10.254: icmp: e
0x0000 0009 0f09 0003 5c85 7e32 16a2 0800 4500 .....\\~2....E.
0x0010 0054 9fef 4000 4001 71ba 0a00 0a02 0a00 .T..@.0.q.....
0x0020 0afe 0800 cec5 1686 0001 905e ae60 dff0 .....^..`...
0x0030 0900 0809 0a0b 0c0d 0e0f 1011 1213 1415 .....
0x0040 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
0x0050 2627 2829 2a2b 2c2d 2c2f 3031 3233 3435 & '() *+,-./012345
0x0060 3637
```

This slide shows two examples of packet capture outputs.

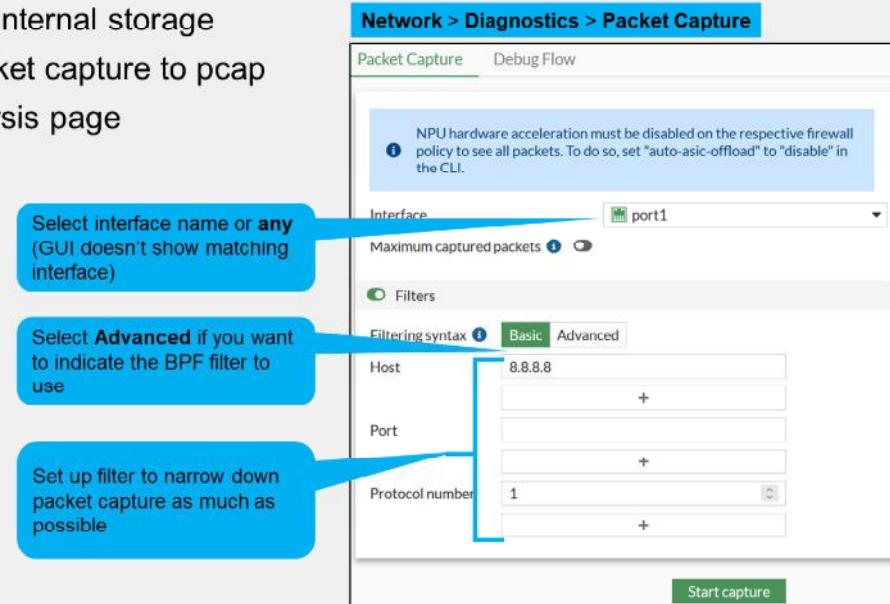
The first example captures all traffic to and from port 443. It uses verbosity 4, so the information is easy to read. It displays one packet per line, containing the incoming and outgoing interface, IP addresses, port numbers, and type of packet (SYN, SYN/ACK, and so on). Note that the interface is set to any, which is useful to capture packets that enter or exit multiple interfaces in the device. This enables you to have a better understanding of how packets flow through the firewall. For example, the output shows a three-way handshake established across FortiGate. From the packet capture, you can conclude that the connection is initiated by 10.1.10.1, which is behind port3, and is destined to 100.64.3.1, which is behind port1. You can also conclude that FortiGate performs SNAT for the connection. That is, in the original direction, FortiGate translates the source address to 100.64.1.1 when packets leave port1. FortiGate then translates the reply packets back to 10.1.10.1 when they exit port3.

The second example captures all ICMP traffic coming from or going to 10.0.10.254. Unlike the first example, which captures packets on any interface, this example limits the capture to packets that enter or leave the Students interface. Although not shown on this slide, the Students interface is a VLAN interface. In addition, the verbosity level is set to 6, which includes the full packet IP payload details. The output is longer and more difficult to read. However, this is one of the two verbosity levels to use (3 being the other one) if you need to export the output to pcap format. You can then view the pcap file using Wireshark or any other compatible packet analysis tool. Moreover, the additional arguments in the command instruct the sniffer to not set a packet count limit (0) and to print the local timestamp for each packet (1).

DO NOT REPRINT
© FORTINET

Packet Capture From the GUI

- Available on devices with internal storage
- Automatically convert packet capture to pcap
- Embedded real-time analysis page



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

59

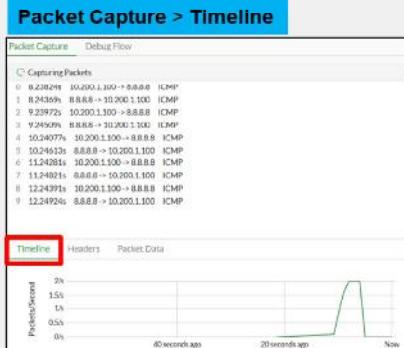
If your FortiGate model has internal storage, you can capture packets on the GUI. Starting FortiOS 7.2, the GUI packet capture tool was improved to also include a real-time analysis tool that enables you to examine the packet capture details directly on the GUI. You also download the respective pcap file in case you prefer to review it using Wireshark or your preferred packet analysis tool.

Before starting the packet capture, you should set up the packet capture filter by using either **Basic** or **Advanced** filter options. When you choose **Basic**, you indicate basic filter options such as host address, port number, and protocol number. In case you want to use your own BPF filter like you do in the CLI, you can choose **Advanced**.

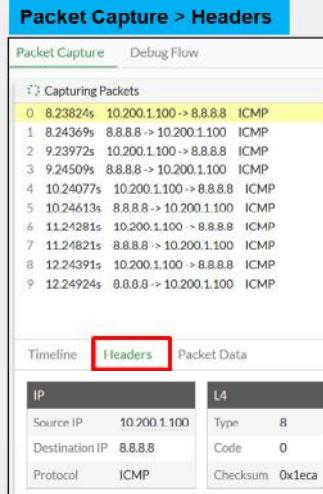
Regardless of which method you use (CLI or GUI), packet capture filters should be very specific to make sure only the relevant packets are captured, and large amounts of data are not being written to the disk.

DO NOT REPRINT
© FORTINET

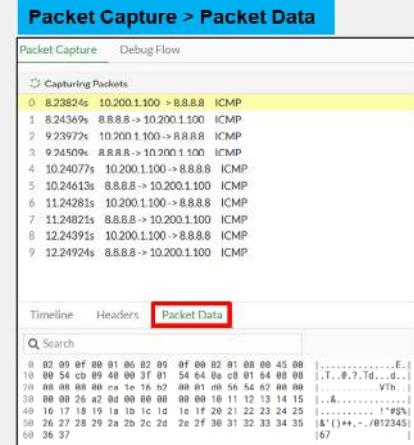
Packet Capture From the GUI (Contd)



- Useful to identify important traffic events



- Basic IP and Layer 4 data



- Full packet data in HEX and ASCII formats

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

60

This slide shows an example of the embedded real-time analysis tool included in the GUI packet capture tool starting FortiOS 7.2. After you start the packet capture, the GUI starts displaying the captured packets based on the filter set.

The **Timeline** tab displays a graph with the number of captured packets per second. The graph is useful to quickly identify peaks of traffic related by important events in the network.

The **Headers** tab enables you to examine basic IP (Layer 3) and Layer 4 information on the packet.

The **Packet Data** tab enables you to examine the full packet data using hexadecimal format. Next to the hexadecimal packet data, FortiOS displays the equivalent output in ASCII format.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the distance value for this route?

10.200.2.0/24 [110/2] via 10.200.2.254, [25/0]

- A. 110
- B. 2

2. Which CLI command can you use to view standby and inactive routes?

- A. get router info routing-table all
- B. get router info routing-table database

3. Which CLI packet capture verbosity level prints interface names?

- A. 3
- B. 4

DO NOT REPRINT**© FORTINET**

Lesson Progress



Routing on FortiGate



Routing Monitor and Route Attributes



Equal Cost Multipath Routing (ECMP)



Reverse Path Forwarding (RPF)



Best Practices



Diagnostics

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Configure static routing
- ✓ Configure and view policy routes
- ✓ Route traffic for well-known internet services using ISDB routes
- ✓ Interpret the routing table on FortiGate
- ✓ Implement ECMP routing
- ✓ Block traffic from spoofed IP addresses using RPF
- ✓ Understand route failover
- ✓ Explore the routing table and routing table database entries
- ✓ Use the built-in sniffer GUI and CLI tools

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

By mastering the objectives covered in this lesson, you learned how to configure, maintain, and troubleshoot the FortiGate routing configuration.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

Virtual Domains (VDOMs)

FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn how to configure VDOMs, and examine examples of common use.

DO NOT REPRINT

© FORTINET

Lesson Overview



VDOM Concepts

VDOM Administrators

Configuring VDOMs

Inter-VDOM Links

Best Practices and Troubleshooting

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

DO NOT REPRINT

© FORTINET

VDOM Concepts

Objectives

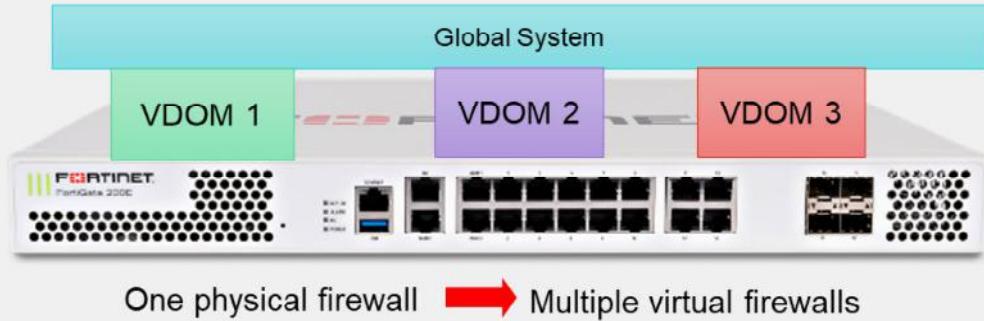
- Define and describe VDOMs

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

By demonstrating competence in VDOMs, you will be able to understand the key benefits and use cases for VDOMs.

DO NOT REPRINT**© FORTINET**

VDOMs



- Multiple VDOMs split FortiGate into multiple virtual devices
 - They employ independent security policies, routing tables, VPN configurations, and so on
- Packets are confined to the same VDOM
- By default, FortiGate supports up to 10 VDOMs
 - High-end models allow for the purchase of additional VDOMs
- Global settings are configured outside of the VDOM

What if a campus wants to keep its departments separate? A datacenter wants to implement various security implementations in a cost-effective manner that maintains all customer traffic separate and secure while also reducing space and making configuration easier? What if you want to segment your network, and subdivide policies and administrators into multiple security domains?

The best solution is to enable FortiGate VDOMs.

A VDOM splits your FortiGate into multiple logical devices and divides one security domain into multiple security domains.

Each VDOM has independent security policies and routing tables. Also, and by default, traffic from one VDOM cannot go to a different VDOM. This means that two interfaces in different VDOMs can share the same IP address, without any overlapping subnet problems.

When you use VDOMs, a single FortiGate device becomes a virtual data center of network security, UTM inspection, and secure communication devices.

DO NOT REPRINT**© FORTINET**

Multi-VDOM Mode

- Can create multiple VDOMs that function as multiple independent units
- FortiGate has two types of multi-VDOMs:
 - **Admin VDOM :**
 - Used for management purposes only
 - Does not pass any data
 - **Traffic VDOM :**
 - Processes all network traffic through FortiGate
 - Can provide separate security policies
- Three main use cases for multi-VDOM mode:
 - Management VDOM
 - Independent VDOM
 - Meshed VDOM



© Fortinet Inc. All Rights Reserved.

5

Use multi-VDOM mode when you want to create multiple logical firewalls from a single FortiGate. Each VDOM acts as an independent FortiGate.

Multi-VDOM mode works well for managed service providers leveraging multi-tenant configurations, or large enterprise environments that desire departmental segmentation. You can give each individual tenant or department, visibility and control of their VDOM, while keeping other VDOMs independent and unseen.

Two types of VDOMs can be created in multi-VDOM Mode: An admin VDOM and a traffic VDOM. Admin VDOMs are for FortiGate administration, and traffic VDOMs permit traffic to travel through FortiGate.

Upon upgrade, if a FortiGate is in split-vgm mode, it is converted to multi-vgm mode. The FG-traffic VDOM becomes a traffic type VDOM. The root VDOM becomes an admin VDOM.

DO NOT REPRINT**© FORTINET**

Management VDOM

- Where all the management traffic for FortiGate originates
- It *must* have access to all global services that FortiGate requires:
 - NTP
 - FortiGuard updates and queries
 - SNMP
 - DNS filtering
 - Logs—both FortiAnalyzer and syslog
 - As well as other FortiGate management-related services
- **By default, the management VDOM is **root****
 - Can be reassigned to any VDOM in multi-vdom mode, but direct internet access is recommended because specific services, such as web filtering using the public FortiGuard servers, will not work without it



© Fortinet Inc. All Rights Reserved.

6

Until now, you've learned about traffic passing *through* FortiGate, from one VDOM to another.

What about traffic originating *from* FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate.

Traffic coming from FortiGate to those global services originates from the *management* VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM.

By default, the root VDOM acts as the management VDOM, but you can manually reassign this task to a different VDOM in multi-vdom mode.

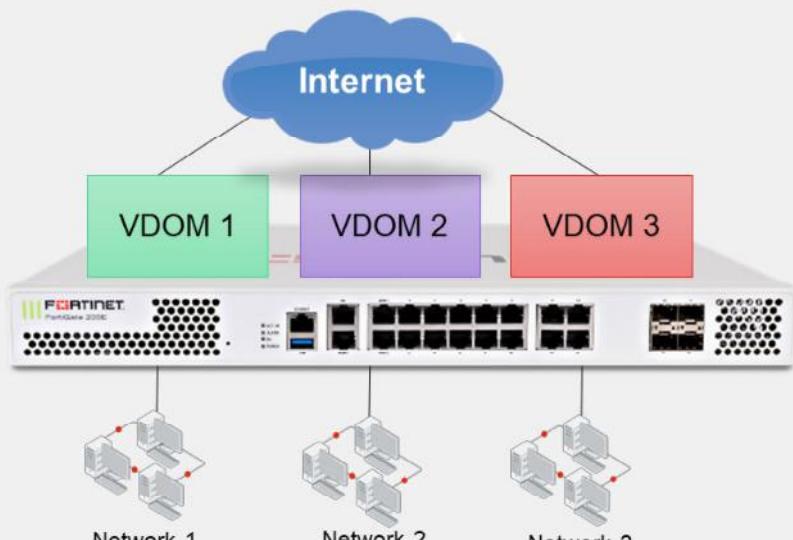
It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate. As such, the management function can be performed by any designated VDOM.

Similar to FortiGate without VDOMs enabled, the administrative VDOM should have outgoing internet access. Otherwise, features such as scheduled FortiGuard updates, fail.

DO NOT REPRINT**© FORTINET**

Independent VDOMs

- Multiple VDOMs are completely separated
- There is no communication between VDOMs
- Each VDOM has its own physical interface link to the internet



There are a few ways you can arrange your VDOMs. In the topology shown on this slide, each network accesses the internet through its own VDOM.

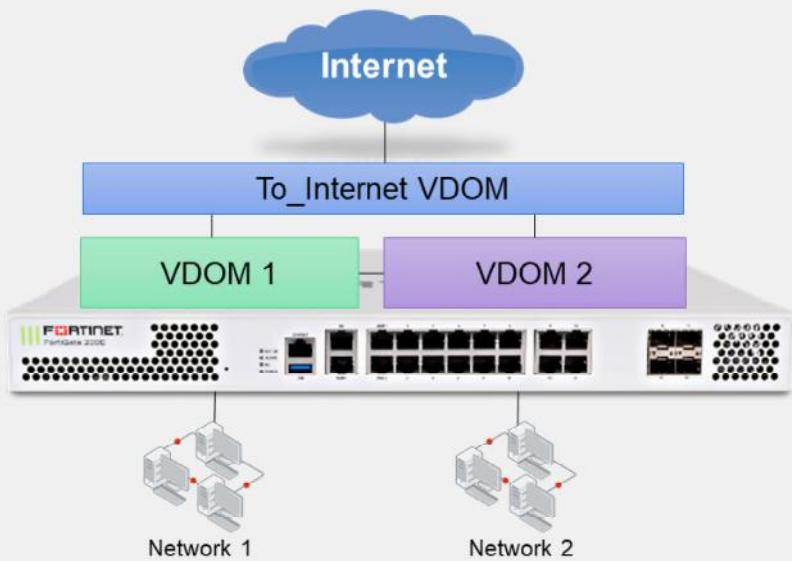
Notice that there are no inter-VDOM links. So, inter-VDOM traffic is not possible unless it physically leaves FortiGate, toward the internet, and is rerouted back. This topology would be most suitable in a scenario where multiple customers are sharing a single FortiGate, each in their own VDOM, with physically separated ISPs.

DO NOT REPRINT

© FORTINET

Meshed VDOMs

- VDOMs connect to other VDOMs through inter-VDOM links
 - Only Internet traffic needs to go through the **To_Internet** VDOM
 - Only the **To_Internet** VDOM is physically connected to the internet



In the example topology shown on this slide, traffic again flows through a single pipe in the **To_Internet** VDOM toward the internet. Traffic between VDOMs doesn't need to leave FortiGate.

However, now inter-VDOM traffic doesn't need to flow through the **To_Internet** VDOM. Inter-VDOM links between VDOMs allow more direct communication.

Similar to the previous example topology, inspection can be done by either the **To_Internet** or originating VDOM, depending on your requirements.

Because of the number of inter-VDOM links, the example shown on this slide is the most complex, requiring the most routes and firewall policies. Troubleshooting meshed VDOMs can also be more time consuming.

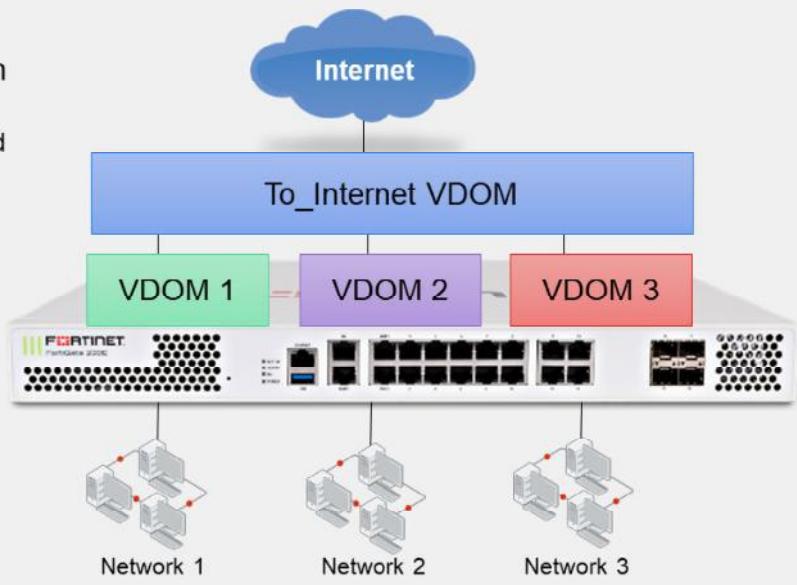
However, meshed VDOMs also provide the most flexibility. For large businesses, inter-VDOM communication may be required. Also, inter-VDOM traffic performance may be better because of a shorter processing path, which bypasses intermediate VDOMs.

DO NOT REPRINT

© FORTINET

Routing Through a Single VDOM

- Traffic destined to the internet will *always* be routed through the designated VDOM (**To_Internet** in this example)
 - The **To_Internet** VDOM is connected to other VDOMs using inter-VDOM links
 - Only the **To_Internet** VDOM is physically connected to the Internet



Like the topology shown on the previous slide, each network in the example topology shown on this slide sends traffic through its VDOM. However, after that, traffic is routed through the **To_Internet** VDOM. So, internet-bound traffic flows through a single pipe in the **To_Internet** VDOM.

This could be suitable in a scenario where multiple customers are sharing a single FortiGate, each in their own VDOM. In this case, the internet-facing VDOM could log and monitor traffic, or provide standard services like antivirus scanning, or both.

The topology shown on this slide has inter-VDOM links. VDOMs are linked only with the **To_Internet** VDOM, but not with each other. If **VDOM1** needs to communicate with **VDOM3**, this traffic would need to be routed through the **To_Internet** VDOM through IP routing decisions and is subject to all firewall policies.

Inspection could be done by either the internet-facing or originating VDOM, depending on your requirements. Alternatively, you could split inspection so that some scans occur in the internet-facing VDOM—ensuring a common security baseline—while other more intensive scans occur in the originating VDOM.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which traffic is always generated from the management VDOM?
 - A. Link Health Monitor
 - B. FortiGuard

2. Which statement about the management VDOM is true?
 - A. It is **root** by default and cannot be changed in multi-vdom mode.
 - B. It is **root** by default, but can be changed to any VDOM in multi-vdom mode.

DO NOT REPRINT

© FORTINET

Lesson Progress



VDOM Concepts



VDOM Administrators



Configuring VDOMs



Inter-VDOM Links



Best Practices and Troubleshooting

Good job! You now understand some basic concepts about VDOMs.

Now, you'll learn about VDOM administrators.

DO NOT REPRINT**© FORTINET**

VDOM Administrators

Objectives

- Create administrative accounts with access limited to one or more VDOMs

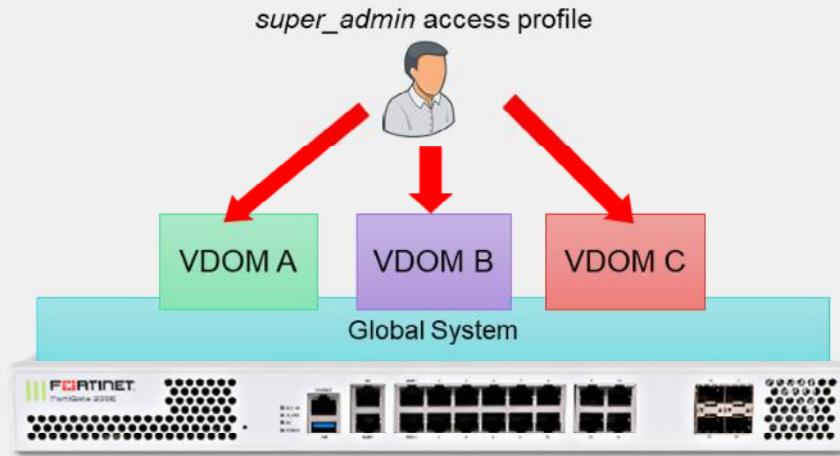
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in creating VDOM administrative accounts, you will be able to understand the differences between the various levels and types of VDOM administrators.

DO NOT REPRINT**© FORTINET**

VDOM Administration

- Only the account named **admin** or accounts with the **super_admin** profile can configure and back up all VDOMs

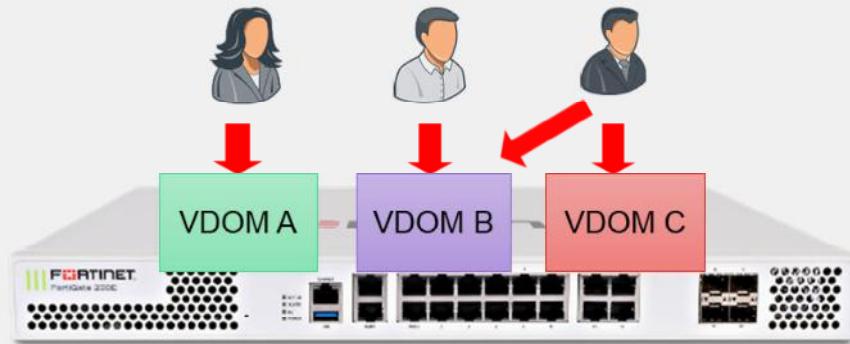


If you want to grant access to all VDOMs and global settings, select **super_admin** as the access profile when configuring the administrator account. Similar to the account named **admin**, this account can configure all VDOMs.

DO NOT REPRINT
© FORTINET

Per-VDOM Administration

- Other administrators can access only their *assigned* VDOMs
 - Cannot access the global settings



In most cases, you start by creating one administrator account per VDOM. That administrator is chiefly responsible for that domain, including the configuration backups of that VDOM. In larger organizations, you may need to make multiple VDOM administrators. You can assign multiple administrators to each VDOM. You can subdivide permissions using access profiles, in order to follow best practices for segregation of duties.

The converse is also possible. If required, you can assign an administrator to multiple VDOMs.

DO NOT REPRINT**© FORTINET**

Creating VDOM Administrators

Global > System > Administrators

New Administrator

Username	customer-admin
Type	Local User
	Match a user on a remote server group
	Match all users in a remote server group
	Use public key infrastructure (PKI) group
Password	*****
Confirm Password	*****
Comments	Write a comment... 0/255
Administrator profile	prof_admin
Virtual Domains	<ul style="list-style-type: none">customerroot

Two-factor Authentication ?

Restrict login to trusted hosts

Restrict admin to guest account provisioning only

OK **Cancel**

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

15

To create new administrator accounts and assign them to a VDOM, click **Global > System > Administrators**.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which type of administrator can make changes to all VDOMs?
 - A. A custom VDOM administrator
 - B. An administrator with the **super_admin** profile

2. Which statement about VDOM administrators is true?
 - A. There can be only one administrator per VDOM.
 - B. Each VDOM can have multiple administrators.

DO NOT REPRINT

© FORTINET

Lesson Progress



VDOM Concepts



VDOM Administrators



Configuring VDOMs



Inter-VDOM Links



Best Practices and Troubleshooting

Good job! You now understand VDOM administrators.

Now, you'll learn how to configure VDOMs.

DO NOT REPRINT

© FORTINET

Configuring VDOMs

Objectives

- Configure VDOMs to split a FortiGate into multiple virtual devices
- Multi VDOM types

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

By demonstrating competence in configuring VDOMs, you will be able to effectively implement VDOMs on your FortiGate.

DO NOT REPRINT**© FORTINET**

Enabling VDOMs

- FortiGate supports only multi-VDOM Mode
- From the GUI:
 - Available only on specific higher-end models
 - If the option does not exist, use the CLI command
- From the CLI:

```
#config system global
    set vdom-mode [no-vdom/multi-vdom]
end
```

System > Settings

System Operation Settings

Virtual Domains  

On the GUI, you can enable VDOMs under **System > Settings**. The GUI option is available only on higher-end FortiGate Models. Most of the FortiGate models, you can enable VDOMs on the CLI only.

Enabling VDOMs does not cause your FortiGate device to reboot, but it does log out all active administrator sessions. Traffic continues to pass through FortiGate.

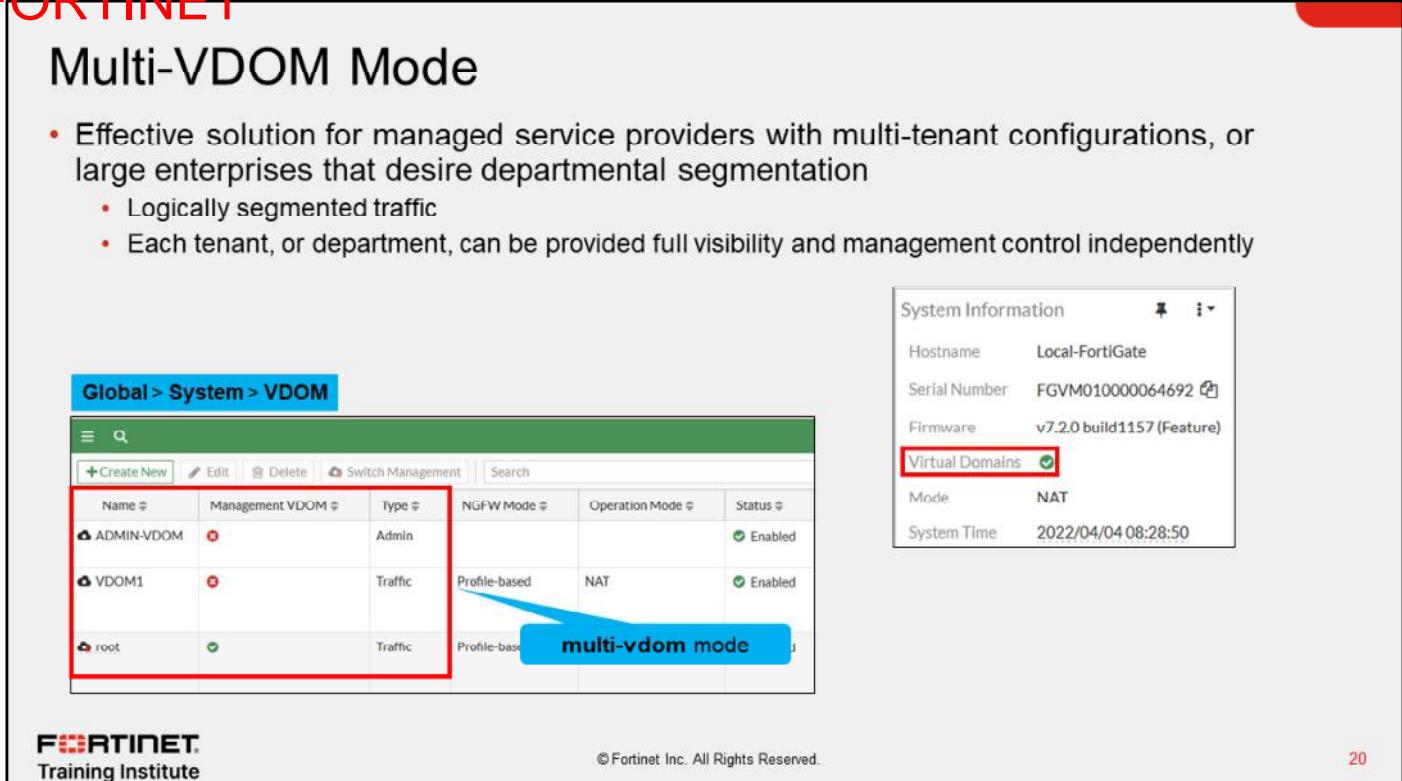
Enabling VDOMs restructures both the GUI and CLI, which you will see when you log in again.

DO NOT REPRINT

© FORTINET

Multi-VDOM Mode

- Effective solution for managed service providers with multi-tenant configurations, or large enterprises that desire departmental segmentation
 - Logically segmented traffic
 - Each tenant, or department, can be provided full visibility and management control independently



The screenshot shows the FortiGate Management Interface. On the left, the 'Global > System > VDOM' page is displayed, showing a list of VDOMs: 'ADMIN-VDOM' (Management, Admin, Profile-based), 'VDOM1' (Traffic, Profile-based), and 'root' (Traffic, Profile-based). A red box highlights the first two VDOMs. A blue callout box labeled 'multi-vdom mode' points to the 'Profile-based' entry for VDOM1. On the right, the 'System Information' panel shows the following details:

System Information	
Hostname	Local-FortiGate
Serial Number	FGVM01000064692
Firmware	v7.2.0 build1157 (Feature)
Virtual Domains	<input checked="" type="checkbox"/>
Mode	NAT
System Time	2022/04/04 08:28:50

At the bottom left is the Fortinet Training Institute logo, and at the bottom right is the page number '20'.

In *multi-vdom mode*, you can create multiple VDOMs that function as multiple independent units. By default, the root is the management VDOM and can be used to do both management tasks and allow other traffic. You can select any VDOM to act as the management VDOM.

DO NOT REPRINT

© FORTINET

Multi-VDOM types

- Multi-VDOMs can be one of the following types:
 - Admin type
 - Traffic type
- Admin type:
 - Used for administrative purposes only
 - Administrators can log in using SSH/HTTPS



Global > System > VDOM

Name	Management VD...	Type	NGFW Mode	Operation Mode	Status	CPU
root	✓	Traffic	Profile-based	NAT	Enabled	8%

Global > System > VDOM

Name	Management VD...	Type	NGFW Mode	Operation Mode	Status	CPU
root	✓	Traffic	Profile-based	NAT	Enabled	8%

When you enable multi-vdom mode, the root VDOM exists. It is the default management VDOM and is a traffic VDOM. You can create another VDOM (traffic or admin). FortiGate supports only one admin VDOM.

DO NOT REPRINT
© FORTINET

Multi -VDOM types (Contd)

- Traffic type:
 - Can pass traffic like regular VDOMs

Global > System > VDOM						
Name		Management VD...	Type	NGFWMode	Operation Mode	Status
root	✓	Traffic	Profile-based	NAT	Enabled	0%

- From CLI:

```
config vdom
edit <vdom>
  config system settings
    set vdom-type [traffic/admin]
  end
```



New Virtual Domain

Virtual Domain	VDOM1
Type	Traffic Admin
NGFW Mode	Profile-based
Central SNAT	<input checked="" type="radio"/>
WiFi country/region	Canada
Comments	

When the VDOM type is set to Traffic, the VDOM can pass traffic like a regular VDOM. If an admin VDOM exists, all newly created VDOMs are configured as traffic VDOMs.

DO NOT REPRINT

© FORTINET

Creating VDOMs

- By default, only the **root** management VDOM exists
 - You can create additional VDOMs.
- NGFW mode per VDOM:
 - Profile-based
 - Policy-based
- Operation mode per VDOM:

```
config vdom
edit <vdom>
  config system settings
    set opmode [nat | transparent]
end
```

Global > System > VDOM						
Name	Management VDOM	NGFW Mode	Operation Mode	Status	CPU	Memory
root	✓	Profile-based	NAT	Enabled	15%	36%

↓

<VDOM> > System > Settings

New Virtual Domain	Virtual Domain: VDOM1
Type:	Traffic Admin
NGFW Mode:	Profile-based Policy-based
Central SNAT:	<input checked="" type="checkbox"/>
WIFI country/region:	Canada
Comments:	

After enabling VDOMs in multi-vdom mode, by default, only one VDOM exists: the root VDOM. It's the default management VDOM.

You need to add a VDOM for each of your security domains. If you're an MSSP, for example, you might add one VDOM for each client company. If you are an enterprise business, you might add one VDOM for each division of your company.

The default inspection-mode is flow, so you can change **NGFW Mode** from **Profile-based** (default) to **Policy-based** directly in **System > Settings** for the VDOM.

The **profile-based** NGFW is the traditional mode and you must create antivirus, web filter, and IPS profiles, which are then applied to the policy. **Policy-based** mode is actually a new policy mode. You can add applications and web filtering categories directly to a policy without having to first create and configure application control or web filtering profiles. NGFW mode is a per-VDOM setting. If you set NGFW mode to **Profile-based**, you can configure policies in that VDOM for either flow or proxy inspection. However, if NGFW mode is **Policy-based**, then the inspection mode for all policies in that VDOM is always flow and there is no option available in the policy to change it.

Switching between NGFW modes results in the loss of all current policies configured in the VDOM. If you don't want this to happen, or you just want to experiment with a particular NGFW mode, consider creating a new VDOM for testing purposes. You could also back up your configuration before switching modes.

Operation mode is a per-VDOM setting. You can combine transparent mode VDOMs with NAT mode VDOMs on the same physical FortiGate.

DO NOT REPRINT**© FORTINET**

FortiGate Operation Modes

- Operation mode defines how FortiGate handles traffic
 - NAT mode:
 - Routes according to OSI Layer 3 (IP address), as a *router*
 - FortiGate interfaces have IP addresses associated with them
 - Transparent mode:
 - Forwards according to OSI Layer 2 (MAC address), as a transparent *bridge*
 - FortiGate interfaces usually have no IP addresses
 - Requires no IP address changes in the network
- FortiGate as a Transparent Bridge
 - Transparent to IP-layer hosts
 - Builds a table for traffic forwarding by analyzing the source MAC addresses of incoming frames
 - Splits your network into multiple collision domains:
 - Reduces traffic and collision levels seen on individual domains
 - Improves network response time



© Fortinet Inc. All Rights Reserved.

24

Traditional IPv4 firewalls and NAT mode FortiGate devices handle traffic the same way that routers do. Each interface must be in a different subnet and each subnet forms a different broadcast domain. FortiGate routes IP packets based on the IP header information, overwriting the source MAC address. So, if a client sends a packet to a server connected to a different FortiGate interface, the packet arrives at the server with a FortiGate MAC address, instead of the client MAC address.

In transparent operation mode, FortiGate forwards frames without changing the MAC addresses. When the client receives a packet from a server connected to a different FortiGate interface, the frame contains the real MAC address of the server—FortiGate doesn't rewrite the MAC header. FortiGate acts as a Layer 2 bridge or switch. So, the interfaces do not have IP addresses and, by default, all belong to the same broadcast domain.

This means that you can install a transparent mode FortiGate in a customer network without having to change the customer's IP address plan. Some customers, especially large organizations, don't want to reconfigure thousands of devices to define a new internal network that is separate from their external network.

A transparent mode FortiGate device acts as a transparent bridge. What does that mean? It means that FortiGate has a MAC address table that contains, among other things, the interface that must be used to reach each MAC address. FortiGate populates this table with information taken from the source MAC address of each frame.

FortiGate, as a transparent switch, splits the network into multiple collision domains, reducing the traffic in the network and improving the response time.

DO NOT REPRINT**© FORTINET**

Forward Domains

- By default, *all* interfaces on a VDOM belong to the same broadcast domain; even interfaces with different VLAN IDs
 - Broadcast domains that contain multiple interfaces can be very large and add unnecessary broadcast traffic to some LAN segments
- Use this command to subdivide a VDOM into multiple broadcast domains:

```
config system interface
    edit <interface_name>
        set forward-domain <domain_ID>
    end
```

- Interfaces with the same domain ID belong to the same broadcast domain

By default, in transparent operation mode, each VDOM forms a separate forward domain; however, interfaces do not. How does this affect the network?

Until you change the initial VDOM configuration, all interfaces, regardless of their VLAN ID, are part of the same broadcast domain. FortiGate broadcasts from every interface in the VDOM in order to find any unknown destination MAC address. On large networks, this could generate massive broadcast traffic and overwhelming replies—a broadcast storm.

DO NOT REPRINT
© FORTINET

Confirmation Prompt When Creating VDOMs

- VDOM confirmation prompt added
 - So that users do not create new VDOMs accidentally in CLI

```
config system global
  set edit-vdom-prompt [enable | disable]
end
```

- Disabled by default
- When enabled, if administrator creates a new VDOM, FortiGate displays prompt:

```
# config vdom
  edit student
  The input VDOM name doesn't exist.
  Do you want to create a new VDOM?
  Please press 'y' to continue, or press 'n' to cancel. (y/n)y
  current vf=student:3
```

Prompt to confirm before the new VDOM is created

A VDOM confirmation prompt has been added so users do not create new VDOMs accidentally on the CLI. This setting is disabled by default. Once enabled, when an administrator creates a new VDOM, FortiGate displays a prompt to confirm before the VDOM is created.

DO NOT REPRINT
© FORTINET

Assigning Interfaces to a VDOM

- You can assign an interface to each VDOM you create

- From CLI:

```
config global
config system interface
  edit <interface_name>
    set vdom <vdom-name>
  end
```

Global > Network > Interfaces

Edit Interface

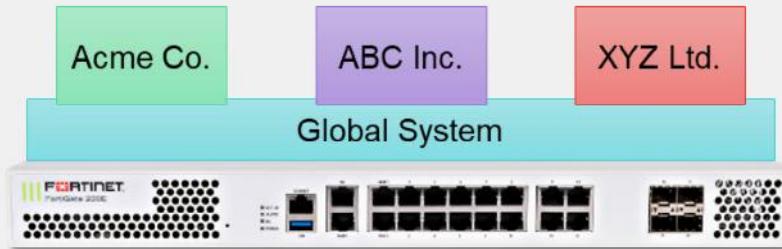
Name	port4
Alias	
Type	Physical Interface
VRF ID	0
Virtual domain	<input type="button" value="root"/> <input type="button" value="root"/> <input type="button" value="VDOM1"/>
Role	<input type="button" value="root"/>
Address	
Addressing mode	Manual <input type="button" value="DHCP"/> <input type="button" value="Auto-managed by FortiPAM"/>
IP/Netmask	192.168.10.254/24
Secondary IP address	<input type="checkbox"/>

After adding a VDOM, you can specify which interface belongs to it. Each interface (physical or VLAN) can belong to only one VDOM.

You can move an interface from one VDOM to another, provided it is not associated with any references, such as firewall policies.

DO NOT REPRINT
© FORTINET

Global and Per-VDOM Settings



Global settings

- Affect all configured VDOMs:
 - Hostname
 - HA settings
 - FortiGuard settings
 - System time
 - Administrative accounts

Per-VDOM settings

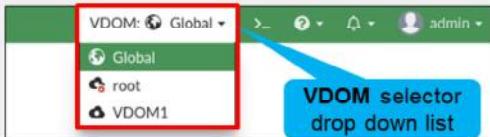
- Configured separately for each VDOM:
 - Operating mode (transparent, NAT/route)
 - NGFW mode (profile-based, policy-based)
 - Routes and network interfaces
 - Firewall policies
 - Security profiles

Global resource limits are an example of global settings. The firmware on your FortiGate device and some settings, such as system time, apply to the entire device—they are not specific to each VDOM.

However, you can configure most settings differently for each VDOM. Some examples are firewall policies, firewall objects, static routes, and protection profiles.

DO NOT REPRINT
© FORTINET

Accessing Global and Per-VDOM Settings



- Accessing global settings:

```
config global
  (global) #
```

- Accessing per-VDOM settings:

```
config vdom
  (vdom) # edit <vdom-name>
  (vdom-name) #
```

VDOM names are case sensitive. Use the correct case for the VDOM name or FortiGate will create a new VDOM

- Executing global and per-VDOM commands from any context:

```
[global | vdom-name] # sudo [global | vdom-name] [diagnose | execute | show | get]
```

When you log with a regular administrator account, you automatically enter the VDOM associated with that account.

When you log in with the account named admin, you have access to all VDOMs. To access a specific VDOM, select it in the drop-down list at the top of the page.

The VDOM submenu should be familiar; it is essentially the same navigation menu from before you enabled VDOMs. However, the global settings are moved to the Global menu.

To access the global configuration settings on the CLI, you must enter config global to enter into the global context. After that, you can run global commands and change global configuration settings.

To access per-VDOM configuration settings on the CLI, you must enter config vdom, then enter edit followed by the VDOM name. From the VDOM context, you can run VDOM-specific commands and change per-VDOM configuration settings. It is important to note that VDOM names are case sensitive. If you enter the name using the incorrect case, FortiGate creates a new VDOM.

Regardless of which context you are in (global or VDOM), you can use the sudo keyword to run diagnostics commands in a context different from your current one. This allows you to run global and per-VDOM commands, for example, without switching back and forth between the global and per-VDOM contexts.

DO NOT REPRINT

© FORTINET

Global Security Profiles

- Global security profiles for multiple VDOMs
- Global profiles support the following features
 - Antivirus
 - Application control
 - Intrusion prevention
 - Web filtering
- Profiles are read-only for VDOM-level administrators
 - Must edit, or delete from global settings
- Global profile name must start with "g-" for identification

The screenshot displays two FortiGate management interface windows. The top window, titled 'Global > Security Profiles > Web Filter', shows the configuration of a global security profile named 'g-default'. The profile is set to 'Default web filtering' and 'Flow-based'. The bottom window, titled 'Customer VDOM > Web Filter', shows the list of security profiles for the 'Customer VDOM'. It lists two profiles: 'g-default' and 'g-wifi-default'. Both profiles are set to 'Default web filtering' and have a 'Scope' of 'Global'. A red arrow points from the 'g-default' profile in the Global window down to the 'g-default' profile in the Customer VDOM window.

Name	Comments	Scope	Ref.
WEB g-default	Default web filtering.	Global	0
WEB g-wifi-default	Default configuration for offload...	Global	1

FORTINET
Training Institute

30

You can configure security profiles globally for use by multiple VDOMs, to avoid creating identical profiles for each VDOM separately. Global profiles are available for the following security features:

- Antivirus
- Application control
- Intrusion prevention
- Web filtering

Some security profile features, such as URL filters, are not available for use in a global profile. The name for any global profile must start with "g-" for identification. Global profiles are available as read-only for VDOM-level administrators and can be edited or deleted only in the global settings. Each security feature has at least one default global profile.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which configuration settings are global settings?
 - A. Firewall policies
 - B. FortiGuard settings

2. Which configuration settings are per-VDOM settings?
 - A. Host name
 - B. NGFW mode

DO NOT REPRINT

© FORTINET

Lesson Progress



VDOM Concepts



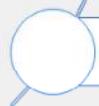
VDOM Administrators



Configuring VDOMs



Inter-VDOM Links



Best Practices and Troubleshooting

Good job! You now understand how to configure VDOMs.

Now, you'll learn about inter-VDOM links.

DO NOT REPRINT

© FORTINET

Inter-VDOM Links

Objectives

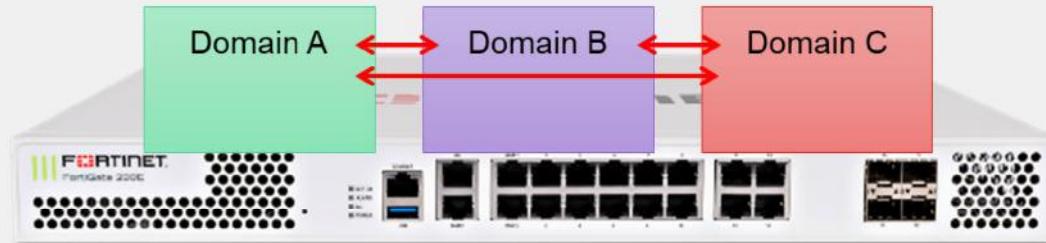
- Route traffic between VDOMs

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

By demonstrating competence in inter-VDOM links, you will be able to effectively and efficiently route traffic between VDOMs on FortiGate.

DO NOT REPRINT**© FORTINET**

Inter-VDOM Links



- Can connect different VDOMs
- Support varies by VDOM operating mode
 - NAT-to-NAT ✓
 - NAT-to-transparent and transparent-to-NAT ✓
 - Transparent-transparent (no Layer 3; potential Layer 2 loops) ✗

To review, each VDOM behaves like it is on a separate FortiGate device. With separate FortiGate devices, you would normally connect a network cable and configure routing and policies between them. But VDOMs are on the same FortiGate. So, how should you route traffic between them?

The solution is inter-VDOM links. Inter-VDOM links are a type of virtual interface that route traffic between VDOMs. This removes the need to loop a physical cable between two VDOMs.

In the case of a NAT-to-NAT inter-VDOM link, both sides of the link must be on the same IP subnet, because you are creating a point-to-point network connection.

Note that like using inter-VLAN routing, Layer 3 must be involved—you cannot create an inter-VDOM link between Layer 2 transparent mode VDOMs. At least one of the VDOMs must be operating in NAT mode. This, among other benefits, prevents potential Layer 2 loops.

DO NOT REPRINT**© FORTINET**

Inter-VDOM Links (Contd)

- Inter-VDOM links allow VDOMs to communicate
 - Traffic is not required to leave a physical interface then re-enter FortiGate
 - Fewer physical interfaces or cables are required
 - This prevents the wasting of physical interfaces, and eliminates the need for a loopback cable
- Routes are required to forward the traffic from one VDOM to another
- Firewall policies are also required to allow traffic from other VDOMs, the same as traffic coming from physical interfaces



© Fortinet Inc. All Rights Reserved.

35

When creating inter-VDOM links, you must create the virtual interfaces. You must also create the appropriate firewall policies in each VDOM, just as you would if the traffic were arriving on a network cable, otherwise, FortiGate will block it.

Additionally, routes are required to correctly route packets between two VDOMs.

DO NOT REPRINT
© FORTINET

Creating Inter-VDOM Links

The screenshot shows the FortiGate GUI under the 'Global > Network > Interfaces' section. A red arrow highlights the 'Create New' dropdown and points to the 'VDOM Link' option in the list. The 'New VDOM Link' dialog is open on the right, showing the configuration for a new interface. The interface is named 'vlink'. It has two virtual domains assigned: 'root' for Interface 0 (vlink0) and 'VDOM1' for Interface 1 (vlink1). Both interfaces have the same IP/Netmask: 10.10.100.1/30 and 10.10.100.2/30 respectively. Administrative access is configured for HTTPS, PING, SSH, and SNMP. The status for both interfaces is 'Enabled'. The dialog also includes fields for comments and security fabric connection options.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

36

On the GUI, you create a network interface in the **Global** settings. To create the virtual interface, click **Create New**, and then select **VDOM Link**.

DO NOT REPRINT**© FORTINET**

Inter-VDOM Link Acceleration

- FortiGate devices with NP4 or NP6 processors include inter-VDOM links that FortiGate can use to accelerate inter-VDOM link traffic
- For a FortiGate device with two NP4 or NP6 processors, there are two accelerated inter-VDOM links, each with two interfaces:
 - **npu0_vlink:**
 - npu0_vlink0
 - npu0_vlink1
 - **npu1_vlink:**
 - npu1_vlink0
 - npu1_vlink1
- These interfaces are visible on the GUI and CLI



© Fortinet Inc. All Rights Reserved.

37

FortiGate devices with NP4 or NP6 processors include inter-VDOM links that FortiGate can use to accelerate inter-VDOM link traffic. For a FortiGate with two NP4 or NP6 processors, there are two accelerated inter-VDOM links, each with two interfaces:

- **npu0_vlink:**
 - npu0_vlink0
 - npu0_vlink1
- **npu1_vlink:**
 - npu1_vlink0
 - npu1_vlink1

These interfaces are visible on the GUI and CLI. By default, the interfaces in each inter-VDOM link are assigned to the root VDOM. To use these interfaces to accelerate inter-VDOM link traffic, assign each interface in the pair to the VDOMs that you want to offload traffic between. For example, if you have added a VDOM named *New-VDOM* to a FortiGate with NP4 processors, you can click **System > Network > Interfaces** and edit the **npu0-vlink1** interface and set the VDOM to *New-VDOM*. This results in an accelerated inter-VDOM link between *root* and *New-VDOM*.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is a requirement for creating an inter-VDOM link between two VDOMs?
 - A. The NGFW mode of at least one VDOM must be profile based.
 - B. At least one of the VDOMs must be operating in NAT mode.

2. Which type of VDOM link requires that both sides of the link be assigned an IP address within the same subnet?
 - A. NAT-to-transparent
 - B. NAT-to-NAT

DO NOT REPRINT**© FORTINET**

Lesson Progress

**VDOM Concepts****VDOM Administrators****Configuring VDOMs****Inter-VDOM Links****Best Practices and Troubleshooting**

Good job! You now understand inter-VDOM Links.

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

DO NOT REPRINT**© FORTINET**

Best Practices and Troubleshooting

Objectives

- Limit the resources allocated globally and per VDOM
- Troubleshoot common VDOM issues

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

By demonstrating competence in VDOM best practices and troubleshooting, you will be able to prevent, identify, and solve common VDOM issues.

DO NOT REPRINT**© FORTINET**

System Resource Allocation

- Global resources limit: apply to resources that are shared by the whole FortiGate
- VDOM resources limit: per-VDOM resources are specific to each VDOM
 - Default per-VDOM resource settings are set to have **no limits**.
 - Guarantees a per-VDOM minimum resource allocation
 - No VDOM can starve the others of all the device resources



© Fortinet Inc. All Rights Reserved.

41

Remember, VDOMs are only a *logical* separation—each VDOM shares physical resources with the others.

By default, all per-VDOM resource settings are set to have no limits. This means that any single VDOM can use all of the FortiGate device's resources. This could deprive other VDOMs of the resources that they require, to the point that could be unable to function.

Unlike FortiGate-VM, VDOMs are not allocated and balanced with weighted vCPU cores, vRAM, and other virtualized hardware.

To fine-tune performance, you can configure resource limits for each feature—IPsec tunnels, address objects, and so on—at the global level and at each VDOM level. This controls the ratio of the system resource usage of each VDOM to the total available resources.

DO NOT REPRINT
© FORTINET

Global and Per-VDOM Resource Limits

The diagram illustrates a FortiGate device with three virtual domains (VDOMs): Global, VDOM1, and VDOM3. Arrows point from the 'Global' and 'VDOM3' labels to their respective configuration screens.

Global > System > Global Resources

Resource	Current Usage	Default Maximum	Override Maximum
Active Sessions	(289)	No Limit Set	<input checked="" type="checkbox"/>
Policy & Objects			
Firewall Policies	(24)	21024	<input checked="" type="checkbox"/>
Firewall Addresses	(54)	11024	<input checked="" type="checkbox"/>
Firewall Address Groups	(10)	5000	<input checked="" type="checkbox"/>
Firewall Custom Services	(107)	No Limit Set	<input checked="" type="checkbox"/>
Firewall Service Groups	(8)	No Limit Set	<input checked="" type="checkbox"/>
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>
Firewall Recurring Schedules	(5)	No Limit Set	<input checked="" type="checkbox"/>
User & Device			

Global > System > VDOM

Per-VDOM resource limits

Resource	Current Usage	Global Maximum	Override Maximum	Guaranteed
Active Sessions	(0)	No Limit Set	<input checked="" type="checkbox"/>	
Policy & Objects				
Firewall Policies	(0)	21024	<input checked="" type="checkbox"/>	
Firewall Address Groups	(0)	11024	<input checked="" type="checkbox"/>	
VPN IPsec Phase1 Tunnels	(0)	2000	<input checked="" type="checkbox"/>	1900
Firewall Service Groups	(4)	No Limit Set	<input checked="" type="checkbox"/>	
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>	

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved.

42

For example, a FortiGate with hardware powerful enough to handle up to 2000 IPsec VPN tunnels and configured with three VDOMs, could be configured as follows to meet specific criteria: VDOM1 and VDOM2 don't use IPsec VPN tunnels often. So, they are allowed to have up to 50 tunnels each. VDOM3, however, uses VPN extensively. Therefore, this FortiGate device is configured to allow VDOM3 to have up to 1900 tunnels, with 1000 guaranteed.

Configure your FortiGate device with global limits for critical features, such as sessions, policies, and so on. Then, configure each VDOM with its own quotas and minimums, within the global limits.

DO NOT REPRINT
© FORTINET

Monitoring VDOM Resources

- VDOM monitor displays:
 - CPU utilization
 - Memory utilization

Global > System > VDOM

Name	Management VDOM	NGFW Mode	Operation Mode	Status	CPU	Memory	Interfaces
customer	✗	Profile-based	NAT	Enabled	0%	7%	port3 SSL-VPN tunnel interface (ssl.customer)
root	✓	Profile-based	NAT	Enabled	0%	38%	port1 port2 port4 port5

On the GUI, you can click **Global > System > VDOM** to see the VDOM monitor. It displays the CPU and memory usage for each VDOM.

DO NOT REPRINT**© FORTINET**

VDOM Administrator Has Difficulty Gaining Access

- Confirm the administrator VDOM
- Confirm the VDOM interfaces
- Confirm the VDOM administrator's access privileges
- Confirm trusted host and IP
- Best Practices
 - Create a VDOM-specific administrator account for each VDOM
 - Avoid giving **super_admin** access

With VDOMs configured, administrators have an extra layer of permissions and may have problems accessing the desired information. If an administrator cannot gain access, check the following:

- Confirm the administrator's VDOM: each administrator account, other than the **super_admin** account, is tied to one or more specific VDOMs. That administrator is not able to access any other VDOM. It may be possible they are trying to access the wrong VDOM (one that they do not have permissions for).
- Confirm the VDOM interfaces: an administrator can access their VDOM only through interfaces that are assigned to that VDOM. If interfaces on that VDOM are disabled or unavailable, there will be no method of accessing that VDOM by its local administrator. The **super_admin** is required to either bring up the interfaces, fix the interfaces, or move another interface to that VDOM to restore access.
- Confirm the VDOM admin access: as with all FortiGate devices, administration access on the VDOM's interfaces must be enabled for the administrators of that VDOM to gain access. For example, if SSH is not enabled, that is not available to administrators. To enable admin access, the **super_admin** clicks **Global > Network > Interfaces** and enables administrator access for the interface in question.
- Confirm trusted host and IP: if trusted hosts are enabled on the administrator account, ensure the user is connecting from the correct, specified host address, and that no intermediate devices are performing NAT functions on the connection.

Best practice dictates that you should usually avoid unnecessary security holes. Do not provide **super_admin** access, if possible. Instead, restrict each administrator to their relevant domain. That way, they cannot accidentally or maliciously impact other VDOMs, and any damage or mistakes will be limited in scope.

DO NOT REPRINT**© FORTINET**

General VDOM Troubleshooting Tips

- Perform a sniffer trace

```
diagnose sniffer packet <interface_name> '<filter>' <verbose> <count>
```

- Perform a packet flow trace

```
diagnose debug enable
diagnose debug flow filter addr <PC1>
diagnose debug flow trace start 100
```

Besides ping and traceroute, there are additional tools for troubleshooting your VDOM configurations. The primary tools for VDOM troubleshooting include packet sniffing and debugging the packet flow.

- Perform a sniffer trace: when troubleshooting networks, it helps to look inside the headers of packets to determine if they are traveling along the expected route. Packet sniffing can also be called a network tap, packet capture, or logic analyzing. The sniffer also indicates what traffic is entering or leaving the egress and ingress interfaces in all VDOMS. This makes it extremely useful for troubleshooting inter-VDOM routing issues.
- Debug the packet flow: traffic should enter and leave the VDOM. If you have identified that network traffic is not entering and leaving the VDOM as expected, debug the packet flow. You can debug only using CLI commands. This tool provides more granular details for help in troubleshooting inter-VDOM traffic because it gives details of routing selection, NAT, and policy selection.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Of these options, what is a possible reason why an administrator might not be able to gain access to a specific VDOM?
 A. The administrator is using an IP address that is not specified as a trusted host.
 B. The administrator is using the super_admin profile.

2. Which troubleshooting tool is most suitable when trying to verify the firewall policy used by an inter-VDOM link?
 A. Sniffer trace
 B. Packet flow trace

DO NOT REPRINT**© FORTINET**

Lesson Progress

**VDOM Concepts****VDOM Administrators****Configuring VDOMs****Inter-VDOM Links****Best Practices and Troubleshooting**

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Define and describe VDOMs
- ✓ Create administrative accounts with access limited to one or more VDOMs
- ✓ Configure VDOMs to split FortiGate into multiple virtual devices
- ✓ Route traffic between VDOMs
- ✓ Limit the resources allocated globally and per VDOM

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

By mastering the objectives covered in this lesson, you learned how to configure VDOMs, and examined examples of common use.

DO NOT REPRINT

© FORTINET



FortiGate Infrastructure

Fortinet Single Sign-On (FSSO)



Last Modified: 13 June 2022

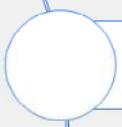
In this lesson, you will learn about Fortinet single sign-on (FSSO). When you use this feature, your users don't need to log on each time they access a different network resource.

DO NOT REPRINT**© FORTINET**

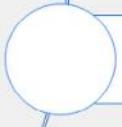
Lesson Overview



FSSO Function and Deployment



FSSO With Active Directory



FSSO Settings



Troubleshooting

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

DO NOT REPRINT**© FORTINET**

FSSO Function and Deployment

Objectives

- Define single sign-on (SSO) and Fortinet single sign-on (FSSO)
- Understand FSSO deployment and configuration

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

By demonstrating competence in understanding SSO concepts, you will be able to more effectively understand FSSO methods.

DO NOT REPRINT**© FORTINET**

SSO and FSSO

- SSO is a process that allows identified users access to multiple applications without having to re-authenticate
- Users who are already identified can access applications without being prompted to provide credentials
 - FSSO software identifies a user's user ID, IP address, and group membership
 - FortiGate allows access based on membership in FSSO groups configured on FortiGate
 - FSSO groups can be mapped to individual users, user groups, organizational units (OUs), or a combination of them
- Each FSSO method gathers login events differently
- FSSO is typically used with directory services, such as Windows Active Directory or Novell eDirectory



© Fortinet Inc. All Rights Reserved.

4

SSO is a process that allows users to be automatically logged in to every application after being identified, regardless of platform, technology, and domain.

FSSO is a software agent that enables FortiGate to identify network users for security policies or for VPN access, in advanced deployments with FortiAuthenticator, without asking for their username and password. When a user logs in to a directory service, the FSSO agent sends FortiGate the username, the IP address, and the list of groups that the user belongs to. FortiGate uses this information to maintain a local database of usernames, IP addresses, and group mappings.

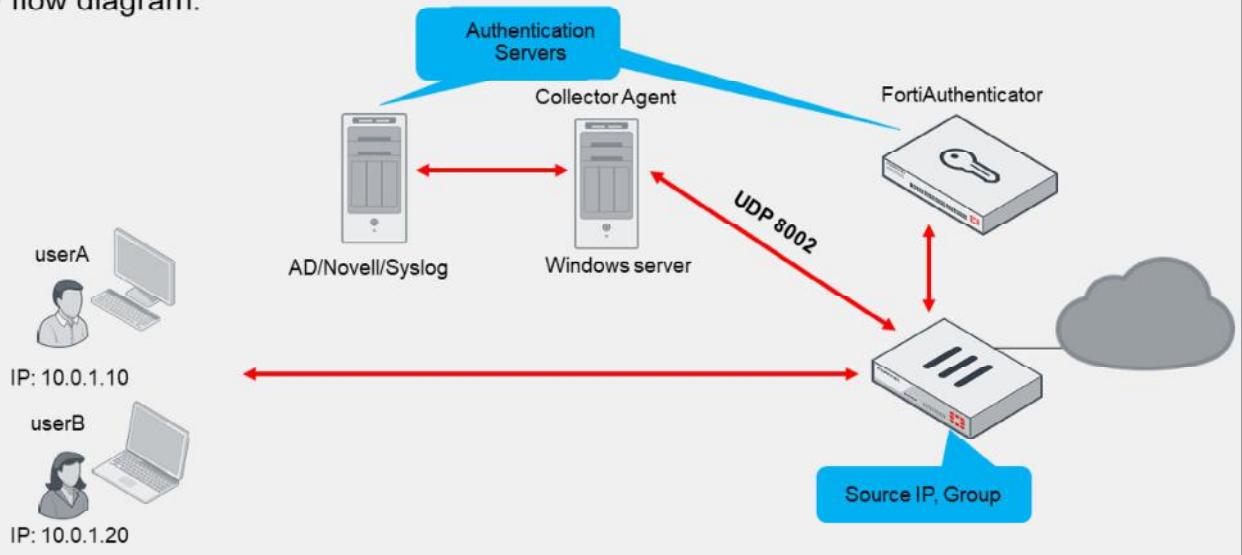
Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSSO is typically used with directory service networks such as Windows Active Directory or Novell eDirectory.

DO NOT REPRINT**© FORTINET**

FSSO—Flow Chart

- FSSO flow diagram:



This slide shows the FSSO flow we discussed in the previous slide.

DO NOT REPRINT**© FORTINET**

FSSO Deployment and Configuration



Microsoft

Active Directory

Microsoft Active Directory (AD)

- Domain controller (DC) agent mode
- Polling mode:
 - Collector agent-based
 - Agentless
- Terminal server (TS) agent
 - Enhances login capabilities of a collector agent or FortiAuthenticator
 - Gathers logins for Citrix and terminal servers where multiple users share the same IP address



Novell eDirectory

- eDirectory agent mode
- Uses Novell API or LDAP setting

How you deploy and configure FSSO depends on the server that provides your directory services.

FSSO for Windows Active Directory (AD) uses a collector agent. Domain controller (DC) agents may also be required, depending on the collector agent working mode. There are two working modes that monitor user sign-on activities in Windows: DC agent mode and polling mode. FortiGate also offers a polling mode that does not require a collector agent, which is intended for simple networks with a minimal number of users.

There is another kind of DC agent that is used exclusively for Citrix and terminal services environments: terminal server (TS) agents. TS agents require the Windows Active Directory collector agent or FortiAuthenticator to collect and send the login events to FortiGate.

The eDirectory agent is installed on a Novell network to monitor user sign-ons and send the required information to FortiGate. It functions much like the collector agent on a Windows AD domain controller. The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. In FSSO, FortiGate allows network access based on _____.
 A. Active user authentication with username and password
 B. Passive user identification by user ID, IP address, and group membership

2. Which working mode is used for monitoring user sign-on activities in Windows AD?
 A. Polling mode (collector agent-based or agentless)
 B. eDirectory agent mode

DO NOT REPRINT**© FORTINET**

Lesson Progress



FSSO Function and Deployment



FSSO With Windows Active Directory



FSSO Settings



Troubleshooting

Good job! You now understand basic concepts about the function of FSSO and how it is deployed.

Now, you'll learn about user login events in Windows Active Directory using FSSO.

DO NOT REPRINT**© FORTINET**

FSSO With Windows Active Directory

Objectives

- Detect user login events in Windows AD using FSSO
- Identify FSSO modes for Windows AD

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

By demonstrating competence in understanding the different ways you can configure FSSO for Windows AD, you will be better able to design the architecture of your SSO system.

DO NOT REPRINT**© FORTINET**

DC Agent Mode

- DC agent mode is the most scalable mode and is, in most environments, the recommended mode for FSSO
- Requires one DC agent (dcagent.dll) installed on each Windows DC in the Windows\system32 directory. The DC agent is responsible for:
 - Monitoring user login events and forwarding them to the collector agents
 - Handling DNS lookups (by default)
- Requires one or more collector agents installed on Windows servers. The collector agent is responsible for:
 - Group verification
 - Workstation checks
 - Updates of login records on FortiGate
 - Sending domain local security group, organizational units (OUs), and global security group information to FortiGate



© Fortinet Inc. All Rights Reserved.

10

DC agent mode is considered the recommended mode for FSSO.

DC agent mode requires:

- One DC agent installed on each Windows DC

If you have multiple DCs, this means that you need multiple DC agents. DC agents monitor and forward user login events to the collector agents.
- A collector agent, which is another FSSO component

The collector agent is installed on a Windows server that is a member of the domain you are trying to monitor. It consolidates events received from the DC agents, then forwards them to FortiGate. The collector agent is responsible for group verification, workstation checks, and FortiGate updates of login records. The FSSO collector agent can send domain local security group, organizational units (OUs), and global security group information to FortiGate devices. It can also be customized for DNS lookups.

When the user logs on, the DC agent intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

The collector agent receives it and then performs a DNS resolution in order to check if the IP of the user has changed.

In some configurations, double DNS resolution is a problem. In this case, you may configure a registry key on the domain controller that hosts the DC agent in order not to resolve the DNS:

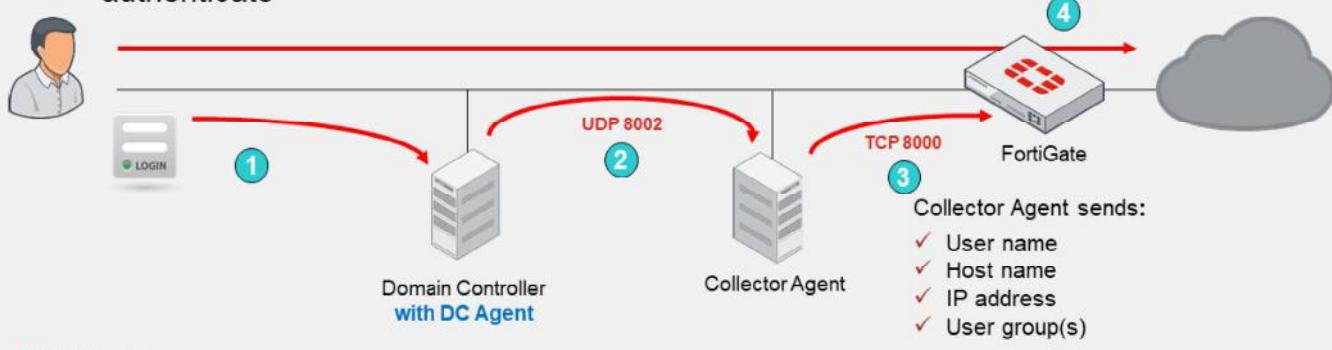
```
donot_resolve = (DWORD) 1 at HKLM\Software\Fortinet\FSAE/dcagent
```

DO NOT REPRINT

© FORTINET

DC Agent Mode Process

1. The user authenticates against the Windows DC
2. The DC agent sees the login event and forwards it to the collector agent
3. The collector agent receives the event from the DC agent and forwards it to FortiGate
4. FortiGate knows the user based on their IP address, so the user does not need to authenticate



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

This slide shows the process of information passing between DC agents, the collector agent, and a FortiGate configured for FSSO authentication.

1. When users authenticate with the DC, they provide their credentials.
2. The DC agent sees the login event, and forwards it to the collector agent.
3. The collector agent aggregates all login events and forwards that information to FortiGate. The information sent by the collector agent contains the user name, host name, IP address, and user group(s). The collector agent communicates with FortiGate over TCP port 8000 (default) and it listens on UDP port 8002 (default), for updates from the DC agents. The ports are customizable.
4. FortiGate learns from the collector agent who the user is, their IP address, and some of the AD groups that the user is a member of. When a user tries to access the internet, FortiGate compares the source IP address to its list of active FSSO users. Because the user in this case has already logged in to the domain, and FortiGate already has their information, FortiGate doesn't prompt the user to authenticate again. Rather it allows or denies the traffic based on the matching firewall policy.

DO NOT REPRINT**© FORTINET**

Collector Agent-Based Polling Mode

- A collector agent must be installed on a Windows server
 - No FSSO DC agent is required
- Every few seconds, the collector agent polls each DC for user login events. The collector agent uses:
 - SMB (TCP 445) protocol, by default, to request the event logs
 - TCP 135, TCP 139, and UDP 137 as fallbacks
- This mode requires a less complex installation, which reduces ongoing maintenance
- Three methods:
 - NetAPI
 - WinSecLog
 - WMI
- Event logging must be enabled on the DCs (except in NetAPI)

Polling mode can be collector agent-based or agentless.

First, you'll look at the collector agent-based polling mode. Like DC agent mode, collector agent-based mode requires a collector agent to be installed on a Windows server, but it *doesn't* require DC agents to be installed on each DC. In collector agent-based polling mode, the collector agent must be more powerful than the collector agent in DC agent mode, and it also generates unnecessary traffic when there have been no login events.

In Windows Event Log Polling, the most commonly deployed polling mode, the collector agent uses the SMB (TCP port 445) protocol to periodically request event logs from the domain controllers. Other methods may gather information differently, but after the login is received by the collector agent, the collector agent parses the data and builds the user login database, which consists of usernames, workstation names/IP addresses, and user group memberships. This information is then ready to be sent to FortiGate.

DO NOT REPRINT**© FORTINET**

Collector Agent-Based Polling Mode Options

WMI

- DC returns all requested login events every 3 seconds*
 - Reads selected event logs
- Improves WinSec bandwidth usage
 - Reduces network load between collector agent and DC

WinSecLog

- Polls all security events on DC every 10 seconds, or more*
 - Log latency if network is large or system is slow
 - Requires fast network links
- Slower, but...
 - Sees all login events
 - Only parses known event IDs by collector agent

NetAPI

- Polls the NetSessionEnum function on Windows every 9 seconds, or less*
 - Authentication session table in RAM
- Retrieves login sessions, including DC login events
- Faster, but...
 - If DC has heavy system load, can miss some login events

Most recommended → Least recommended

* The poll interval times are estimates. The interval times depend on the number of servers and network latency.

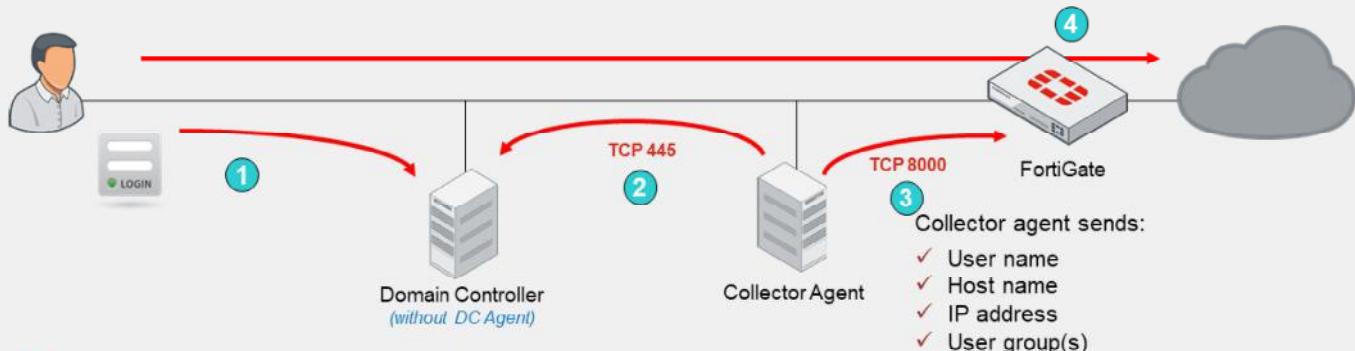
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **WMI:** is a Windows API that gets system information from a Windows server. The DC returns all requested login events. The collector agent is a WMI client and sends WMI queries for user login events to the DC, which, in this case, is a WMI server. The collector agent doesn't need to search security event logs on the DC for user login events; instead, the DC returns all requested login events. This reduces network load between the collector agent and DC.
- **WinSecLog:** polls all the security event logs from the DC. It doesn't miss any login events that have been recorded by the DC because events are not normally deleted from the logs. There can be some delay in FortiGate receiving events if the network is large and, therefore, writing to the logs is slow. It also requires that the audit success of specific event IDs is recorded in the Windows security logs. For a full list of supported event IDs, visit the Fortinet Knowledge Base (<http://kb.fortinet.com>).
- **NetAPI:** polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some login events if a DC is under heavy system load. This is because sessions can be quickly created and purged from RAM, before the agent has a chance to poll and notify FortiGate.

DO NOT REPRINT
© FORTINET

Collector Agent-Based Polling Mode Process

1. The user authenticates with the DC
2. The collector agent frequently polls the DCs to collect user login events
3. The collector agent forwards logins to FortiGate
4. The user does not need to authenticate



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

14

This slide shows an example of FSSO using the collector agent-based polling mode. This example includes a DC, a collector agent, and FortiGate, but the DC doesn't have the dcagent (or, alternatively, dcagent.dll) installed.

1. The user authenticates with the DC, providing their credentials.
2. The collector agent periodically (every few seconds) polls TCP port 445 of each DC directly, to ask if anyone has logged in.
3. The collector agent sends login information to FortiGate over TCP port 8000. This is the same information that is sent in DC agent mode.
4. When user traffic arrives at FortiGate, FortiGate already knows which users are at which IP addresses, and no repeated authentication is required.

DO NOT REPRINT**© FORTINET**

Agentless Polling Mode

- Similar to agent-based polling, but FortiGate polls instead
- Doesn't require an external DC agent or collector agent
 - FortiGate collects the data directly
- Event logging must be enabled on the DCs
- More CPU and RAM required by FortiGate
- Support for polling option WinSecLog only
 - FortiGate uses the SMB protocol to read the event viewer logs
- Fewer available features than collector agent-based polling mode
- FortiGate doesn't poll workstation
 - Workstation verification is not available in agentless polling mode

You can deploy FSSO without installing an agent. FortiGate polls the DCs directly, instead of receiving login information indirectly from a collector agent.

Because FortiGate collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

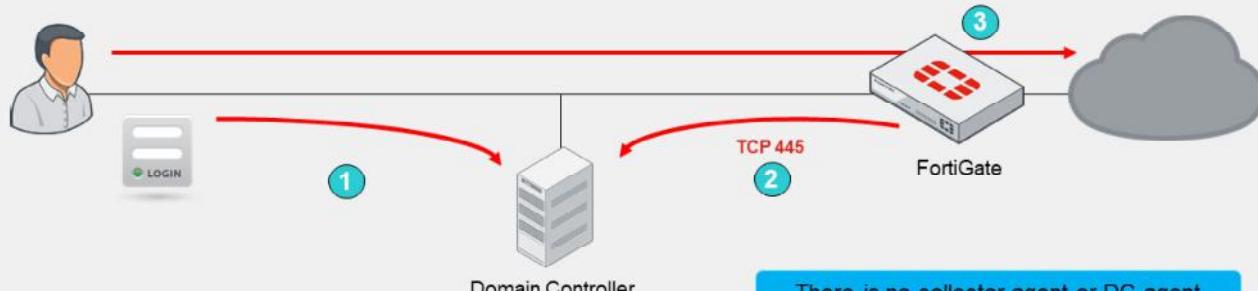
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

In agentless polling mode, FortiGate acts as a collector. It is responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

DO NOT REPRINT
© FORTINET

Agentless Polling Mode Process

1. FortiGate frequently polls DCs to collect user login events
2. The user authenticates with the DC
 - o FortiGate discovers the login event in next poll
3. The user does not need to authenticate
 - o FortiGate already knows whose traffic it is receiving



This slide shows how communication is processed without agents. (There is no collector agent or DC agent.)

1. FortiGate polls the DC TCP port 445 to collect user login events.
2. After the user authenticates with the DC, FortiGate registers a login event during its next poll, obtaining the following information: the user name, the host name, and the IP address. FortiGate then queries for the user's user group(s).
3. When the user sends traffic, FortiGate already knows whose traffic it is receiving; therefore, the user does not need to authenticate.

DO NOT REPRINT**© FORTINET**

Comparing Modes

	DC agent mode	Polling mode
Installation	Complex—multiple installations (one per DC). Requires reboot.	Easy—one or no installations. No reboot required.
DC agent required	Yes	No
Resources	Shares with DC agents	Has own resources
Scalability	Higher	Lower
Redundancy	Yes	Yes
Level of confidence	Captures all logins	Might miss a login (NetAPI), or have a delay (WinSecLog)

This table summarizes the main differences between DC agent mode and polling mode.

DC agent mode is more complex. It requires not only a collector agent, but also a DC agent for each monitored domain controller. However, it is also more scalable because the work of capturing logins is done by the DC agents who pass their information directly to the collector.

In polling mode, the collector needs to query every domain controller, every few seconds. So, with each DC that is added, the number of queries grows. If you want to add a second collector agent for redundancy in polling mode, both collector agents need to query every DC individually.

In DC agent mode, the DC agent just has to collect the log once, and send a copy of the necessary information to all the collector agents. In comparison, if you use polling mode, some login events might be missed or delayed, depending on the polling option used.

You do not have to install a collector agent on the DC, you can install it on any Windows machine on the network.

DO NOT REPRINT**© FORTINET**

Additional FSSO AD Requirements

- The DNS server must be able to resolve all workstation names
 - Microsoft login events contain workstation names, but might not IP addresses
 - The collector agent uses a DNS server to resolve the workstation name to an IP address
- For full feature functionality, the collector agent must be able to poll workstations
 - This informs the collector agents whether or not the user is still logged in
 - TCP ports 445 (default) and 139 (backup) must be open between collector agents or FortiGate and all hosts
 - Remote registry service might be needed on each workstation

Regardless of the collector method you choose, some FSSO requirements for your AD network are the same:

- Microsoft Windows login events have the workstation name and username, but not the workstation IP address. When the collector agent receives a login event, it queries a DNS server to resolve the IP address of the workstation. So, FSSO requires that you have your own DNS server. If a workstation IP address changes, DNS records must be updated immediately in order for the collector agent to be aware of the change and report them to FortiGate.
- For full feature functionality, collector agents need connectivity with all workstations. Since a monitored event log is not generated on logout, the collector agent (depending on the FSSO mode) must use a different method to verify whether users are still logged in. So, each user workstation is polled to see if users are still there.
- The DC agent, when the user logs in, intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

The collector agent receives the DNS and then performs a DNS resolution in order to check if the IP of the user has changed.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which is the recommended mode for FSSO deployments?
 A. DC agent mode
 B. Polling mode: Agentless

2. Which FSSO mode requires more FortiGate system resources (CPU and RAM)?
 A. Polling mode: Collector agent-based
 B. Polling mode: Agentless

DO NOT REPRINT**© FORTINET**

Lesson Progress

**FSSO Function and Deployment****FSSO With Windows Active Directory****FSSO Settings****Troubleshooting**

Good job! You now understand how FortiGate detects login events in Windows Active Directory (AD) using FSSO.

Now, you'll learn how to configure FSSO settings.

DO NOT REPRINT**© FORTINET**

FSSO Settings

Objectives

- Configure SSO settings on FortiGate
- Install FSSO agents
- Configure the Fortinet collector agent

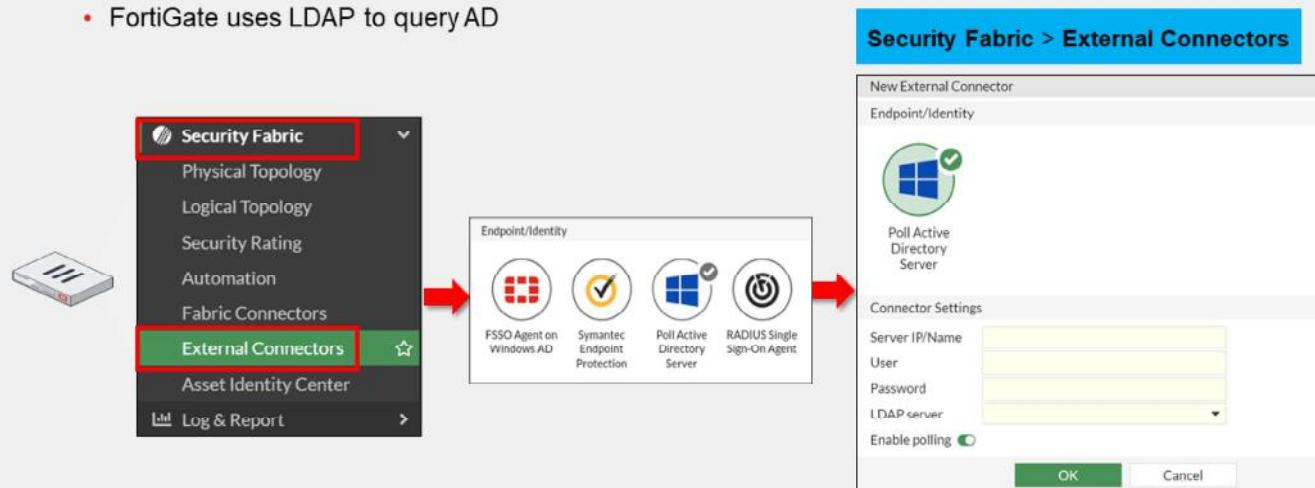
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring the FSSO settings on FortiGate, and installing and configuring the FSSO agents, you will be able to implement FSSO within your network.

DO NOT REPRINT
© FORTINET

FSSO Configuration—Agentless Polling Mode

- Agentless polling mode:
 - FortiGate uses LDAP to query AD



FortiGate FSSO configuration is straightforward.

If FortiGate is acting as a collector for agentless polling mode, you must select **Poll Active Directory Server** and configure the IP addresses and AD administrator credentials for each DC.

FortiGate uses LDAP to query AD to retrieve user group information. For this to happen, you must add the LDAP server to the **Poll Active Directory Server** configuration.

DO NOT REPRINT

© FORTINET

FSSO Configuration—Collector Agent-Based Polling or DC Agent Mode

- Collector agent-based polling or DC agent mode:
 - The FSSO agent can monitor users' login information from AD, Exchange, Terminal, Citrix, and eDirectory servers

The screenshot shows the 'Security Fabric > External Connectors' section. On the left, under 'Endpoint/Identity', there are four icons: 'FSSO Agent on Windows AD' (selected), 'Symantec Endpoint Protection', 'Poll Active Directory Server', and 'RADIUS Single Sign-On Agent'. A red arrow points from the 'FSSO Agent on Windows AD' icon to the 'User group source' dropdown in the configuration dialog. The configuration dialog is titled 'New External Connector' and shows the following settings:

- User group source:** Collector Agent Local (highlighted with a red box)
- LDAP server:** (dropdown menu)
- Proactively retrieve from LDAP server:** (radio button)
- Connector Settings:**
 - Name:** (input field)
 - Primary FSSO agent:** (input field) Server IP/Name, with a 'Password' field and a '+' button.
 - Trusted SSL certificate:** (checkbox)
 - User group source:** (dropdown menu) Collector Agent Local (highlighted with a red box)
 - Users/Groups:** 0
- Buttons:** Apply & Refresh, OK, Cancel

At the bottom of the interface, it says '© Fortinet Inc. All Rights Reserved.' and '23'.

If you have collector agents, using either the DC agent mode or the collector agent-based polling mode, you must select **Fortinet Single-Sign-On Agent** and configure the IP address and password for each collector agent.

The FSSO collector agent can access Windows AD in one of two modes:

- **Collector Agent:** You create group filters are created on the collector agent. You can set FortiGate to **Collector Agent** mode, and the collector agent can still use **Advanced** mode to access nested groups.
- **Local:** You create group filters on FortiGate, using the LDAP server. If you set FortiGate to **Local** mode, you must set the collector agent to **Advanced** mode, otherwise the collector agent does not recognize the group filter sent by FortiGate and does not pass down any user logins.

DO NOT REPRINT

© FORTINET

FSSO Agent Installation

1. Visit the Fortinet support website:
 - <https://support.fortinet.com>
2. Click **Download > Firmware Images**
3. Select **FortiGate**, then click **Download**.
4. Click **v7.00 > 7.2 > 7.2.0 > FSSO**

Example image below:

The screenshot shows the Fortinet Support website interface. At the top, there is a navigation bar with links for Home, Asset Assistance, Download (which is highlighted in red), and Feedback. Below the navigation bar, there is a 'Customer Service & Support' section with a 'Welcome' message and links for Home, Firmware Images (which is highlighted in red), Firmware Image Checksums, and HQIP Images. The main content area is titled 'Select Product' and shows a dropdown menu for 'FortiGate'. Below the dropdown are buttons for 'Release Notes', 'Download' (which is highlighted in blue), 'Upgrade Path', and 'FortiGate Support Tool'. The 'Image File Path' field contains the URL '/FortiGate/v7.00/7.2/7.2.0/FSSO/'. The 'Image Folders/Files' section shows a table of files with the following data:

Name	Size (KB)	Date Created	Date Modified	HTTPS Checksum
DCAgent_Setup_5.0.0295.exe	3,445	2021-03-30 16:03:42	2021-03-30 16:03:43	HTTPS Checksum
DCAgent_Setup_5.0.0295.msi	3,112	2021-03-30 16:03:47	2021-03-30 16:03:48	HTTPS Checksum
DCAgent_Setup_5.0.0295_x64.exe	4,105	2021-03-30 16:03:53	2021-03-30 16:03:55	HTTPS Checksum
DCAgent_Setup_5.0.0295_x64.msi	3,772	2021-03-30 16:03:58	2021-03-30 16:03:59	HTTPS Checksum
FSSO_Setup_5.0.0295.exe	9,617	2021-03-30 16:03:36	2021-03-30 16:03:39	HTTPS Checksum
FSSO_Setup_5.0.0295_x64.exe	9,909	2021-03-30 16:03:04	2021-03-30 16:03:07	HTTPS Checksum
FSSO_Setup_x64.exe	3,549	2021-03-30 16:03:56	2021-03-30 16:03:57	HTTPS Checksum
FSSO500WATs_build0295.sum	1	2021-03-30 16:03:45	2021-03-30 16:03:45	HTTPS Checksum
TSAgent_Setup_5.0.0295.exe	4,465	2021-03-30 14:03:01	2021-03-30 14:03:03	HTTPS Checksum
TSAgent_Setup_5.0.0295.msi	4,132	2021-03-30 16:03:50	2021-03-30 16:03:52	HTTPS Checksum

Available agents:

- DC agent: DCAgent_Setup
- CA for Microsoft servers: FSSO_Setup
- CA for Novell: FSSO_Setup_edirectory
- TS Agent: TAgent_Setup

The FSSO agents are available on the Fortinet Support website. There you will find the following:

- The DC agent
- The collector agent for Microsoft servers: FSSO_Setup
- The collector agent for Novell directories: FSSO_Setup_edirectory
- The terminal server agent (TAgent) installer for Citrix and terminal servers: TAgent_Setup

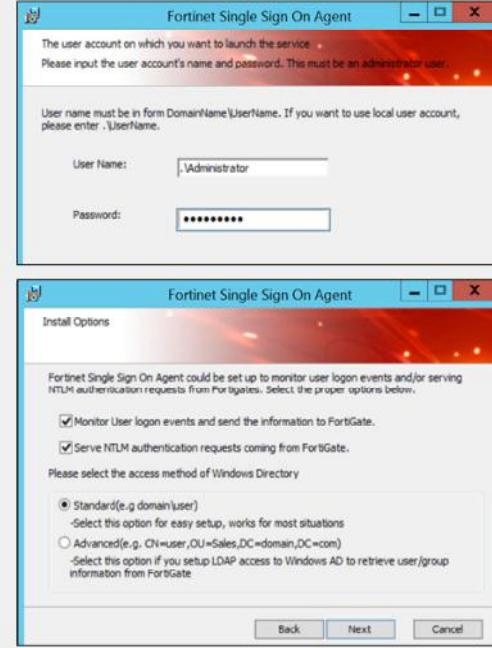
Also, for each agent, there are two versions: the executable (.exe) and Microsoft Installer (.msi).

Notice that you do not need to match the FSSO version with your exact FortiGate firmware version. When installing FSSO, grab the latest collector agent for your major release. You do however, need to match the DC agent version to the collector agent version.

DO NOT REPRINT
© FORTINET

FSSO Collector Agent Installation Process

1. Run the installation process as Administrator
2. Enter the user name in the following format:
 - DomainName\UserName
3. Configure the collector agent for:
 - Monitoring logins
 - NTLM authentication
 - Directory access
4. Optionally, launch the DC agent installation wizard before exiting the collector agent installation wizard



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

25

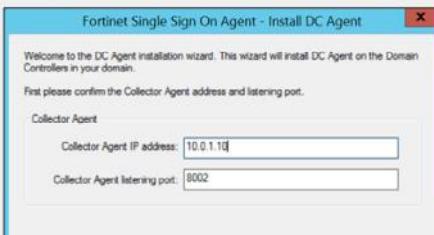
After you've downloaded the collector agent, run the installation process as Administrator and follow these steps in the installation wizard:

1. Read and accept the license agreement.
2. Optionally, change the installation location. The default folder is named **FSAE** (Fortinet Server Authentication Extension).
3. Enter the username. By default, the agent uses the name of the currently running account; however, you can change it using the format: **DomainName\UserName**.
4. Alternatively, configure your collector agent for monitoring, NTLM authentication, and directory access. These options are also customizable after installation. Although the default is **Standard** mode, when doing new FSSO setups it is always a best practice to install in **Advanced** mode. You will look at some of the advantages in this lesson.
5. If you want to use DC agent mode, make sure that **Launch DC Agent Install Wizard** is selected. This automatically starts the DC agent installation.

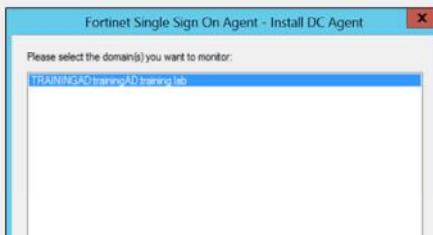
DO NOT REPRINT
© FORTINET

DC Agent Installation Process

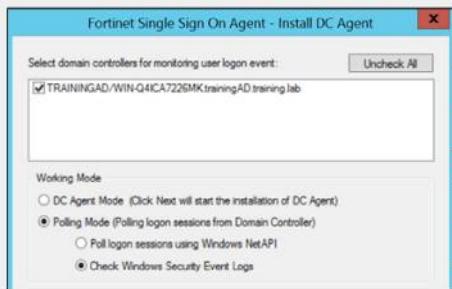
1 IP and port for collector agent



2 Domains to monitor



3 Remove users



4 Select domain controllers to install the DC agent

5 **DC Agent Mode** – to install DC agent on selected DC
Polling Mode – DC agent will not be installed

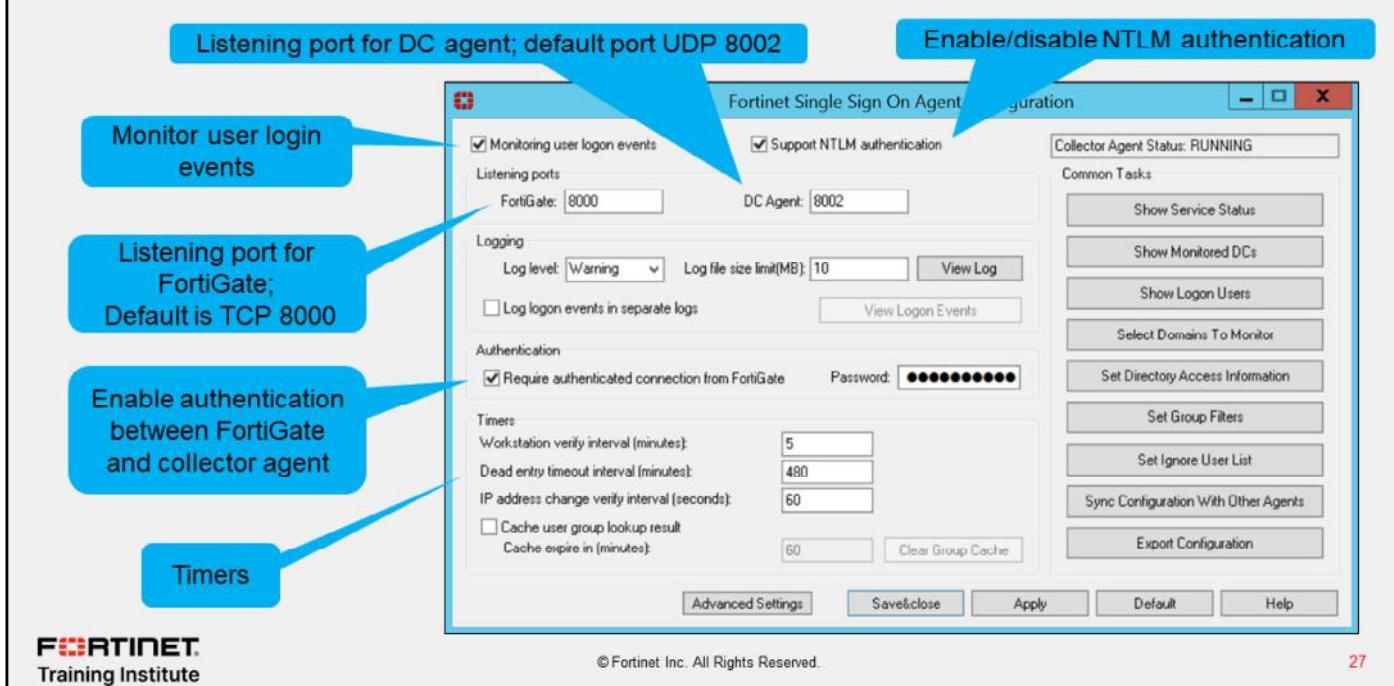
If you have just installed the collector agent and you selected **Launch DC Agent Install Wizard**, the installation process for domain controller agent automatically starts.

1. Enter the IP address for the collector agent. Optionally, you can customize the listening port, if the default value is already used by another service.
2. Select the domains to monitor. If any of your required domains are not listed, cancel the wizard and set up the correct trusted relationship with the domain controller. Then, run the wizard again. Note that this could also be a result of using an account without all the necessary permissions.
3. Optionally, select users that you do not want to monitor; these users' login events are not recorded by the collector and therefore are not passed to FortiGate. While these users are still able to generate login events to the domain, when they are detected by the collector agent, they are discarded so as to not interfere with the logged in user. This is especially useful in environments with a centrally managed antivirus solution, or a scheduled backup service that uses an AD account to start. These accounts can create login events for the collector agent that overwrite existing user logins. This may result in FortiGate applying the incorrect policies and profiles based on the overriding account. You can also customize the option to ignore users after installation is complete.
4. Optionally, clear the checkboxes of domain controllers that you don't want to install the DC agent on. Remember, for DC agent mode FSSO, at least one domain controller must have the DC agent installed. Also remember that installing the DC agent requires a reboot of the DC before it will start gathering login events. You can add or remove the DC agent to DCs at any time after the installation is complete.
5. Select **DC Agent Mode** as the working mode. If you select **Polling Mode**, the DC agent will not be installed.

Finally, the wizard requests a system reboot.

DO NOT REPRINT
© FORTINET

FSSO Collector Agent Configuration



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

27

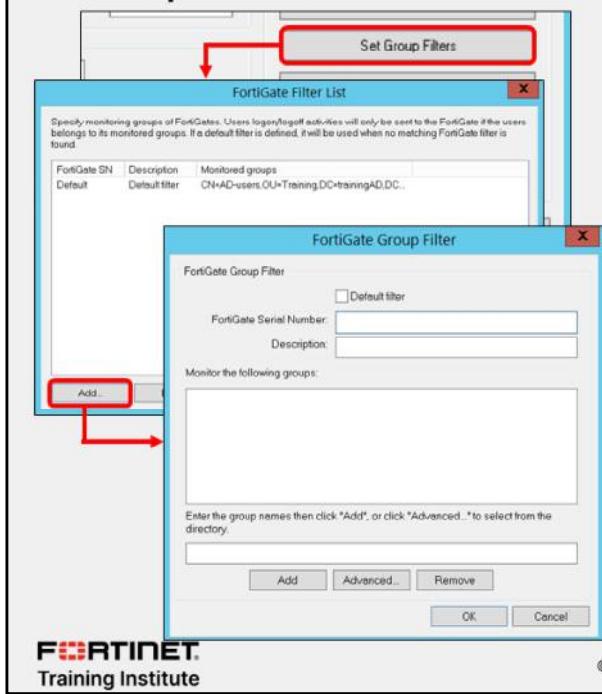
On the FSSO agent configuration GUI, you can configure settings such as:

- The listening port for the communication with the DC agents (UDP)
- The listening port for the communication with FortiGate (TCP)
- NTLM authentication support
- Password authentication between the collector agent and FortiGate
- Timers

DO NOT REPRINT

© FORTINET

Group Filter



- The FSSO collector agent manages FortiGate group filters
- FortiGate group filters control which user's login information is sent to that FortiGate device
 - Filters are tied to the FortiGate serial number
- All FortiGate devices support at least 256 Windows AD user groups
 - The group filter support is for VDOMs
- If FortiGate FSSO is set up in user group source local mode (group filtering configured on FortiGate is pushed to Collector agent), FortiGate filter will take precedence over filter set on collector agent
- The default filter applies to any FortiGate device that does not have a specific filter defined in the list
- You can set filters for groups, OUs, users, or a combination

© Fortinet Inc. All Rights Reserved.

28

The FSSO collector agent allows you to configure a FortiGate group filter, which actively controls what user login information is sent to each FortiGate device. So, you can define which groups the collector agent passes to individual FortiGate devices.

Monitoring the entire group list in a large AD structure is highly inefficient, and a waste of resources. Most FSSO deployments need group segmentation (at least four or five groups), with the intention of assigning varying levels of security profile configurations to the different groups, using identity-based policies.

Group filters also help to limit the traffic sent to FortiGate. The maximum number of Windows AD user groups allowed on FortiGate depends on the model. Low-end FortiGate models support 256 Windows AD user groups. Mid-range and high-end models can support more groups. This is per VDOM, if VDOMs are enabled on FortiGate.

You can filter on FortiGate instead of the collector agent, but only if the collector agent is operating in advanced mode. In this case, the collector agent uses the list of groups you selected on FortiGate as its group filter for that device.

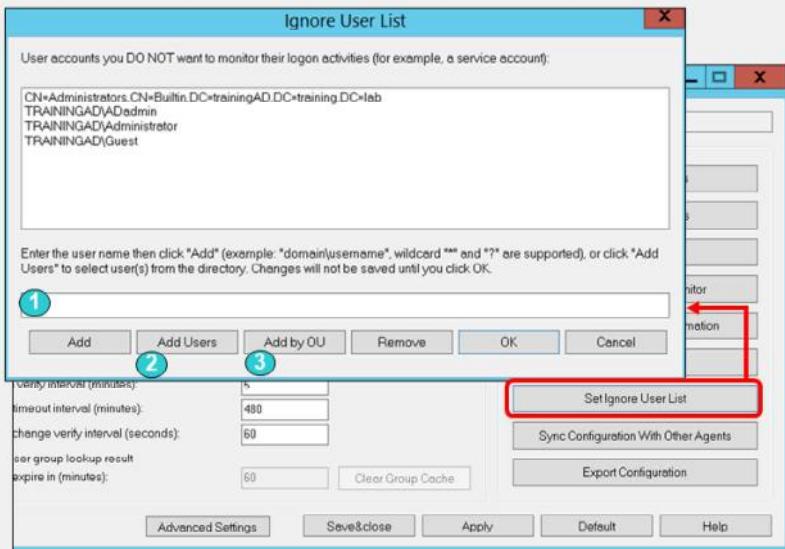
The filter list is initially empty. At a minimum, you should create a default filter that applies to all FortiGate devices without a defined filter.

Note that if you change the AD access mode from **Standard** to **Advanced** or **Advanced** to **Standard**, you must recreate the filters because they vary depending on the mode.

DO NOT REPRINT

© FORTINET

Ignored User List



- The collector agent ignores any login events that match the **Ignore User List** entries
 - Example: network service accounts
- User logins are not reported to FortiGate
- This helps to ensure users get the correct policies and profiles on FortiGate

To add users to the ignore list:

1. Manual entry
2. **Add Users:** Select users you do not want to monitor
3. **Add by OU:** Select an OU from the directory tree
 - All users under the selected OU are added to the **Ignore User List**

The FSSO collector agent ignores any login events that match the **Ignore User List** entries. Therefore, these login events are not recorded by the collector agent, nor are they reported to FortiGate.

It is a good practice to add all network service accounts to the **Ignore User List**. Service accounts tend to overwrite user login events, and create issues with identity-based policy matching.

You can add users to the **Ignore Users List** in the following ways:

- Manually enter the username.
- Click **Add Users**, and then choose the users you do not want to monitor.
- Click **Add by OU**, and then select an OU from the directory tree.

DO NOT REPRINT**© FORTINET**

Collector Agent Timers

Workstation verify interval

- Verifies if a user is still logged on
- Uses remote registry service to verify
- Default: 5 minutes
- Disable: Set value to 0

Timers

Workstation verify interval [minutes]:	5
Dead entry timeout interval [minutes]:	480
IP address change verify interval [seconds]:	60
<input type="checkbox"/> Cache user group lookup result	
Cache expire in [minutes]:	60

IP address change verify interval

- Important on DHCP or dynamic environments
- Default – 60 seconds

Dead entry timeout interval

- Applies to unverified entries only
- Used to purge login information
- Default: 480 minutes (8h)
- Disable: Set value to 0

• Under the workstation verify interval

Cache user group lookup result

- Collector agent remembers user group membership

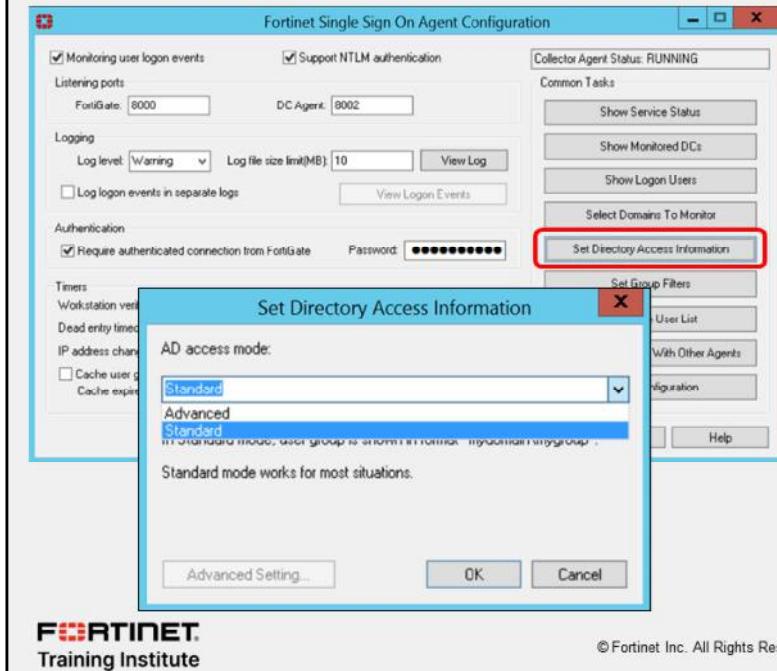
The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

Now, you'll take a look at each one and how they work.

- **Workstation verify interval.** This setting controls when the collector agent connects to individual workstations on port 139 (or port 445), and uses the remote registry service to verify if a user is still logged in to the same station. It changes the status of the user under **Show login User**, to **not verified** when it cannot connect to the workstation. If it does connect, it verifies the user and the status remains **OK**. To facilitate this verification process, you should set the remote registry service to auto start on all domain member PCs.
- **Dead entry timeout interval.** This setting applies only to entries with an unverified status. When an entry is not verified, the collector starts this timer. It's used to age out the entry. When the timer expires, the login is removed from the collector. From the perspective of FortiGate, there is no difference between entries that are **OK** and entries that are **not verified**. Both are considered valid.
- **IP address change verify interval.** This setting checks the IP addresses of logged in users and updates FortiGate when a user's IP address changes. This timer is especially important in DHCP or dynamic environments to prevent users from being locked out if they change IP address. The domain DNS server should be accurate; if the DNS server does not update the affected records promptly, the collector agent's IP information is inaccurate.
- **Cache user group lookup result.** This setting caches the user group membership for a defined period of time. It is not updated, even if the user changes group membership in AD.

DO NOT REPRINT
© FORTINET

AD Access Mode Configuration



Standard Access Mode

- Windows convention:
 - Domain\groups
- UTM profiles to groups
 - Nested group is not supported
- Group filters at collector agent

Advanced Access Mode

- LDAP convention user names:
 - CN=User, OU=Name, DC=Domain
- UTM profile to users, groups and OUs
 - Supports nested or inherited groups
- Group filtering:
 - FortiGate as an LDAP client, or group filter on collector agent
 - Filter groups defined on FortiGate

Another important FSSO setting is the AD access mode. You can set the AD access mode by clicking **Set Directory Access Information**. The AD access mode specifies how the collector agent accesses and collects the user and user group information. There are two modes that you can use to access AD user information: **Standard** and **Advanced**.

The main difference between modes is the naming convention used:

- **Standard** mode uses the Windows convention, NetBios: Domain\groups, while
- **Advanced** mode uses the LDAP convention: CN=User, OU=Name, DC=Domain.

Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored *parent* groups. Additionally, in advanced mode, FortiGate can apply security profiles to individual users, user groups, and OUs.

In comparison, in standard mode, you can apply security profiles only to user groups, not individual users.

In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.

If the LDAP on the collector agent fails, it doesn't matter what the LDAP on the FortiGate says, FSSO won't work. If the FortiGate LDAP fails, but the LDAP on the collector agent is still running, the FortiGate may not be able to collect logs, but the collector agent still collects logs.

Fortinet strongly encourages users to create filters from the collector agent.

DO NOT REPRINT**© FORTINET**

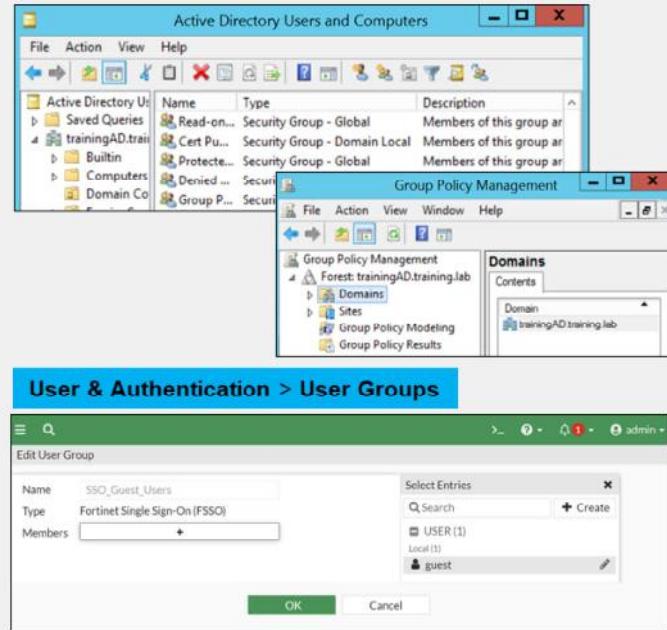
AD Group Support

Group type supported:

- Security groups
- Universal groups
- Groups inside OUs
- Local or universal groups that contain universal groups from child domains (only with Global Catalog)

If the user is not part of an FSSO group:

- For passive FSSO authentication:
 - User is part of **SSO_Guest_Users**
- For passive and active FSSO authentication:
 - User is prompted to log in



In AD settings, not all group types are supported. AD settings supports filtering groups only from:

- Security groups
- Universal groups
- Groups inside OUs
- Local or universal groups that contain universal groups from child domains (only with Global Catalog)

All FortiGate configurations include a user group called **SSO_Guest_Users**. When only passive authentication is used, all the users that do not belong to any FSSO group are automatically included in this guest group.

This allows an administrator to configure limited network access to guest users that do not belong to the Windows AD domain.

However, if both passive and active authentication are enabled for specific traffic, you cannot use **SSO_Guest_Users**, because traffic from IP addresses not on the FSSO user list must be prompted to enter their credentials.

DO NOT REPRINT**© FORTINET**

Advanced Settings

Citrix/Terminal Server

- Terminal server (TS) agent mode: monitors user logins in real time
- Requires a collector agent
 - No polling support from FortiGate

RADIUS Accounting

- Notify the firewall upon login and logout events

Syslog Servers

- Notify the firewall upon login and logout events

Exchange Server

- Monitor MS Exchange Server
- Allow users access to emails through the domain account
 - Accessing from the domain or not

© Fortinet Inc. All Rights Reserved. 33

Depending on your network, you might need to configure advanced settings in your FSSO collector agent.

Citrix servers support FSSO. Terminal server (TS) agent mode allows the server to monitor user logins in real time. The TS agent is like a DC agent, it also needs the collector agent to collect and send the login events to FortiGate. It then uses the same ports to report the logins back to the collector agent.

The collector agent on its own can get accurate login events only from Citrix servers if each user gets their own IP address. Otherwise, if multiple users share the same IP address, the TS agent is needed so that it can report to the collector agent the user, IP address, and source port range assigned to that user. The TS agent cannot forward logs directly to FortiGate, the logs first have to be gathered by a collector. This does not work with polling from FortiGate.

A RADIUS server configured as a RADIUS-based accounting system can interact in your network by sending accounting messages to the collector agent. The FSSO collector agent also supports integration with syslog servers for the same purpose.

The FSSO collector agent can also monitor a Microsoft Exchange server, which is useful when users access their email using their domain account.

For **Windows Security Event Logs** polling mode, you can configure **Event IDs to poll** here. For specific event IDs, visit the Fortinet Knowledge Base (<http://kb.fortinet.com>).

DO NOT REPRINT

© FORTINET

Knowledge Check

1. If you have collector agents using either the DC agent mode or the collector agent-based polling mode, which fabric connector should you select on FortiGate?
 - A. Poll Active Directory Server
 - B. Fortinet Single Sign-On Agent

2. Which naming conventions does the FSSO collector agent use to access the Windows AD in **Standard** access mode?
 - A. Windows convention - NetBios: Domain\groups
 - B. LDAP convention: CN=User,OU=Name,DC=Domain

DO NOT REPRINT**© FORTINET**

Lesson Progress



FSSO Function and Deployment



FSSO With Active Directory



FSSO Settings



Troubleshooting

Good job! You now understand how to configure the SSO settings on FortiGate and the FSSO collector agent.

Now, you'll learn about some basic troubleshooting options.

DO NOT REPRINT**© FORTINET**

Troubleshooting

Objectives

- Recognize and monitor FSSO-related log messages
- Perform basic FSSO troubleshooting

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

By demonstrating competence in FSSO monitoring and troubleshooting, you will be able to prevent, identify, and solve common issues related to FSSO.

DO NOT REPRINT

© FORTINET

FSSO Log Messages on FortiGate

- FSSO logs are generated from authentication events, such as user login and logout events and NTLM authentication events
 - To log all events, set the minimum log level to **Notification** or **Information**

1 Log & Report > System Events > User Events

User	Action	Message
ADUSER1	authentication	User ADUSER1 succeeded in logout
ADUSER1	FSSO-logoff	FSSO-logoff event from TrainingDomain: user ADUSER1 logged off 10.0.1.10
ADUSER1	FSSO-logon	FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10

2 Details

Event

Message: FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10

Other

Destination: TrainingDomain
Log ID: **43014**
Sub Type: user
roll: 65533

3

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication successful
43017	Notification	NTLM authentication failed

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

37

FSSO-related log messages are generated from authentication events. These include user login and logout events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues.

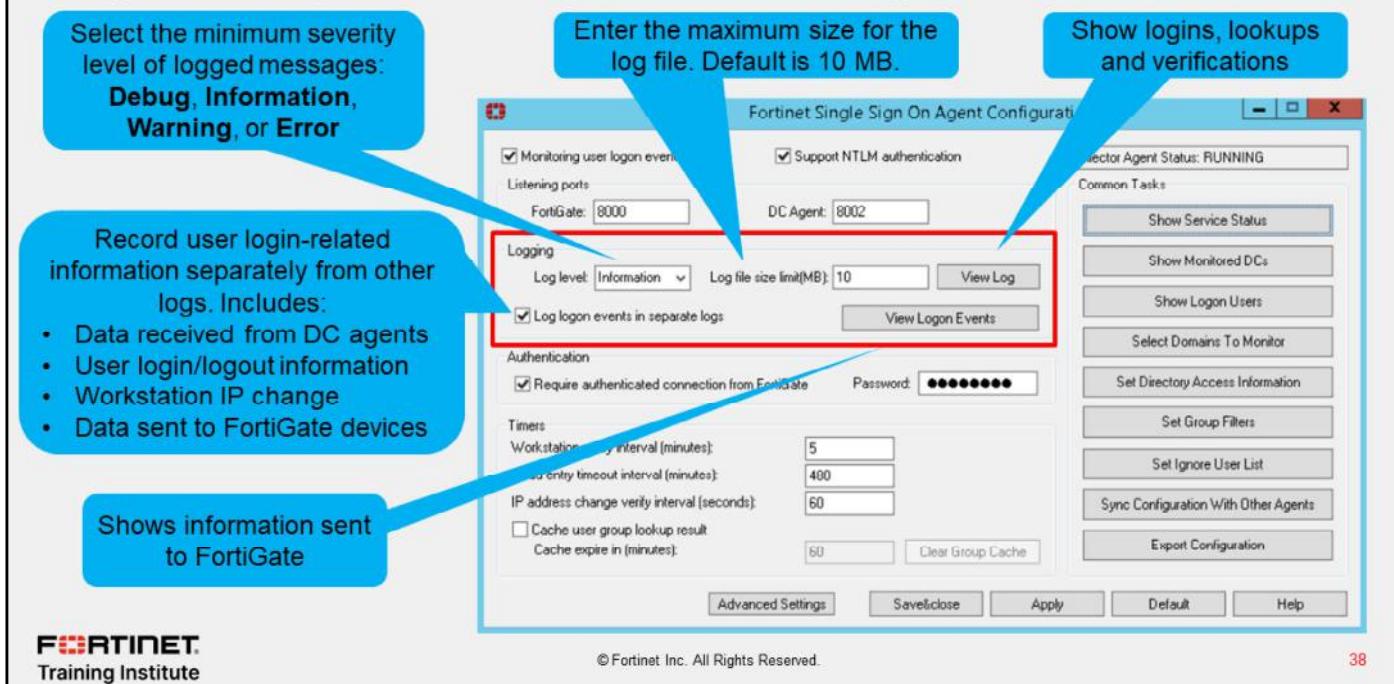
To ensure you log all the events needed, set the minimum log level to **Notification** or **Information**. Firewall logging requires **Notification** as a minimum log level. The closer the log level is to **Debug** level, the more information is logged.

FortiGate Infrastructure 7.2 Study Guide

152

DO NOT REPRINT
© FORTINET

Log Messages on FSSO Collector Agent



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

38

When troubleshooting FSSO agent-based deployments, you might want to look at the log messages generated directly on the FSSO collector agent.

The **Logging** section of the FSSO collector agent allows the following configurations:

- **Log level:** Select the minimum severity level of logged messages. Includes these levels:
 - **Debug:** the most detailed log level. Use it when actively troubleshooting issues.
 - **Information:** includes details about login events and workstation checks. This is the recommended level for most troubleshooting.
 - **Warning:** the default level. It provides information about failures.
 - **Error:** lists only the most severe events.
- **Log file size limit (MB):** Enter the maximum size for the log file in MB. The default is 10.
- **View Log:** View all FSSO agent logs.
- **Log login events in separate logs:** Record user login-related information separately from other logs. The information in this log includes: data received from DC agents, user login/logout information, workstation IP change information, and data sent to FortiGate devices. When selected, a summary of events sent and removed from FortiGate is listed under **View login Events**, while all other information remains under **View Log**.
- **View login Events:** If **Log login events in separate logs** is enabled, you will can view user login-related information.

DO NOT REPRINT

© FORTINET

Troubleshooting Tips for FSSO

1. Ensure all firewalls allow the FSSO required ports
 - For example: ports 139 (workstation verification), 445 (workstation verification and event log polling), 389 (LDAP), 445, 636 (LDAPS), and 3268, 3269 (TLS)
2. Guarantee at least 64 Kbps bandwidth between FortiGate and domain controllers
 - Configure traffic shaping to ensure the minimum bandwidth is always available
3. Configure the timeout timer to flush inactive sessions after a shorter time
 - Alternatively, encourage users to log out of one machine before logging in to another machine
4. Ensure DNS is configured and updating IP addresses if the host IP address changes
5. Never set the timer workstation verify interval to 0
 - This prevents the collector agent from aging out stale entries. They can be removed only by a new event overwriting them
 - This can be dangerous in environments where FSSO and non-FSSO users share the same DHCP pool
6. Include all FSSO groups in the firewall policies when using passive authentication
 - Even add the SSO_Guest_Users to an identity-based security policy to allow traffic
 - If active authentication is used as a backup, ensure that SSO_Guest_User is not added to policies



© Fortinet Inc. All Rights Reserved.

39

Begin with the following tips, which are useful in many FSSO troubleshooting situations:

- FSSO has a number of required ports that you must allow through all firewalls, or connections will fail. These include ports: 139 (workstation verification), 445 (workstation verification and event log polling), 389 (LDAP), and 445 and 636 (LDAPS).
- Configure traffic shaping between FortiGate and the domain controllers to ensure that the minimum bandwidth is always available. If there is insufficient bandwidth, some FSSO information might not reach FortiGate.
- In an all-Windows environment, flush inactive sessions. Otherwise, you can have a session for a non-authenticated machines go out as an authenticated user. This can occur if the DHCP lease expires for the authenticated user with the collector agent being able to verify that the user has indeed logged out.
- Ensure DNS is configured correctly and updating IP addresses, if workstation IP addresses change.
- Never set the workstation verify interval to 0. This prevents the collector agent from aging out stale entries. They can be removed only by a new event overwriting them. This can be especially dangerous in environments where FSSO and non-FSSO users share the same DHCP pool.
- When using passive authentication only, include the group of guest users in a policy and give them access. Associate their group with a security policy. If you use active authentication as a backup, ensure you do not add SSO_Guest_User to policies. SSO_Guest_User and active authentication are mutually exclusive.

DO NOT REPRINT
© FORTINET

Currently Logged-On Users

```
# diagnose debug authd fssso list
----FSSO logins----
IP: 10.0.1.10 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training
IP: 192.168.131.5 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training

Total number of logins listed: 2, filtered: 0
----end of FSSO logins----
```

IP address: 10.0.1.10

Workstation name: WIN-INTERNAL

User name: ADUSER1

User group: TRAININGAD/AD-USERS

Group created on FortiGate: Training

Dashboard > Users & Devices > Firewall Users

User Name	IP Address	User Group	Duration	Traffic Volume	Method
ADUSER1	10.0.1.10	Training	1 minute(1s)	217.40	Fortinet Single Sign-On
		TRAININGAD/AD-USERS			

Show all FSSO Logins

User Group: Training
 Members: TRAININGAD/AD-USERS
 Group Type: Fortinet Single Sign-On (FSSO)

execute fssso refresh

FORTINET
 Training Institute

40

If applying the tips from the previous slide didn't solve your FSSO issues, you may need to apply some `debug` commands.

To display the list of FSSO users that are currently logged in, use the CLI command `diagnose debug authd fssso list`.

For each user, the user name, user group, IP address, and the name of the workstation from which they logged in shows. The `MemberOf` section shows the group that was created on the firewall, to which you mapped the AD group. The same group should show in the **User group** screen on the GUI.

Also, use `execute fssso refresh` to manually refresh user group information from any directory service servers connected to FortiGate, using the collector agent.

DO NOT REPRINT**© FORTINET**

Connection to FortiGate

- Check connectivity between collector agent and FortiGate

```
# diagnose debug enable
# diagnose debug authd fssso server-status

  Server Name      Connection Status      Version      Address
  -----          -----          -----          -----
  TrainingDomain  connected          FSAE server 1.1  10.0.1.10
```



© Fortinet Inc. All Rights Reserved.

41

To show the status of communication between FortiGate and each collector agent, you can use the CLI command `diagnose debug authd fssso server-status`.

However, before you use that command, you must first run the command `diagnose debug enable`.

DO NOT REPRINT**© FORTINET**

Additional Commands

# diagnose debug authd fss0 <...>	
filter	Filters used for list or clear logins
list	Show currently logged on users
refresh-groups	Refresh group mapping
summary	Summary of currently logged on users
clear-logins	Delete cached login status
refresh-logins	Resynchronize login database
server-status	Show status of FSSO server connection
# diagnose firewall auth clear	Clears all filtered users
# diagnose firewall auth filter	Filter specific group, id, and so on
# diagnose firewall auth list	List authenticated users

Also, available under `diagnose debug authd fss0` are commands for clearing the FortiGate cache of all currently logged in users, filtering the display of the list of logged in users, and refreshing the login and user group information.

DO NOT REPRINT

© FORTINET

Polling Mode

```
diagnose debug fssso-polling detail
AD Server Status:
ID=1, name(10.0.1.10),ip=10.0.1.10,source(security),users(0)
port=auto username=administrator
read log offset=251636, latest login timestamp: Wed Feb 4 09:47:31 2015
polling frequency: every 10 second(s) success(246), fail(0)
LDAP query: success(0), fail(0)
LDAP max group query period(seconds): 0
most recent connection status: connected
```

Status of polls by FortiGate to DC

```
diagnose debug fssso-polling refresh-user
refresh completes. All login users are obsolete. Please re-login to make them available.
```

Active FSSO users

```
diagnose sniffer packet any 'host ip address and tcp port 445'
```

```
diagnose debug application fssod -1
```

Sniff polls



© Fortinet Inc. All Rights Reserved.

43

The command `diagnose debug fssso-polling detail` displays status information and some statistics related to the polls done by FortiGate on each DC in agentless polling. If the `read log offset` is incrementing, FortiGate is connecting to and reading the logs on the domain controller. If the `read log offset` is incrementing but you are not getting any login events, check that the group filter is correct and that the domain controller is creating the correct event IDs.

The command `diagnose debug fssso-polling refresh-user` flushes information about all the active FSSO users.

In agentless polling mode, FortiGate frequently polls the event viewer to get the login events. You can sniff this traffic on port 445.

Also, there is a specific FortiGate daemon that handles polling mode. It is the `fssod` daemon. To enable agentless polling mode real-time debug, use the `diagnose debug application fssod -1` command.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which logging level shows the login events on the collector agent?
 A. Information
 B. Warning

2. The command `diagnose debug fssso-polling detail` displays information for which mode of FSSO?
 A. Agentless polling
 B. Collector agent-based polling

DO NOT REPRINT**© FORTINET**

Lesson Progress



Fortinet FSSO Function and Deployment



FSSO with Active Directory



FSSO Settings



Troubleshooting

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Define SSO and FSSO
- ✓ Understand FSSO deployment and configuration
- ✓ Detect user login events in Windows AD using FSSO
- ✓ Identify FSSO modes for Windows AD
- ✓ Configure SSO settings on FortiGate
- ✓ Install FSSO agents
- ✓ Configure a Fortinet collector agent
- ✓ Recognize and monitor FSSO-related messages
- ✓ Perform basic FSSO troubleshooting

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

By mastering the objectives covered in this lesson, you learned how to use FSSO so that your users don't need to log in each time they access a different network resource.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

ZTNA

FortiOS 7.2

Last Modified: 23 August 2022

In this lesson, you will learn about zero-trust network access (ZTNA).

DO NOT REPRINT

© FORTINET

Lesson Overview

ZTNA Introduction

Comparing ZTNA to SSL and IPSec VPN

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

ZTNA

Objectives

- Understand the benefits of using ZTNA
- Understand the fundamentals of ZTNA
- Understand how to establish device identity and trust
- Understand SSL certificate-based authentication
- Configure ZTNA access on FortiOS
- Describe types of ZTNA configuration

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

By demonstrating competence in ZTNA, you will be able to understand key ZTNA concepts and how to configure ZTNA.

DO NOT REPRINT**© FORTINET**

What is ZTNA?

- Access control method that provides role-based application access
- ZTNA method uses:
 - Client device identification
 - Authentication
 - Zero-trust tags
- Provides flexibility to manage both on-net and off-net users
- ZTNA has two modes:
 - ZTNA access proxy
 - IP/MAC-based access control (on-fabric, devices for IT compliances, and rules enforcement)

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

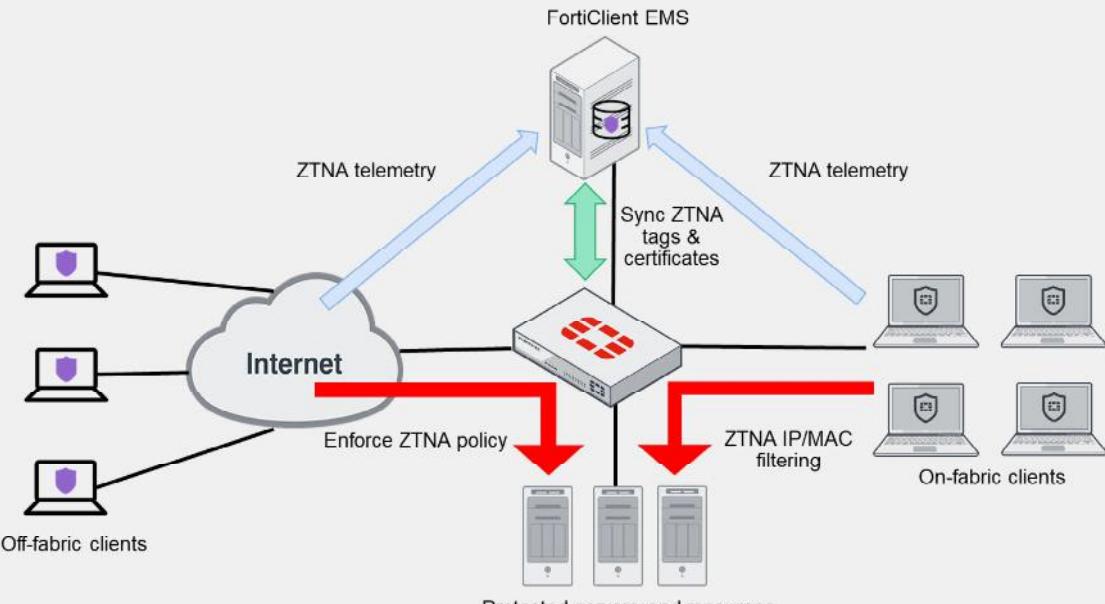
Traditionally, a user and a device have different sets of rules for on-fabric access and off-fabric VPN access to company resources. With a distributed workforce, and access that spans company networks, data centers, and the cloud, managing the rules can be complex. User experience is also affected when an organization needs multiple VPNs to access various resources.

ZTNA has two modes:

- ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.
- IP/MAC filtering uses ZTNA tags to provide an additional factor for identification, and a security posture check to implement role-based zero-trust access. IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for remote users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check to implement role-based zero-trust access. Firewall policies are configured that use ZTNA tags to control access between on-net devices and an internal webserver. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control.

DO NOT REPRINT**© FORTINET**

ZTNA Workflow

**FORTINET**
Training Institute

© Fortinet Inc. All Rights Reserved.

5

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

DO NOT REPRINT

© FORTINET

Device Roles

- Device identity and trust are integral to ZTNA
- Identity is established through client certificates
- Trust is established between:
 - FortiClient
 - Provides endpoint information (device information, logged on users, and security posture)
 - Obtains client certificate from FortiClient EMS
 - FortiClient EMS
 - Issues and signs the client certificate
 - Synchronizes certificate to FortiGate
 - Uses tagging rules to tag endpoints
 - FortiGate
 - Maintains continuous connection to FortiClient EMS to synchronize endpoint information
 - When device information changes, FortiClient EMS updates FortiGate
 - FortiGate WAD daemon uses this information when processing ZTNA traffic

Device identity and trust are integral to ZTNA. Device identity is established through client certificates, and trust is established among FortiClient, FortiClient EMS, and FortiGate devices. In ZTNA, devices perform specific roles.

FortiClient provides the following information to FortiClient EMS when it registers:

- Device information (network details, operating system, model, and so on)
- Logged in user information
- Security posture (on-fabric and off-fabric, antivirus software, vulnerability status, and so on)

FortiClient also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) on its first attempt to connect to the access proxy. The client uses this certificate to identify itself to FortiGate.

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. FortiClient EMS then synchronizes the certificate with FortiGate. FortiClient EMS also shares its EMS ZTNA CA certificate with FortiGate, so that FortiGate can use it to authenticate the clients. FortiClient EMS uses zero-trust tagging rules to tag endpoints based on the information that it has on each endpoint. FortiClient EMS also shares the tags with FortiGate.

FortiGate maintains a continuous connection to FortiClient EMS to synchronize endpoint device information such as FortiClient UID, client certificate SN, FortiClient EMS SN, network details (IP and MAC address), and so on. When device information changes, such as when a client moves from on-fabric to off-fabric, or their security posture changes, FortiClient EMS updates the device information, and then updates the FortiGate.

DO NOT REPRINT**© FORTINET**

FortiClient

- Provides a comprehensive network security solution for endpoints while improving your visibility and control
 - Allows you to manage security of multiple endpoints from the FortiClient EMS
 - Allows you to manage endpoints locally or remotely, stationary or mobile, using FortiClient EMS
 - Supports multiple platform protection:
 - Windows devices
 - Mac OS devices
 - Linux OS devices
 - iOS devices
 - Android mobile devices
 - Chromebook



© Fortinet Inc. All Rights Reserved.

7

FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linux-based desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

FortiClient enables every device—local or remote, stationary or mobile—to integrate with your FortiClient EMS and FortiGate. FortiClient supports Windows, Mac OS, Linux, iOS, Android mobile devices and Chromebook, and also integrates your home offices, mobile workers, and visiting partners.

DO NOT REPRINT**© FORTINET**

FortiClient (Contd)

- FortiClient is used with EMS to use all APT and security features
- FortiClient must connect to FortiClient EMS to activate the license
- You can change FortiClient configurations only from the management device
- FortiClient is either used with FortiClient EMS only or in the Security Fabric
- Enforces endpoint compliance and provides endpoint awareness
- Automates prevention of known and unknown threats
- Provides secure remote access



© Fortinet Inc. All Rights Reserved.

8

FortiClient must be used with FortiClient EMS. FortiClient must connect to FortiClient EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in FortiClient EMS. You cannot use any FortiClient features until FortiClient is connected to FortiClient EMS and licensed.

When FortiClient is connected only to FortiClient EMS, FortiClient EMS provisions and manages FortiClient. FortiClient EMS also sends zero-trust tagging rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. Only FortiClient EMS can control the connection between FortiClient and FortiClient EMS. However, FortiClient cannot participate in the Fortinet Security Fabric.

FortiClient in the security fabric connects to FortiClient EMS to receive a profile of configuration information as part of an endpoint policy. FortiClient EMS is connected to FortiGate to participate in the Security Fabric. FortiClient EMS sends FortiClient endpoint information to FortiGate. FortiGate can also receive dynamic endpoint group lists from FortiClient EMS and use them to build dynamic firewall policies.

FortiClient also provides secure remote access to corporate assets through VPN.

DO NOT REPRINT**© FORTINET**

FortiClient EMS

- FortiClient EMS is a security management solution that enables:
 - Scalable and centralized management of multiple endpoints (computers)
 - Efficient and effective administration of endpoints running FortiClient
- Provides visibility across the network to securely share information and assign security profiles to endpoints
- Works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users
- Designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users



© Fortinet Inc. All Rights Reserved.

9

FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows computers
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile, and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

DO NOT REPRINT
© FORTINET

FortiGate and FortiClient EMS Connectivity

- FortiGate uses FortiClient EMS fabric connector to connect
- FortiGate must verify the FortiClient EMS server certificate
 - Need to install CA certificate on FortiGate, otherwise certificate is not trusted
- FortiClient EMS must authorize the FortiGate as fabric device

The screenshot displays the FortiGate GUI and FortiClient EMS interface. On the left, the 'Security Fabric > Fabric Connectors' screen shows the configuration of a 'FortiClient EMS' connector. A blue callout labeled 'FortiGate GUI' points to this screen. On the right, the 'Administration > Fabric Devices' screen shows a 'Fabric Device Authorization Request' for a 'FortiGate' device. A blue callout labeled 'Fabric connector status' points to this screen. The FortiClient EMS GUI is also shown in a separate window at the top right.

Security Fabric > Fabric Connectors

Administration > Fabric Devices

FortiClient EMS GUI

Fabric connector status

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved.

10

You can configure the on-premises FortiClient EMS connector on FortiGate by clicking **Security Fabric > Fabric Connectors**. After applying the FortiClient EMS settings, FortiGate must accept the FortiClient EMS server certificate. However, when you configure a new connection to FortiClient EMS server, the certificate might not be trusted. To resolve, you must manually export and install the root CA certificate on FortiGate. The FortiClient EMS certificate that is used by default for the SDN connection is signed by the CA certificate that is saved on the Windows server when you first install FortiClient EMS. This certificate is stored in the **Trusted Root Certification Authorities** folder on the server. For more information about exporting and installing certificates on FortiGate, refer to the *FortiOS-7.0.1 Administration Guide*.

Next, you must authorize FortiGate on FortiClient EMS. If you log in to FortiClient EMS, a pop-up window opens, requesting you to authorize FortiGate. If you do not log in, you can click **Administration > Devices**, select the FortiGate device, and then authorize it. Note that the FortiClient EMS connector status appears down until you authorize FortiGate on FortiClient EMS.

FortiGate automatically synchronizes ZTNA tags after it connects to FortiClient EMS.

DO NOT REPRINT

© FORTINET

Zero-Trust Tagging Rules

- You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android
- When using tagging rules with EMS and FortiClient
 - EMS sends zero-trust tagging rules to endpoints
 - FortiClient checks endpoints using the provided rules and sends the results to EMS
 - EMS dynamically groups endpoints together using the tag configured for each rule
 - You can view the dynamic endpoint groups in **Zero Trust Tags > Zero Trust Tag Monitor**

zero-trust Tags > zero-trust Tagging Rules

Zero Trust Tagging Rule Set

Name	Malicious-File-Detected
Tag Endpoint As	Malicious-File-Detected
Enabled	<input checked="" type="checkbox"/>
Comments	Optional
Rules Edit Logic <input type="button" value="Add Rule"/>	
Type	Value
File	C:\virus.txt

zero-trust Tags > zero-trust Tagging Monitor

Endpoint with Tag					
1 Remote-Endpoints (1)					
Endpoint	User	OS	IP	Tagged on	
Remote-Client	Administrator	Microsoft Windows Ser ...	10.0.2.20	2021-08-26 02:43:06	

You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android endpoints. The following happens when using zero-trust tagging rules with FortiClient EMS and FortiClient:

- FortiClient EMS sends zero-trust tagging rules to endpoints through telemetry communication.
- FortiClient checks endpoints using the provided rules and sends the results to FortiClient EMS.
- FortiClient EMS receives the results from FortiClient.
- FortiClient EMS dynamically groups endpoints together using the tag configured for each rule. You can view the dynamic endpoint groups by clicking **Zero Trust Tags > Zero Trust Tag Monitor**.

Note that when the endpoint network changes or user login and logout events occur, FortiClient triggers an X-FFCK-TAG message to EMS, even if there are no tag changes. After FortiClient EMS receives the tags, it processes them immediately, and updates the FortiOS tags within five seconds of the REST API response. For other tag changes, FortiClient sends the information to FortiClient EMS regularly.

DO NOT REPRINT
© FORTINET

FortiClient EMS Certificate Management

- FortiClient EMS has a default root CA certificate
- ZTNA CA uses root certificate to sign CSRs from the FortiClient endpoints
- You can revoke and update root CA
 - Force updates to the FortiGate and FortiClient endpoints by generating new certificates
- FortiClient EMS manages individual client certificates

System Settings > EMS Setting

EMS Settings

Pre-defined hostname: AD-Server/AD-Server/training/AD training lab,10.0.1.100,192.168.0

Custom hostname: Optional

Management IP and Port: Optional, e.g. 443

Redirect HTTP request to HTTPS:

SSL certificate: FCTEMS0000101875.1 2038-01-19

EMS CA certificate (ZTNA): default_ZTNArootCA.pem 2048-07-16

Reset Started Deployment Interval: 12 hours

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

12

FortiClient EMS has a **default_ZTNArootCA** certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client. FortiClient EMS can also manage individual client certificates. You can also revoke the certificate that is used by the endpoint when certificate private keys show signs of being compromised. Click **Endpoint > All Endpoints**, select the client, and then click **Action > Revoke Client Certificate**.

Do not confuse the FortiClient EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by FortiClient EMS for HTTPS access and fabric connectivity to the FortiClient EMS server.

**DO NOT REPRINT
© FORTINET**

FortiClient EMS Certificate Management (Contd)

- On Windows endpoints, FortiClient automatically installs certificates in the certificate store
 - Certificate information, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate
 - **Certificates > Personal > Certificates**
 - You can verify by CLI command on FortiGate

- diagnose endpoint record list <optional IP address>

三

```
MQ-FortiGate # diagnose endpoint record list  
Record #1:
```

IP Address = 10.0.1.100
MAC Address = 00:50:56:a1:1b:15

MAC list = 00:50:56:a1:19:7a,00:50:56:a1:1b:15;
VDOM = root (0)
MAC denied sessions: 8C00000000010195

```
IP Address: 206.47.132.124
Guacamole: 206.47.132.124:4822
Online status: online
Registration status: registered
On-net status: on-net
Gateway Interface: port3
FotileClient version: 7.0.0
AVDB version: 98.336
FotileClient app signature version: 18.148
FotileClient compatibility: on-going-version: 3.21
FotileClient UUID: 37081E98-1154-4708-BADD-0177F76B816
Host Name: AD-Server
OS Type: WIN84
OS Version: Microsoft Windows Server 2012 R2 Standard Edition
4-bit (build 9600)
Host Description:
  domain: training00.training.lab
  Last Login User: Administrator
  Owner:
  Host Model: VMware Virtual Platform
  Host Manufacturer: VMware, Inc.
```

The screenshot shows the 'Certificate Information' tab of a certificate properties dialog. It includes sections for certificate details, purpose, and issuer information, along with a note about a private key and a 'View Certificate' button.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

13

In Windows, FortiClient automatically installs certificates in the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate. To locate certificates on other operating systems, consult the vendor documentation.

You can use the CLI command `diagnose endpoint record list a` to verify the presence of a matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on the FortiGate. If any of the information is missing or incomplete, client certificate authentication might fail because FortiClient cannot locate the corresponding endpoint entry.

This slide shows that client certificate information is synchronized with FortiGate.

DO NOT REPRINT

© FORTINET

SSL Certificate-Based Authentication

- An endpoint obtains a client certificate when it registers to FortiClient EMS
- FortiClient automatically submits CSR request
- FortiClient EMS signs and returns the client certificate
- Certificate is stored in OS certificate store
- By default:
 - Client certificate authentication is enabled on access proxy
 - Empty certificate response is set to block
 - Options can be configured on CLI only

```
config firewall access-proxy
  edit <name>
    set client-cert enable
    set empty-cert-action block
  end
```

- Currently, ZTNA supports the Microsoft Edge and Google Chrome browsers

Endpoint obtains a client certificate when it registers to FortiClient EMS. FortiClient automatically submits a CSR request and the FortiClient EMS signs and returns the client certificate. This certificate is stored in the operating system certificate store for subsequent connections. The endpoint information is synchronized between FortiGate and FortiClient EMS. When an endpoint disconnects or is unregistered from FortiClient EMS, its certificate is removed from the certificate store and revoked on FortiClient EMS. The endpoint obtains a certificate again when it reconnects to the FortiClient EMS.

By default, client certificate authentication is enabled on the access proxy, so when FortiGate receives the HTTPS request, the FortiGate WAD process challenges the client to identify itself with its certificate. The FortiGate makes a decision based on specific possibilities.

If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:

- If the client UID and certificate SN match the record on FortiGate, the client is allowed to continue with the ZTNA proxy rule processing.
- If the client UID and certificate SN do not match the record on FortiGate, the client is blocked from further ZTNA proxy rule processing.

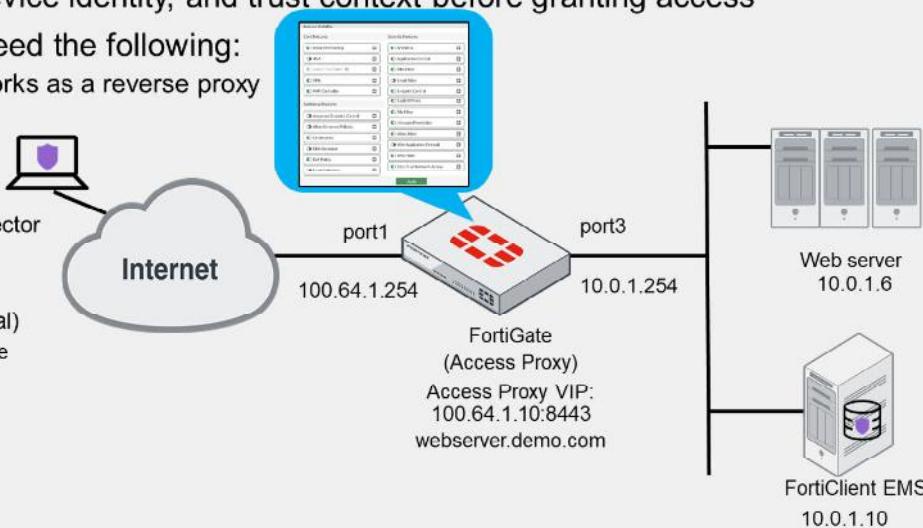
If the client cancels and responds with an empty client certificate, the client is allowed to continue with ZTNA proxy rule processing when you can set `empty-cert-action` to `accept`. If `empty-cert-action` is set to `block`, FortiGate blocks the client from further ZTNA proxy rule processing.

DO NOT REPRINT

© FORTINET

ZTNA HTTPS Access Proxy

- HTTPS access proxy works as a reverse proxy
- Verifies user identity, device identity, and trust context before granting access
- To deploy ZTNA, you need the following:
 - HTTPS access proxy works as a reverse proxy
 - FortiClient endpoint
 - FortiClient EMS
 - FortiGate
 - FortiClient EMS connector
 - ZTNA server
 - ZTNA rule
 - Authentication (optional)
 - Explicit proxy enable



The FortiGate HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a web page hosted by the protected server, the address resolves to the FortiGate access proxy VIP (100.64.1.10:8443), as shown on this slide. FortiGate proxies the connection and takes steps to authenticate the device. It prompts the user for the endpoint certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the FortiClient EMS.

To enable ZTNA on the GUI, you must click **System > Feature Visibility**, and then enabling **Zero Trust Network Access**.

ZTNA configuration on FortiGate requires the following configuration:

- FortiClient EMS adds a fabric connector in the Security Fabric. FortiGate maintains a continuous connection to the EMS server to synchronize endpoint device information, and also automatically synchronizes ZTNA tags. You can create groups and add tags to use in the ZTNA rules and firewall policies.
- The ZTNA server defines the access proxy VIP and the real servers that clients connect to. You can also enable authentication.
- A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. You can configure security profiles to protect this traffic.

You can also configure authentication to the access proxy. ZTNA supports basic HTTP and SAML methods.

DO NOT REPRINT
© FORTINET

ZTNA HTTPS Access Proxy (Contd)

- ZTNA server

Policy & Objects > ZTNA > ZTNA Servers

ZTNA Servers

Virtual host matching rules

Real server IP address and port

- ZTNA rule

Policy & Objects > ZTNA > ZTNA Rules

ZTNA Rules

Denying access based on malicious tag

After you configure FortiClient EMS as the fabric connector and you sync ZTNA tags with FortiGate, you must create a ZTNA server or access proxy. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service and server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic.

Note that UTM processing of the traffic happens at the ZTNA rule.

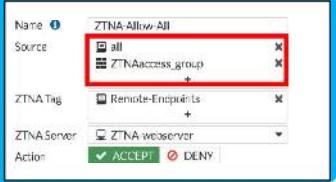
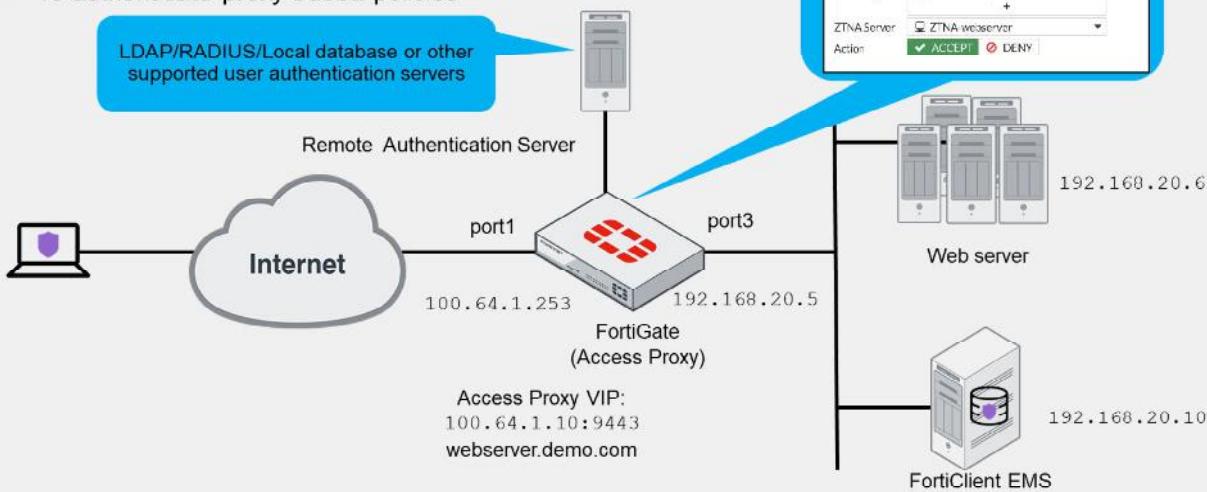
DO NOT REPRINT

© FORTINET

ZTNA HTTPS Access Proxy With Basic Authentication

- You can add authentication to the access proxy
- Requires authentication scheme and authentication rule
 - To authenticate proxy-based policies

LDAP/RADIUS/Local database or other supported user authentication servers



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

You can add authentication to the access proxy, which requires you to configure an authentication scheme and authentication rule on the FortiGate CLI. You use authentication schemes and authentication rules to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. ZTNA supports basic HTTP and SAML methods. Each method has additional settings to define the data source. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

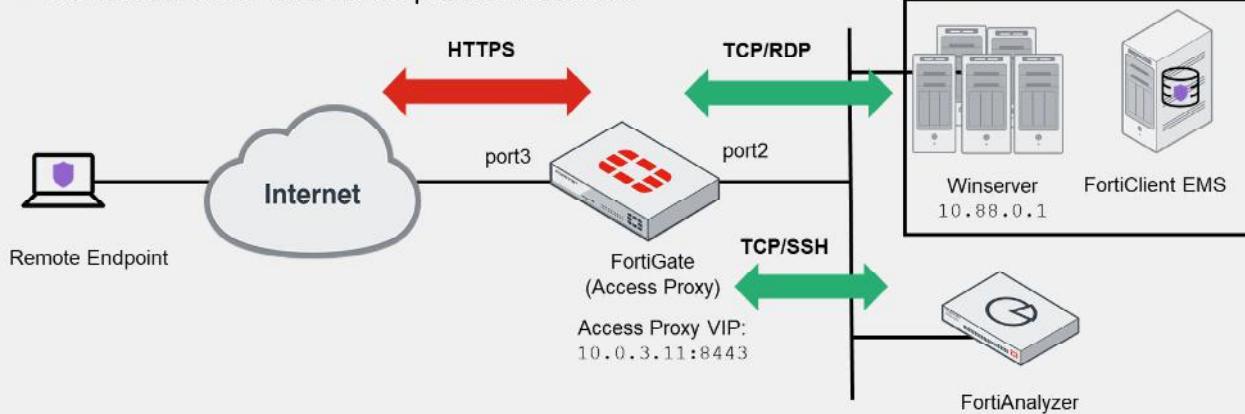
The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they are with basic authentication. After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to.

In the ZTNA rule and proxy policy, you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy. This slide shows the ZTNA rule example that user group **ZTNAaccess_group** was added to the authentication configuration after the authentication scheme and authentication rule were added to FortiGate.

DO NOT REPRINT
© FORTINET

ZTNA TCP Forwarding Access Proxy

- TCP forwarding access proxy demonstrates an HTTPS reverse proxy that forwards TCP traffic to the resource
- TCP forwarding access proxy:
 - Tunnels TCP traffic between the client and FortiGate over HTTPS
 - Forwards the TCP traffic to the protected resource



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

18

In the example shown on this slide, a TCP forwarding access proxy (TFAP) is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

RDP access is configured to Winserver, and SSH access to FortiAnalyzer. The topology shown on this slide uses IP address 10.0.3.11 and port-8443 for the external access proxy VIP.

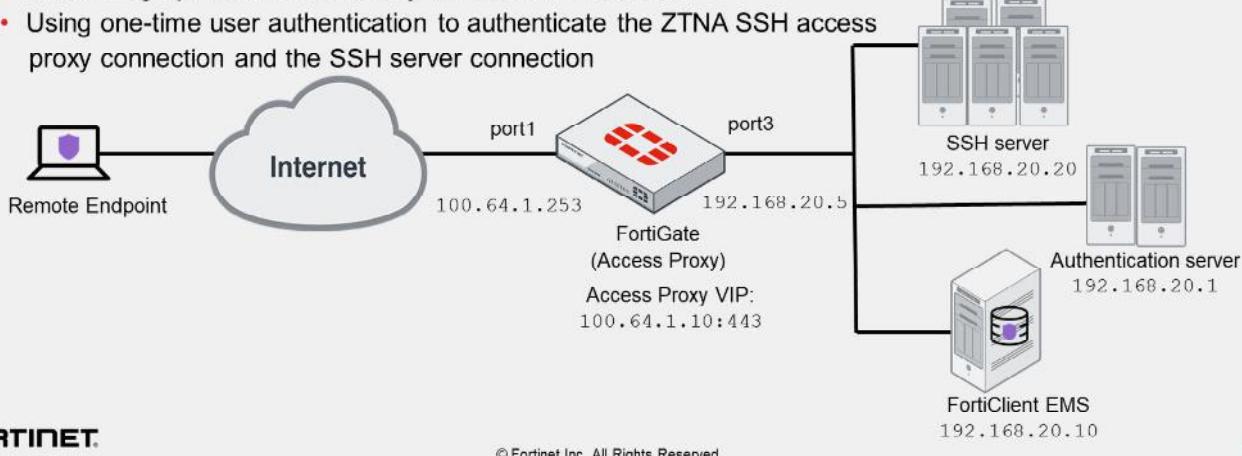
You can also add authentication and a security posture check for TCP Forwarding Access Proxy, which you learned about earlier in this lesson.

DO NOT REPRINT

© FORTINET

ZTNA SSH Access Proxy

- ZTNA supports SSH access proxy to provide seamless SSH connection
- Advantages over TCP forwarding access proxy:
 - Establishing device trust context with user identity and device identity checks
 - Applying SSH deep inspection to the traffic through the SSH related profile
 - Performing optional SSH host-key validation of the server
 - Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

You can configure ZTNA with an SSH access proxy to provide a seamless SSH connection to the server.

Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:

- Establishing device trust context with user identity and device identity checks
- Applying SSH deep inspection to the traffic through the SSH related profile
- Performing optional SSH host-key validation of the server
- Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection

To act as a reverse proxy for the SSH server, FortiGate must perform SSH host-key validation to verify the identity of the SSH server. FortiGate does this by storing the public key of the SSH server in its SSH host-key configurations. When endpoint makes a connection to the SSH server, if the public key matches one that is used by the server, then the connection is established. If there is no match, then the connection fails.

DO NOT REPRINT
© FORTINET

ZTNA IP/MAC-Based Access Control

- ZTNA IP/MAC-based access control enhances security when endpoints are physically on the corporate network
 - Use ZTNA tags to control access
- IP/MAC-based access control focuses on access for fabric users
- This mode does not require the use of the access proxy, and only uses ZTNA tags for access control

ZTNA IP/MAC-based firewall policy

Name: Block-Malicious

Incoming Interface: port3

Outgoing Interface: port1

Source: all

IP/MAC Based Access Control: FCTEMS_ALL_FORTICLOUD_SEI

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy

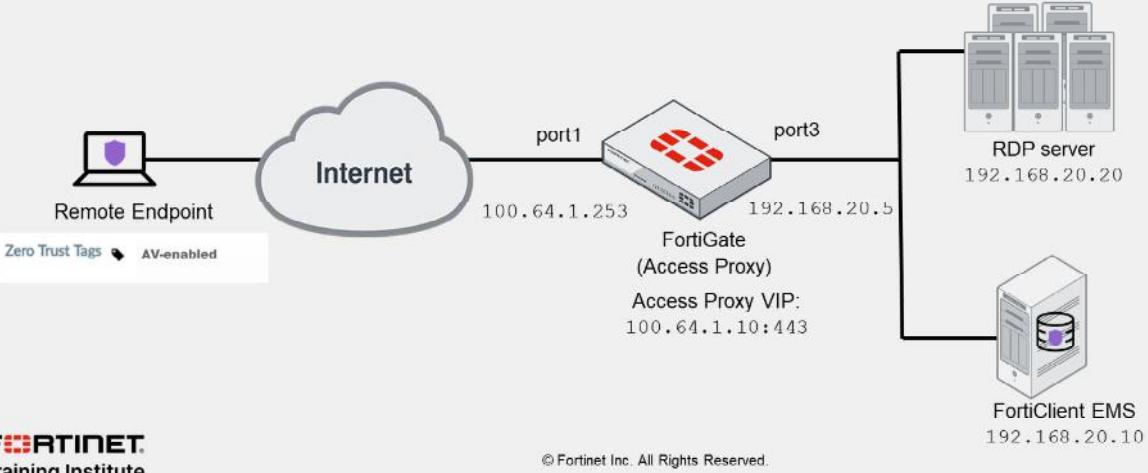
ZTNA IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for fabric users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check, to implement role-based zero-trust access. Firewall policies are configured that use ZTNA tags to control access between on-net devices and an internal webserver. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control.

The example firewall policy on this slide uses the existing tag to control access. Traffic is denied to the internet when the FortiClient endpoint is tagged with **FCTEMS_ALL_FORTICLOUD_Malicious**.

DO NOT REPRINT
© FORTINET

Posture Check Verification for Active ZTNA Session

- Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified
 - Terminates session if the endpoint is no longer compliant with the ZTNA policy
- FortiGate monitors changes to the endpoint tags, when FortiGate detects change:
 - The endpoint's active session must reevaluate again to match the ZTNA policy before a data can pass



Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy. The FortiGate monitors changes to the endpoint tags that are updated by FortiClient EMS. When a change is detected, the endpoint's active ZTNA sessions must match the ZTNA policy again before data can pass.

Note that changes to the ZTNA policy, such as changing the ZTNA tag matching logic, will also trigger re-verification of the client device against the policy.

In the example on this slide, a ZTNA rule is configured to allow access for endpoints that have the **AV-enabled** tag. After an RDP session is established, Windows antivirus is disabled on the remote endpoint. The FortiGate re-verifies the session and the active RDP session is removed from the FortiGate session table, causing the RDP session to be disconnected.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which component issues and signs the client certificate?

- A. FortiClient EMS
- B. FortiClient

2. Which internet browser supports Fortinet ZTNA?

- A. Firefox
- B. Chrome

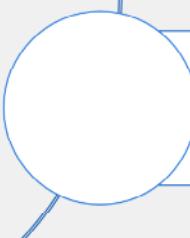
DO NOT REPRINT

© FORTINET

Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPsec VPN

Good job! You now understand key ZTNA concepts and how to configure ZTNA

Now, you will compare ZTNA to SSL and IPsec VPN.

DO NOT REPRINT

© FORTINET

Comparing ZTNA to SSL and IPsec VPN

Objectives

- Describe the differences between SSL VPN, IPsec VPN, and ZTNA access
- Understand the evolution of teleworker remote access with ZTNA

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

By demonstrating competence in understanding the evolution of remote access with ZTNA, you will be able to migrate from VPN to ZTNA HTTPS access proxy.

DO NOT REPRINT

© FORTINET

Comparing SSL VPN, IPsec VPN, and ZTNA Access

	IPsec VPN	SSL VPN	ZTNA
Tunnel type:	IPsec tunnel only	Session-based OR tunnel	Session-based only
Configured between:	FortiClient and FortiGate FortiGate and FortiGate FortiGate and compatible third-party IPsec VPN gateway FortiGate and compatible third-party IPsec VPN clients	Browser and FortiGate FortiClient and FortiGate FortiGate (SSL Client) and FortiGate (SSL Server)	Browser and FortiGate FortiClient and FortiGate (TCP forwarding access)
Log in through:	IPsec client	HTTPS web page on FortiGate FortiClient FortiGate (SSL Client)	HTTPS hostname or IP and port number FortiClient (TCP forwarding access)

How are SSL VPN and ZTNA access different from IPsec VPNs?

SSL and TLS are commonly used to encapsulate and secure e-commerce and online banking on the internet (HTTP). SSL VPNs and ZTNA use a similar technique, and support non-HTTP protocol encapsulation as well. 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 different methods to provide confidentiality and integrity. The primary protocol used in IPsec is ESP, which encapsulates and encrypts UDP, RDP, HTTP, or other protocols inside the IPsec tunnel.

IPSec is also an industry-standard protocol that can work with multiple vendors and supports peers that are devices and gateways—not just user clients with FortiGate only, like SSL VPN or ZTNA does.

The client software is also different. In an SSL VPN or ZTNA, your web browser might be the only client software you need. You can go to the FortiGate SSL VPN portal (an HTTPS web page) and then log in. Alternatively, you can install FortiClient or configure FortiGate as an SSL VPN client. In comparison, to use IPsec VPN, install special client software or have a local gateway, such as a desktop model FortiGate, to connect to the remote gateway. You might also need to configure firewalls between VPN peers to allow IPsec protocols.

DO NOT REPRINT

© FORTINET

Comparing SSL VPN, IPsec VPN, and ZTNA Access (Contd)

	IPsec VPN	SSL VPN	ZTNA
Category:	Industry standard	Vendor specific	Vendor specific
Ease of use (Configuration):	<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 	<ul style="list-style-type: none"> Does not require installation Simpler setup <ul style="list-style-type: none"> Client-to-FortiGate FortiGate-to-FortiGate No user-configured settings Technical support less requested 	<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
Better for:	Office-to-office traffic Data centers	Provides flexibility tunnel-mode or session-based access	Session-based access only
Attack surface protection	<ul style="list-style-type: none"> Traditional perimeter protection: <ul style="list-style-type: none"> Defends against external threats only Doesn't address threat inside the network 	<ul style="list-style-type: none"> Traditional perimeter protection: <ul style="list-style-type: none"> Defends against external threats only Doesn't address threat inside the network 	<ul style="list-style-type: none"> zero-trust philosophy <ul style="list-style-type: none"> No one inside or outside should be trusted Based on identity authentication

After you log 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 ZTNA and SSL VPN ideal for non-technical users, or users who connect from public computers, such as those found in public libraries and internet cafés. ZTNA takes this a step further and makes it easier for administrators to perform device compliance checks and configuration. ZTNA also provides an additional authentication mechanism for access control without any interaction required from the end user.

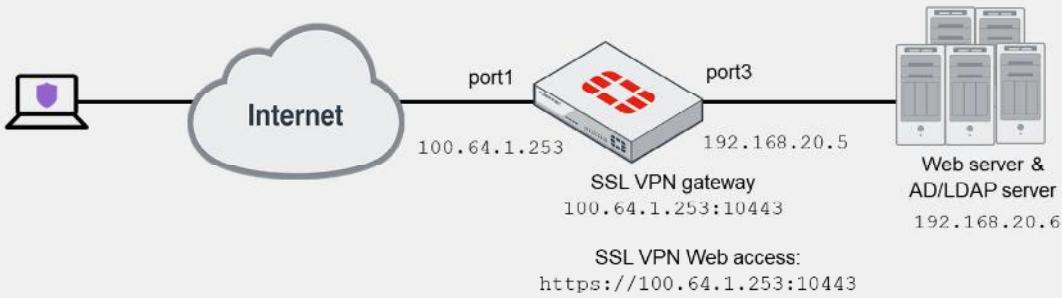
ZTNA follows the zero-trust philosophy to protect the attack surface that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. zero-trust also assumes that every attempt to access the network or an application is a threat.

Both IPsec and SSL VPN are traditional perimeter-based security approach that only distrusts factors outside the existing network and fail to address threats that already exist within the network.

DO NOT REPRINT**© FORTINET**

Moving to ZTNA From SSL VPN

- You can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy



You can use ZTNA to replace VPN-based teleworking solutions. The example on this slide shows that you can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy, and continue to use the same authentication server and groups to authenticate your remote users.

In addition, by integrating with FortiClient EMS, you can also ensure that FortiGate performs device identification using client certificates, and checks the security posture before allowing the remote user into the website. This provides granular control over who can access the web resource using role-based access control. It also gives the user transparent access to the website using only their browser. You can even configure ZTNA IP/MAC filtering mode for on-fabric devices to provide similar access control while users are on the network.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which remote access solution proxies HTTP and TCP over a secure HTTPS connection?

- A. ZTNA
- B. IPSec

2. What does FortiClient EMS integration ensure?

- A. Device identification
- B. User identification

DO NOT REPRINT

© FORTINET

Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPSec
VPN

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

29

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Understand the benefits and fundamentals of ZTNA
- ✓ Understand how to establish device identity and trust
- ✓ Understand SSL certificate-based authentication
- ✓ Configure ZTNA access on FortiOS
- ✓ Describe types of ZTNA configuration



© Fortinet Inc. All Rights Reserved.

30

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

By mastering the objectives covered in this lesson, you learned about how to configure and use ZTNA.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

SSL VPN

FortiOS 7.2

Last Modified: 13 June 2022

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



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

SSL VPN Deployment Modes

Objectives

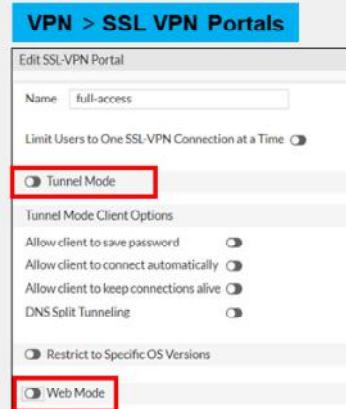
- Describe the differences between SSL VPN modes

After completing this section, you should be able to achieve the objective shown on this slide. By demonstrating competence in understanding the different ways FortiGate allows SSL VPN connections, you will be able to better 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 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



```
config vpn ssl web portal
  edit <portal-name>
    set tunnel-mode [enable|disable]
    set web-mode [enable|disable]
  end
```

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 the FortiClient remote access feature or FortiClient VPN-only client.

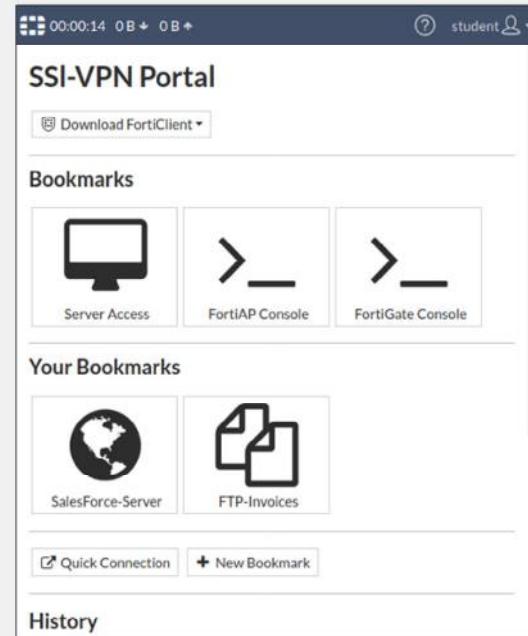
Web mode requires only a web browser, but supports a limited number of protocols.

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



Web mode 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:

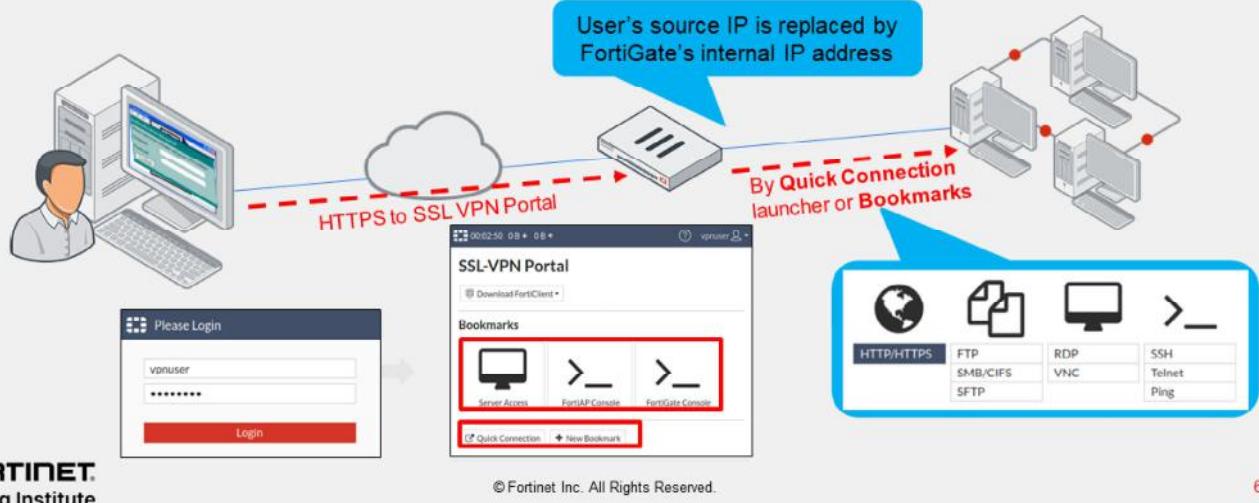
- All interaction with the internal network must be done using the browser exclusively (through the web portal). External network applications running on the user's PC cannot send data across the VPN.
- This a secure HTTP/HTTPS gateway mechanism that doesn't work for accessing everything, but just few 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
Training Institute

6

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/>



FortiClient

Next Generation Endpoint Protection

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)



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 (fortissl1). 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—FortiGate as Client

- Connect to server FortiGate device as SSL VPN client
 - Use SSL VPN *Tunnel* interface type
 - Devices connect to client FortiGate device can access the resources behind server FortiGate
- Tunnel establishes between two FortiGate devices
 - Hub-and-spoke topology
 - Client FortiGate dynamically adds route to remote subnets
 - Assigns a virtual IP address to the client FortiGate device from a pool of reserved addresses
- Advantage:
 - Any IP network application on the user machines connect to client FortiGate device can send traffic through the tunnel
 - Useful to avoid issues caused by intermediate devices, such as:
 - ESP packets being blocked.
 - UDP ports 500 or 4500 being blocked.
 - Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.
- Disadvantage:
 - Requires proper CA certificate on SSL VPN Server FortiGate
 - SSL VPN Client FortiGate user uses PSK and PKI client certificate to authenticate



© Fortinet Inc. All Rights Reserved.

9

The FortiGate can be configured as an SSL VPN client, using an *SSL-VPN Tunnel* interface type. When an SSL VPN client connection is established, the client dynamically adds a route to the subnets that are returned by the SSL VPN server. Policies can be defined to allow users that are behind the client to be tunneled through SSL VPN to destinations on the SSL VPN server.

This setup provides IP-level connectivity in tunnel mode and allows hub-and-spoke topologies to be configured with FortiGates as both the SSL VPN hub and spokes. This can be useful to avoid issues caused by intermediate devices, such as:

- ESP packets being blocked.
- UDP ports 500 or 4500 being blocked.
- Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.

If the client specified destination is *all*, a default route is effectively dynamically created on the SSL VPN client, and the new default route is added to the existing default route in the form of ECMP. You can modify route's distance or priority according to your requirements. To avoid a default route being learned on the SSL VPN client, on the SSL VPN server define a specific destination. Split tunneling is used so that only the destination addresses defined in the server's firewall policies are routed to the server, and all other traffic is connected directly to the internet.

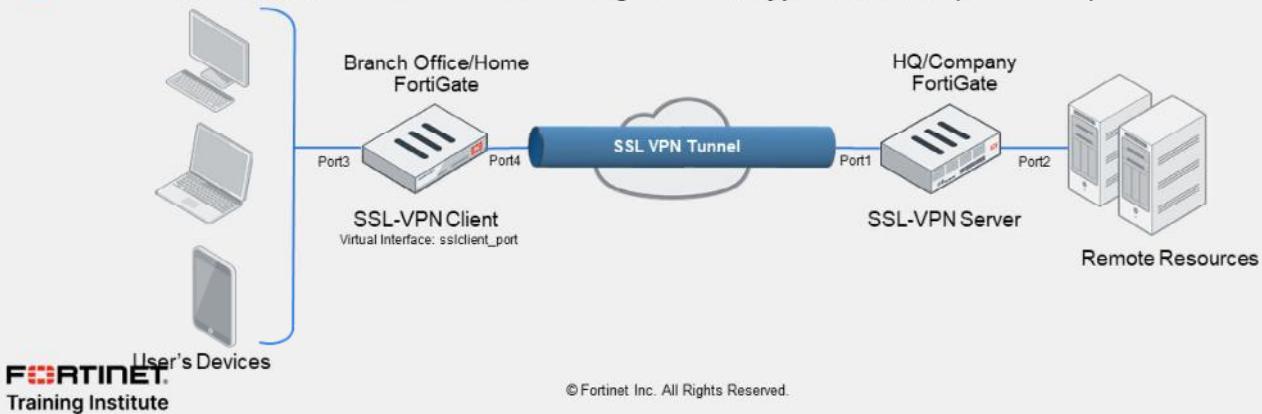
This configuration requires proper CA certificate installation as the SSL VPN client FortiGate/user uses PSK and a PKI client certificate to authenticate. The FortiGate devices must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.

DO NOT REPRINT

© FORTINET

Tunnel Mode—FortiGate as Client (Contd)

1. SSL VPN client FortiGate initiates connection to SSL VPN server FortiGate
2. SSL VPN client FortiGate uses PSK(local user account) and PKI client to authenticate
3. The virtual *SSL VPN tunnel* interface creates the tunnel
 - IP address assigned from SSL VPN server FortiGate
 - Route is added to client to access subnets on remote FortiGate
4. User's devices access resources through an encrypted tunnel (SSL/TLS)



© Fortinet Inc. All Rights Reserved.

10

How does tunnel mode work when FortiGate is configured as client?

1. Client FortiGate connects to server FortiGate using SSL/TLS
2. Client FortiGate provides credentials to successfully authenticate. It includes both PSK (local or remote user account) and PKI (certificate) accounts.
3. Server FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter. 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 behind client FortiGate.

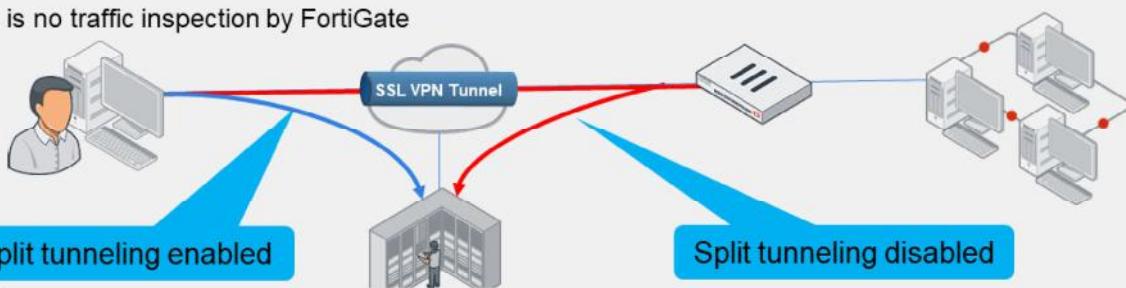
SSL VPN client FortiGate device encrypts all traffic from the remote computer and sends it over the SSL VPN tunnel. SSL VPN server FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

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
 - There is no traffic inspection by FortiGate



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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.

In a FortiGate (client) to FortiGate (server) setup, a default route is effectively dynamically created on the SSL VPN client FortiGate, and the new default route is added to the existing default route in the form of ECMP. The following options are available to configure routing:

- To make all traffic default to the SSL VPN server and still have a route to the server's listening interface, on the SSL VPN client, set a lower distance for the default route that is learned from the server.
- To include both default routes in the routing table, with the route learned from the SSL VPN server taking priority, on the SSL VPN client, set a lower distance for the route learned from the server. If the distance is already zero, then increase the priority on the default route.

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. There is no traffic inspection by FortiGate.

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 is the source IP address of the HTTP request the web server receives?
 - A. The remote user 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 bookmarks.
3. A web-mode SSL VPN user uses _____ to access internal network resources.
 - A. bookmarks
 - B. FortiClient

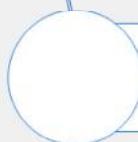
DO NOT REPRINT

© FORTINET

Lesson Progress



SSL VPN Deployment Modes



Configuring SSL VPNs



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
- Configure client integrity check

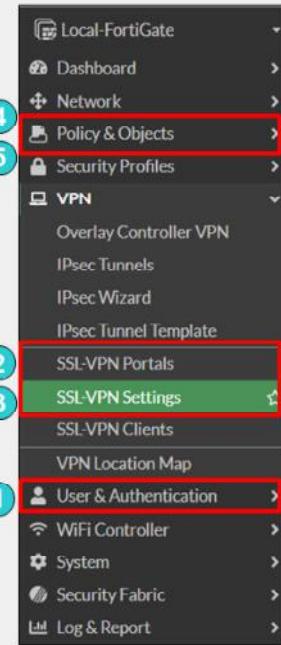
After completing this section, you should be able to achieve the objectives shown on this slide.

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—User as Client

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
5. Optionally:
 - 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



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.

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).

Some steps can be configured in a different order than what is shown on this slide.

DO NOT REPRINT

© FORTINET

Configure the SSL VPN Portal

VPN > SSL VPN Portals

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

- SSL VPN portals determine the access profiles
 - Configure portals for different user or groups
- SSL VPN portals can operate in:
 - Tunnel mode
 - Activate split tunneling in the **Enable Split Tunneling** option
 - Assign an IP address to the end user virtual network adapter in **Source IP Pool**: `fortissl`
 - Web mode
 - Use direct connection or bookmarks to several applications such as: FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, TELNET, VNC

Tunnel Mode

Web Mode

Administrator-defined bookmarks

© Fortinet Inc. All Rights Reserved.

The next 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 either **Enabled Based on Policy Destination** or **Enabled for Trusted Destination** setting, which usually specifies networks behind the FortiGate for the SSL VPN users to access. **Enabled Based on Policy Destination** allows client traffic in which destination is matched with the destination configured on the SSL VPN firewall policy where as **Enabled for Trusted Destination** allows client traffic that does not match the explicitly trusted destination.

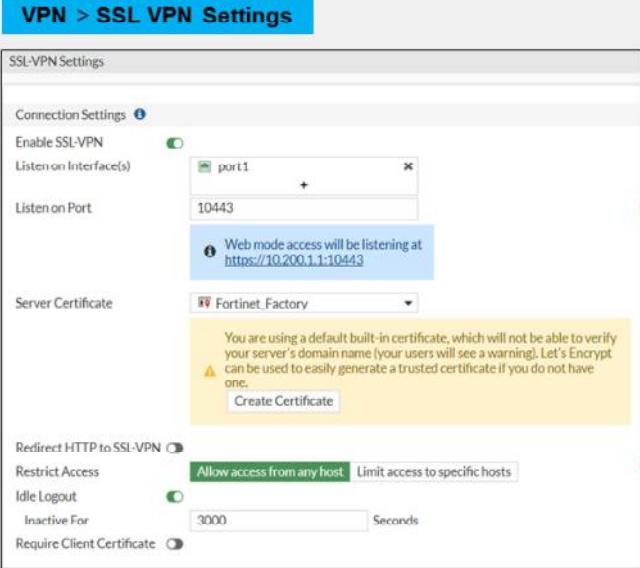
Also, for tunnel mode you need to select an IP pool for users to acquire an IP address when connecting. There is a default pool available within the address objects if you do not create your own.

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

Configure SSL VPN Settings



- FortiGate interface for SSL VPN portal:
 - Default port is 443
 - By default, the admin GUI interface and the 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, generate a trusted certificate or install the self-signed certificate on all clients

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

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 port443 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 port443 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). You can also generate a certificate for interface. Alternatively, you can load the FortiGate self-signed digital certificate into the browser as a trusted authority.

DO NOT REPRINT**© FORTINET**

Configure SSL VPN Settings (Contd)

- Define the IP range for the SSL VPN

- IPs are assigned to clients' virtual adapters while joined to VPN
- IP allocation has two methods:

- First-available (default) or Round robin
- CLI only

```
conf vpn ssl settings
  set tunnel-addr-assigned-method first-available/round-robin
end
```

- 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

Users/Groups	Portal
All Other Users/Groups	full access

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. There are two IP allocation methods and only available in CLI as shown in the slide:

- First-available (default setting)
- Round robin

Please note when round-robin is used, address pools defined in web portal is ignored, and the `tunnel-ip-pools` or `tunnel-ipv6-pools` under `ssl vpn` setting must be set. Only one set of IP pool address is allowed.

DNS server resolution is effective only 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

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**

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.

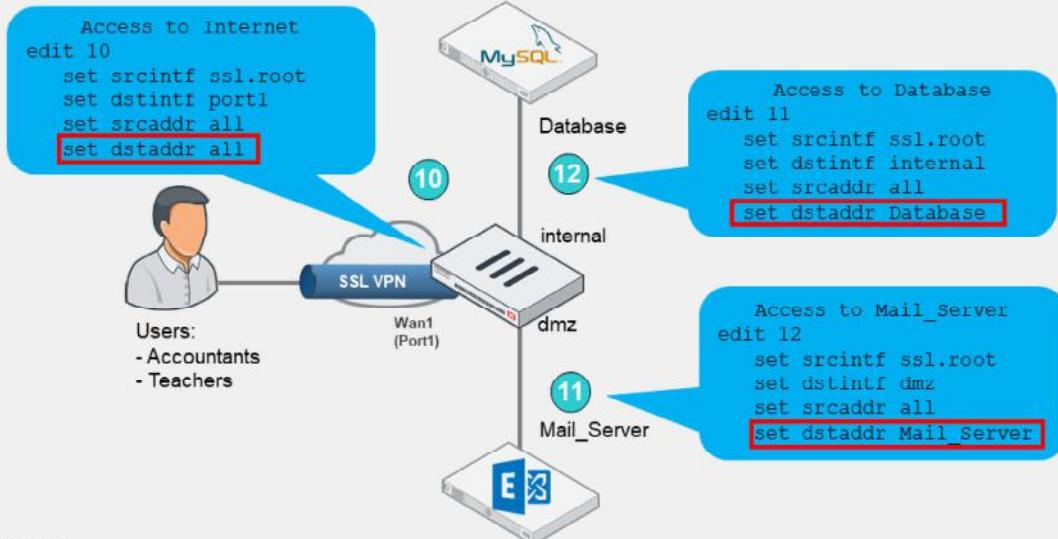
If there are resources behind other interfaces that users need access to, then you need to create additional policies that allow traffic from `ssl.root` to exit those interfaces.

DO NOT REPRINT

© FORTINET

Example: Access to Resources

- All traffic generated by the user exits through the `ssl.<vdom_name>` interface
 - Applies to both web and tunnel mode



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

20

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.

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

Configuring SSL VPN—FortiGate as Server

- SSL VPN Server FortiGate

- Set up user accounts and groups for remote SSL VPN users
 - Create two accounts: local/remote and PKI
 - Require clients to authenticate using their certificates as well as username and password
- Configure SSL VPN portals
- Configure SSL VPN settings
 - Authentication rules include both accounts using CLI
- Create a firewall policy to and from the SSL VPN interface
- Create a firewall policy to allow SSL VPN traffic to the internet (optional)

Use CLI to create first PKI user to get PKI menu on GUI

User & Authentication > User Definition

Edit User	
Username	clientfortigate
User Account Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
User Type	Local User
Password	*****
User Group	<input checked="" type="radio"/> SSL-VPN-Users <input type="radio"/> +
<input type="checkbox"/> Two-factor Authentication	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

User & Authentication > PKI

Edit PKI User	
Name	pki
Subject	
CA	CA.Cert.1
<input type="checkbox"/> Two-factor authentication	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

```
config user peer
  edit pki
    set ca "CA_Cert_1"
    set cn "FGVM01TM905"
  end
```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

21

To configure SSL VPN, you must take these steps:

SSL VPN server FortiGate:

- Set up user accounts and groups for remote SSL VPN users.
 - Create two accounts: local/remote and PKI. The PKI menu is only available in the GUI after a PKI user has been created using the CLI, and a CN can only be configured in the CLI. If no CN is specified, then any certificate that is signed by the CA will be valid and matched.
 - Require clients to authenticate using their certificates as well as username and password.
- Configure SSL VPN portals.
- Configure SSL VPN settings.
 - Authentication rules include both accounts using CLI.
- Create a firewall policy to and from the SSL VPN interface.
- Create a firewall policy to allow SSL VPN traffic to the internet (optional).

DO NOT REPRINT

© FORTINET

Configuring SSL VPN—FortiGate as Client

- SSL VPN Client FortiGate

- Create PKI user
 - Select CA certificate that allows the FortiGate to complete the certificate chain and verify the server's certificate
- Create SSL VPN tunnel interface using `ssl.<vdom>` interface
- Create and configure the SSL VPN Client settings on **VPN > SSL-VPN Clients**
- Create a firewall policy from internal interface to the SSL VPN interface

The image shows two screenshots of the FortiGate Management Interface. The left screenshot shows the 'Network > Interface > Create New' dialog. It has fields for 'Name' (sslclient_port), 'Interface Name' (sslclient_port), 'Type' (SSL-VPN Tunnel), 'Interface' (port4), 'VRF ID' (0), and 'Role' (LAN). A callout points to the 'Interface Name' field with the text 'Interface Name'. Another callout points to the 'Interface' field with the text 'Type: ssl.<vdom_name>'. A third callout points to the 'Interface' field with the text 'Select port to reach server FortiGate'. A fourth callout points to the 'Interface' field with the text 'Administrative Access' and lists 'IPv4' with checkboxes for 'HTTPS' (checked), 'SSH' (unchecked), 'RADIUS Accounting' (unchecked), 'PING' (checked), 'SNMP' (unchecked), and 'Security Fabric Connection' (unchecked). The right screenshot shows the 'VPN > SSL-VPN Clients > Create New' dialog. It has fields for 'Name' (SSLClienttoHQ), 'Interface' (sslclient_port), 'Server' (10.200.1.1), 'Port' (10443), 'Username' (ClientFortigate), 'Pre-shared Key' (*****), 'Client Certificate' (disabled), 'Peer' (pkd), 'Administrative Distance' (10), 'Priority' (0), 'Status' (Enabled), and 'Comments' (0/255). A callout points to the 'Name' field with the text 'Client Name'. Another callout points to the 'Interface' field with the text 'Virtual SSLInterface'. A third callout points to the 'Server' field with the text 'Server FortiGate IP Address and SSL Port'. A fourth callout points to the 'Username' field with the text 'Local and PKI user details including local cert to identify this client'. A fifth callout points to the 'Priority' field with the text 'Dynamic route priority and distance settings'.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

22

To configure SSL VPN, you must take these steps:

SSL VPN Client FortiGate:

- Create PKI user:
 - Set the same CN using CLI if PKI user on server FortiGate has CN configured.
 - Select CA certificate that allows the FortiGate to complete the certificate chain and verify the server's certificate.
- Create SSL VPN tunnel interface using `ssl.<vdom>` interface.
- Create and configure the SSL VPN client settings on **VPN > SSL-VPN Clients**, it includes:
 - Client name
 - Virtual SSL VPN interface
 - SSL VPN server FortiGate IP address and SSL port number
 - Local username and password and PKI(Peer) user. The **Client Certificate** is the local certificate that is used to identify this client, and is assumed to already be installed on the FortiGate. The SSL VPN server requires it for authentication.
 - When split tunnel is disabled, new default route is added and priority and distance plays an important role.
- Create a firewall policy to allow traffic from internal interface to the SSL VPN interface.

DO NOT REPRINT**© FORTINET**

Client Integrity Checking

- SSL-VPN gateway checks client integrity
 - Requires Microsoft Windows
 - Supported in SSL VPN tunnel mode only
- 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**
Training Institute

© Fortinet Inc. All Rights Reserved.

23

When a user connects to your network through an SSL-VPN, a portal is established between your network and the user's 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 checks to increase the security of the connection.

One method of increasing your security is by using 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 supports only 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 GUIDs. A 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 tunnel mode only.

DO NOT REPRINT

© FORTINET

Configure the Client Integrity Check

- Uses external vendor software to ensure client integrity:
FortiClient, AVG, CA, F-Secure, Kaspersky, McAfee, Norton, Symantec, Panda, Sophos, Trend-Micro, Zone Alarm,...
- Checks whether the software is installed on host client:
 - Configure through CLI or GUI
 - Software must 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 the software is not installed, 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
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

FortiGate performs the client integrity check while the VPN is still establishing, just after user authentication has finished. If the required software is not running on the user's PC, FortiGate rejects the VPN connection attempt, even with valid user credentials. You enable client integrity for each web portal, and you configure it 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 the custom setting is available only 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 up to date 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 and maintain this feature.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which step is necessary to configure SSL VPN connections?
 A. Create a firewall policy from the SSL VPN interface to the resource's interface.
 B. Enable event logs for SSL VPN traffic: users, VPN, and endpoints.

2. Which 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 DNS server as the client system DNS

DO NOT REPRINT

© FORTINET

Lesson Progress



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

Good job! You now understand how to configure FortiGate for SSL VPN connections.

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.

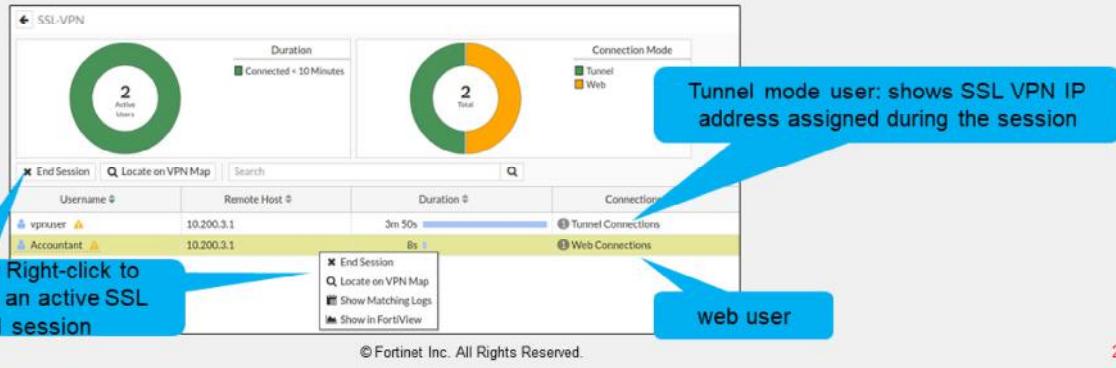
By demonstrating competence in SSL VPN monitoring and troubleshooting, you will be able to avoid, identify, and solve common issues and misconfigurations.

DO NOT REPRINT
© FORTINET

Monitoring SSL VPN Sessions

- Monitor which SSL VPN users are connected
 - GUI: Dashboard > Network > SSL VPN
- 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



FOR
NET
 Training Institute

28

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. The 'System Events' menu item is highlighted with a red box. A red arrow points from this menu item to two widgets: 'VPN Events' and 'User Events'. Blue callout boxes highlight the event logs for each. The 'VPN Events' log shows the following entries:

Date/Time	Level	Action	Status	Message
2020/01/21 04:50:...	ssl-new-con	ssl-new-con	SSL tunnel established	SSL new connection
2020/01/21 04:50:...	tunnel-down	tunnel-down	SSL tunnel shutdown	SSL tunnel statistics
2020/01/21 04:49:...	tunnel-stats	tunnel-stats	SSL tunnel statistics	SSL tunnel established
2020/01/21 04:39:...	tunnel-up	tunnel-up	SSL tunnel established	SSL new connection
2020/01/21 04:39:...	ssl-new-con	ssl-new-con	SSL tunnel established	SSL new connection

The 'User Events' log shows the following entries:

Date/Time	Level	User	Action	Message
2020/01/21 04:50:33	Student	auth-logout	User Student removed from auth logon	
2020/01/21 04:39:02	Student	auth-logon	User Student added to auth logon	

- 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

You can also review SSL VPN logs. On **Log & Report > System Events**:

- Select **VPN Events** widget to show new connection requests, and if the SSL VPN tunnel is established or closed.
- Select **User Events** widget 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

The screenshot shows the 'VPN > SSL VPN Settings' configuration page. It includes fields for 'Redirect HTTP to SSL-VPN' (disabled), 'Restrict Access' (set to 'Allow access from any host'), and 'Idle Logout' (enabled, set to 'Inactive For 300 Seconds'). A blue arrow points from the 'Idle Logout' section to a displayed CLI command:

```
config vpn ssl settings
  set idle-timeout <0-259200>
end
```

Below the interface, the Fortinet Training Institute logo is visible, along with the copyright notice '© Fortinet Inc. All Rights Reserved.' and the page number '30'.

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

When connected to SSL VPN 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.

32

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
# diagnose debug enable
```

Display debug messages for SSL VPN; -1 debug level
produces detailed results

- Check debug logs on the FortiClient



© Fortinet Inc. All Rights Reserved.

33

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`: Enables or disables SSL VPN old tunnel mode IP allocation method
- `web-mode-test`: Enables or disables 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. Also, check SSL VPN debug logs on FortiClient.

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      No acceleration hardware detected
cipher=on
```

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 statement about SSL VPN timers is correct?
 A. SSL VPN timers can prevent logouts when SSL VPN users experience long network latency.
 B. The login timeout is a non-customizable hard value.

DO NOT REPRINT

© FORTINET

Lesson Progress



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

36

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ 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 the client integrity check
- ✓ Monitor SSL VPN connected users
- ✓ Review SSL VPN logs
- ✓ Configure SSL VPN timers
- ✓ Troubleshoot common SSL VPN issues



© Fortinet Inc. All Rights Reserved.

37

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

By mastering the objectives covered in this lesson, you learned how to configure and use SSL VPNs to give remote users access to your private network.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

IPsec VPN

FortiOS 7.2

Last Modified: 23 August 2022

In this lesson, you will learn about the architectural components of IPsec VPN and how to configure them.

DO NOT REPRINT

© FORTINET

Lesson Overview



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

IPsec Introduction

Objectives

- Describe the benefits of IPsec VPN
- Be familiar with the IPsec protocol
- Understand how IPsec works
- Select an appropriate VPN topology

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

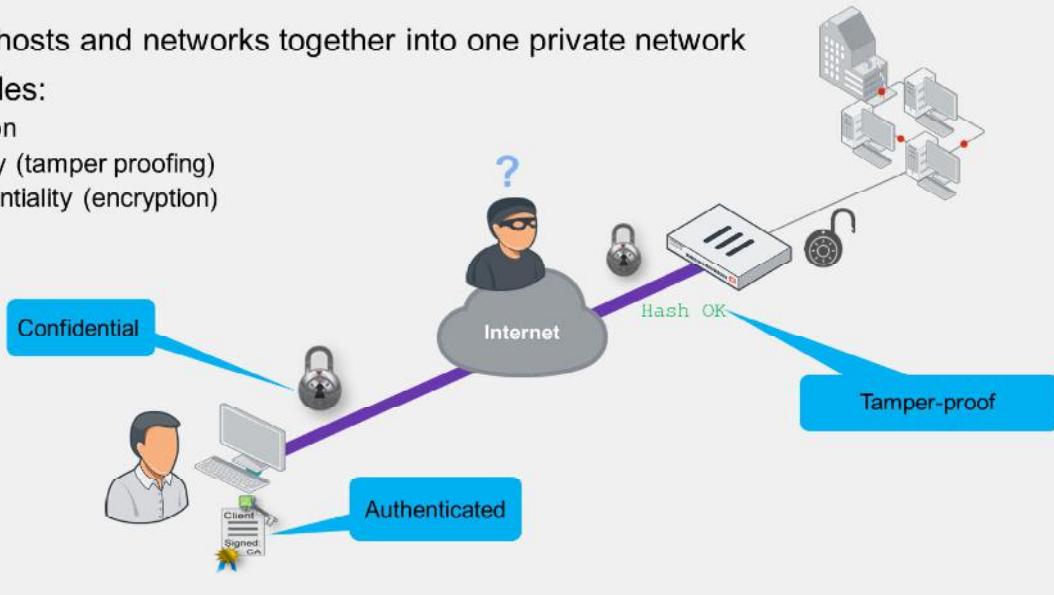
By demonstrating competence in IPsec basics, you will be able to understand IPsec concepts and benefits.

DO NOT REPRINT

© FORTINET

What Is IPsec?

- Joins remote hosts and networks together into one private network
- Usually provides:
 - Authentication
 - Data integrity (tamper proofing)
 - Data confidentiality (encryption)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

What is IPsec? When should you use it?

IPsec is a vendor-neutral set of standard protocols that is used to join two physically distinct LANs. The LANs are joined as if they were a single logical network, despite being separated by the internet.

In theory, IPsec *does* support null encryption—that is, you can make VPNs that don't encrypt traffic. IPsec also supports null data integrity. But does that provide any advantages over plain traffic? No. No one can trust traffic that may have had an attack injected by an attacker. Rarely do people want data sent by an unknown source. Most people also want private network data, such as credit card transactions and medical records, to remain private.

Regardless of the vendor, IPsec VPNs almost always have settings that allow them to provide three important benefits:

- Authentication: to verify the identity of both ends
- Data integrity (or HMAC): to prove that encapsulated data has not been tampered with as it crosses a potentially hostile network
- Confidentiality (or encryption): to make sure that only the intended recipient can read the message

DO NOT REPRINT

© FORTINET

What Is the IPsec Protocol?

- Multiple protocols that work together
 - Authentication Header (AH) provides integrity but not encryption
 - AH is defined in the RFC, but FortiGate does not use it
- Port numbers and encapsulation vary by network address translation (NAT)

Protocol	NAT Traversal (NAT-T)	No NAT
IKE RFC 2409 (IKEv1) RFC 4306 (IKEv2)	IP protocol 17: UDP port 500 (UDP 4500 for rekey, quick mode, mode-cfg)	IP protocol 17: UDP port 500
ESP RFC 4303	IP protocol 17: UDP port 4500 (encapsulated)	IP protocol 50

- If required, set a custom port for both IKE and IKE NAT-T (initiator and responder)*:

```
config system settings
  set ike-port <port>
end
```

* Custom port range: 1024–65535. FortiGate always listens on UDP port 4500 (responder only)

If you're passing your VPN through firewalls, it helps to know which protocols to allow.

IPsec is a suite of separate protocols, which includes:

- Internet Key Exchange (IKE): used to authenticate peers, exchange keys, and negotiate the encryption and checksums that will be used—essentially, it is the *control channel*
- AH: contains the authentication header—the checksums that verify the integrity of the data
- Encapsulating Security Payload (ESP): the encapsulated security payload—the encrypted payload, which is essentially the *data channel*

So, if you must pass IPsec traffic through a firewall, remember that allowing only one protocol or port number is usually not enough.

Note that the IPsec RFC mentions AH, however, AH does not offer encryption, which is an important benefit. Therefore, FortiGate does not use AH. As a result, you don't need to allow the AH IP protocol (51).

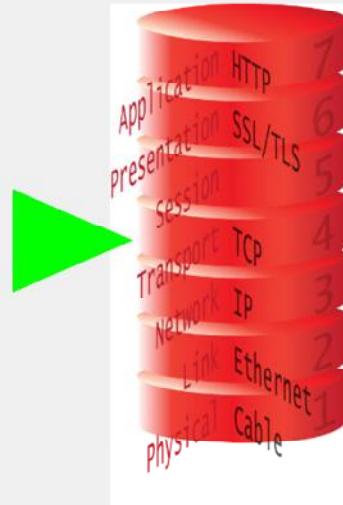
To set up a VPN, you must configure matching settings on both ends of the VPN—whether the VPN is between two FortiGate devices, FortiGate and FortiClient, or a third-party device and FortiGate. If the settings don't match, the tunnel setup fails.

The default ports for standard IKE traffic and IKE NAT-T traffic is UDP 500 and UDP 4500, respectively. You can use the CLI command shown on this slide to configure a custom port for both IKE and IKE NAT-T. The custom port is used to initiate and respond to tunnel requests. If NAT is detected, then the custom port can be used for both IKE and UDP-encapsulated ESP traffic. Note that FortiGate always listens for port UDP 4500 regardless of the custom port settings. This enables FortiGate to negotiate NAT-T tunnels on custom and standard ports.

DO NOT REPRINT**© FORTINET**

How Does IPsec Work?

- Encapsulation
 - Other protocols wrapped inside IPsec
 - What's inside? Varies by mode:
 - Transport mode—TCP/UDP
 - Tunnel mode—additional IP layer, then TCP/UDP
- Negotiation
 - Authentication
 - Handshake to exchange keys, settings

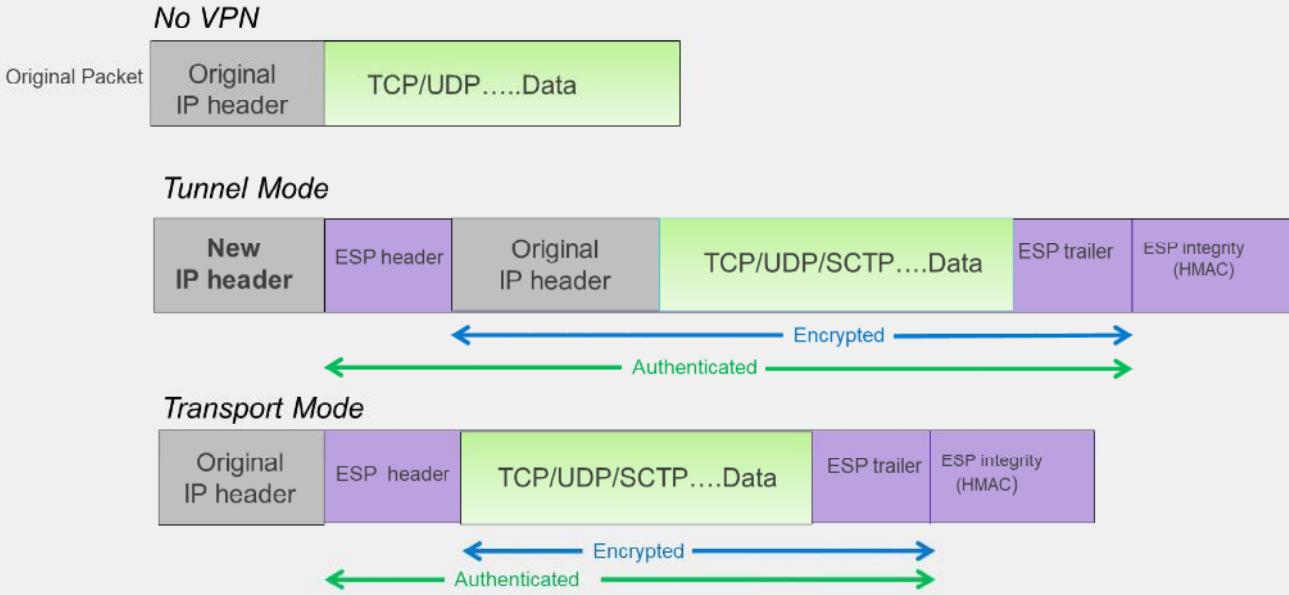


IPsec provides services at the IP (network) layer. During tunnel establishment, both ends negotiate the encryption and authentication algorithms to use.

After the tunnel has been negotiated and is up, data is encrypted and encapsulated into ESP packets.

DO NOT REPRINT
© FORTINET

ESP Encapsulation—Tunnel or Transport Mode



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

7

What's encapsulated? It depends on the encapsulation mode being used. IPsec can operate in two modes: transport mode and tunnel mode.

- Transport mode directly encapsulates and protects the fourth layer (transport) and above. The original IP header is not protected and no additional IP header is added.
- Tunnel mode is a true tunnel. The whole IP packet is encapsulated and a new IP header is added at the beginning. After the IPsec packet reaches the remote LAN and is unwrapped, the original packet can continue on its journey.

Note that after you remove the VPN-related headers, a transport mode packet can't be transmitted any further; it has no second IP header inside, so it's not routable. For that reason, this mode is usually used only for end-to-end (or client-to-client) VPNs.

DO NOT REPRINT**© FORTINET**

What Is IKE?

- Default ports: UDP port 500 (and UDP port 4500 when crossing NAT)
- Negotiates a tunnel's private keys, authentication, and encryption
- Phases:
 - Phase 1
 - Phase 2
- Versions
 - IKEv1 (legacy, wider adoption)
 - IKEv2 (new, simpler operation)



© Fortinet Inc. All Rights Reserved.

8

IKE uses UDP port 500. If NAT-T is enabled in a NAT scenario, IKE uses UDP port 4500.

IKE establishes an IPsec VPN tunnel. FortiGate uses IKE to negotiate with the peer and determine the IPsec security association (SA). The IPsec SA defines the authentication, keys, and settings that FortiGate uses to encrypt and decrypt that peer's packets. It is based on the Internet Security Association and Key Management Protocol (ISAKMP).

IKE defines two phases: phase 1 and phase 2.

There are two IKE versions: IKEv1 and IKEv2. Even though IKEv2 is a newer version and features a simpler protocol operation, this lesson focuses on IKEv1 only, because of its much wider adoption.

DO NOT REPRINT

© FORTINET

IKEv1 vs. IKEv2

Feature	IKEv1	IKEv2
Exchange modes	<ul style="list-style-type: none"> Main <ul style="list-style-type: none"> Total messages: 9 (6 for phase 1, 3 for phase 2) Aggressive <ul style="list-style-type: none"> Total messages: 6 (3 for phase 1, 3 for phase 2) 	<ul style="list-style-type: none"> One exchange procedure only Total messages: 4 (one child SA only)
Authentication methods	Symmetric: <ul style="list-style-type: none"> Pre-shared key (PSK) Certificate signature Extended authentication (XAuth) 	Asymmetric: <ul style="list-style-type: none"> PSK Certificate signature EAP (pass-through—no client support)
NAT-T	Supported as extension	Native support
Reliability	Unreliable—messages are not acknowledged	Reliable—messages are acknowledged
Dial-up phase 1 matching by ID	<ul style="list-style-type: none"> Peer ID + aggressive mode + PSK Peer ID + main mode + certificate signature 	<ul style="list-style-type: none"> Peer ID Network ID
Traffic selector narrowing	Not supported	Supported

This slide shows a table comparing some of the IKEv1 and IKEv2 features that FortiOS supports. IKEv2 provides a simpler operation, which is the result of using a single exchange mode and requiring less messages to bring up the tunnel.

Authentication-wise, both versions support PSK and certificate signature. Although only IKEv1 supports XAuth, IKEv2 supports EAP, which is equivalent to XAuth. However, the FortiOS IKEv2 EAP implementation is pass-through only. That is, FortiOS doesn't support EAP as a client, which means that you cannot revoke access to peers using IKEv2 unless you use a certificate signature. With IKEv1, you can deny access to VPN peers without having to use a certificate signature by using XAuth. IKEv2 also supports asymmetric authentication, which enables you to configure each peer to use a different authentication method.

Both IKE versions support NAT-T. However, IKEv2 supports NAT-T natively, while IKEv1 supports NAT-T as an extension. Also, IKEv2 is a more reliable protocol than IKEv1 because, like TCP, peers must acknowledge the messages exchanged between them. IKEv1 doesn't support such a mechanism.

When you configure multiple dial-up IPsec VPNs, IKEv2 makes it simpler to match the intended gateway by peer ID. With IKEv2, you can either use the standard peer ID attribute or the Fortinet proprietary network ID attribute to indicate the phase 1 gateway to match on the dial-up server, regardless of the authentication mode in use. However, with IKEv1, you can use the peer ID only, and then combine it with aggressive mode and pre-shared key authentication, or with main mode and certificate signature authentication.

Finally, IKEv2 allows the responder to choose a subset of the traffic the initiator proposes. This is called traffic selector narrowing and enables you to have more flexible phase 2 selector configurations. Traffic selector narrowing enables a peer to automatically narrow down its traffic selector addresses, so it agrees with the traffic selector the remote peer proposes.

DO NOT REPRINT**© FORTINET**

Negotiation—Security Association (SA)

- IKE allows the parties involved in a transaction to set up their Security Associations (SAs)
 - SAs are the basis for building security functions into IPsec
 - In normal two-way traffic, the exchange is secured by a pair of SAs
 - IPsec administrators decide the encryption and authentication algorithms that can be used in the exchange
- IKE uses two distinct phases:
 - Phase 1 → Outcome: IKE SA
 - Phase 2 → Outcome: IPsec SA



© Fortinet Inc. All Rights Reserved.

10

In order to create an IPsec tunnel, both devices must establish their SAs and secret keys, which are facilitated by the IKE protocol.

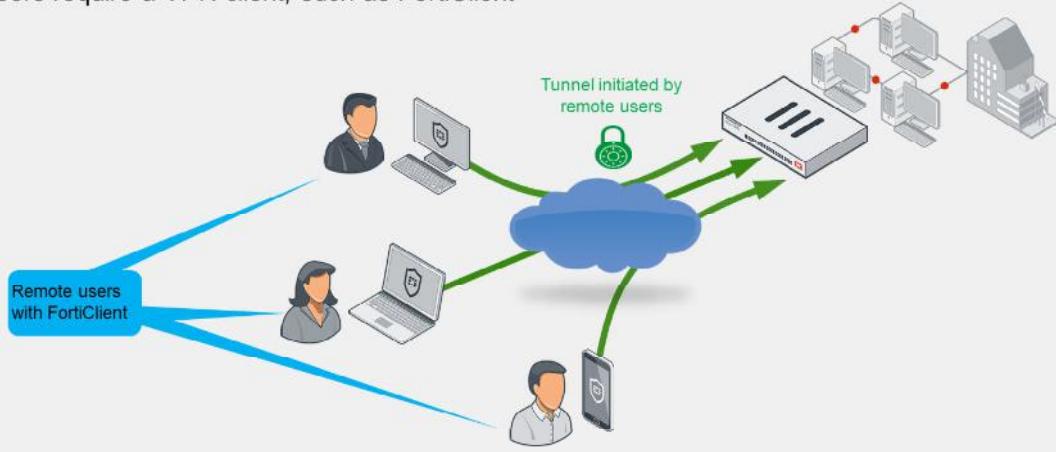
The IPsec architecture uses SAs as the basis for building security functions into IPsec. An SA is the bundle of algorithms and parameters being used to encrypt and authenticate data travelling through the tunnel. In normal two-way traffic, this exchange is secured by a pair of SAs, one for each traffic direction. Essentially, both sides of the tunnel must agree on the security rules. If both sides cannot agree on the rules for sending data and verifying each other's identity, then the tunnel is not established. SAs expire and need to be renegotiated by the peers after they have reached their lifetime.

IKE uses two distinct phases: phase 1 and phase 2. Each phase negotiates different SA types. The SA negotiated during phase 1 is called IKE SA, and the SA negotiated during phase 2 is called IPsec SA. FortiGate uses IKE SAs for setting up a secure channel to negotiate IPsec SAs. FortiGate uses IPsec SAs for encrypting and decrypting the data sent and received, respectively, through the tunnel.

DO NOT REPRINT
© FORTINET

VPN Topologies—Remote Access

- Remote users connect to corporate resources
 - FortiGate is configured as dial-up server—only clients can initiate the VPN
 - Users require a VPN client, such as FortiClient



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

Use remote access VPNs when remote internet users need to securely connect to the office to access corporate resources. The remote user connects to a VPN server located on the corporate premises, such as FortiGate, to establish a secure tunnel. After the user is authenticated, FortiGate provides access to network resources, based on the permissions granted to that user.

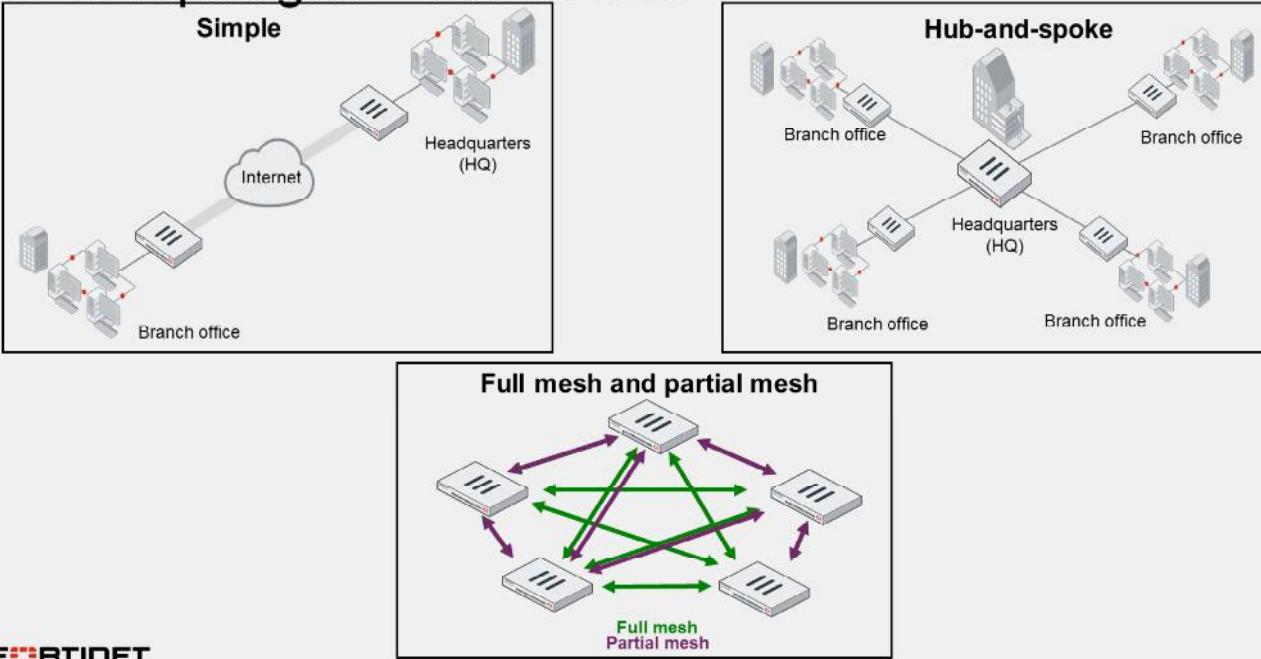
In a remote access VPN, FortiGate is usually configured as a dial-up server. You will learn more about dial-up VPNs in this lesson. The IP address of the remote internet user is usually dynamic. Because FortiGate does not know the IP address of the remote user, only the remote user can initiate a VPN connection request.

The remote user side needs a VPN client, such as FortiClient. You must configure FortiClient to match the VPN server settings. FortiClient takes care of establishing the tunnel, as well as routing the traffic destined to the remote site through the tunnel.

In addition, you can use one remote access VPN configuration on your FortiGate device for many remote users. FortiGate establishes a separate tunnel for each of them.

DO NOT REPRINT
© FORTINET

VPN Topologies—Site-to-Site



12

Site-to-site VPN is also known as LAN-to-LAN VPN. A simple site-to-site deployment involves two peers communicating directly to connect two networks located at different offices.

When you need to connect more than two locations, you can use a hub-and-spoke topology. In hub-and-spoke, all clients connect through a central hub. In the example shown on this slide, the clients—spokes—are branch office FortiGate devices. For any branch office to reach another branch office, its traffic must pass through the hub. One advantage of this topology is that the configuration needed is easy to manage. Another advantage is that only the FortiGate at HQ must be very powerful because it handles all tunnels simultaneously, while the branch office FortiGate devices require much fewer resources because they maintain only one tunnel. One disadvantage is that communication between branch offices through HQ is slower than in a direct connection, especially if your HQ is physically distant. Also, if the FortiGate device at HQ fails, VPN failure is company-wide.

In a mesh topology, you can connect FortiGate devices directly and therefore bypass HQ. Two variations of mesh topology exist: full mesh and partial mesh. Full mesh connects every location to every other location. The higher the number of FortiGate devices, the higher the number of tunnels to configure on each FortiGate device. For example, in a topology with five FortiGate devices, you would need to configure four tunnels on each device, for a total of 20 tunnels. This topology causes less latency and requires much less HQ bandwidth than hub-and-spoke, but requires each FortiGate device to be more powerful. Partial mesh attempts to compromise, minimizing required resources but also latency. Partial mesh can be appropriate if communication is not required between every location. However, the configuration of each FortiGate device is more complex than in hub-and-spoke. Routing, especially, may require extensive planning.

Generally, the more locations you have, hub-and-spoke will be cheaper, but slower, than a mesh topology. Mesh places less strain on the central location. It's more fault-tolerant, but also more expensive.

DO NOT REPRINT**© FORTINET**

VPN Topologies—Comparison

Hub-and-Spoke	Partial Mesh	Full Mesh
Easy configuration	Moderate configuration	Complex configuration
Few tunnels	Medium number of tunnels	Many tunnels
High central bandwidth	Medium bandwidth in hub sites	Low bandwidth
Not fault tolerant	Some fault tolerance	Fault tolerant
Low system requirements on average, but high for center	Medium system requirements	High system requirements
Scalable	Somewhat scalable	Difficult to scale
No direct communication between spokes	Direct communication between some sites	Direct communication between all sites

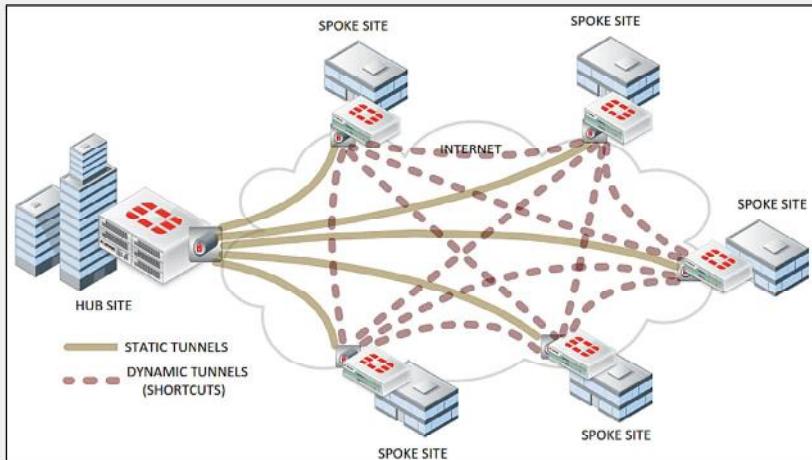
To review, this slide shows a high-level comparison of VPN topologies. You should choose the topology that is most appropriate to your situation.

DO NOT REPRINT

© FORTINET

Auto-Discovery VPN

- Dynamically negotiates on-demand direct VPNs between spokes
 - Provides the benefits of a full mesh topology over a hub-and-spoke or partial mesh deployment
 - Dynamic routing is recommended to learn routes between hub and spokes and scale up easier
 - Static routing also works, but should be used for small deployments only



FORTINET
Training Institute

14

Each VPN topology has its advantages and disadvantages.

Auto-discovery VPN (ADVPN) is a FortiGate feature that achieves the benefits of a full-mesh topology with the easier configuration and scalability benefits of hub-and-spoke and partial-mesh topologies.

First, you add the VPN configurations for building either a hub-and-spoke or a partial-mesh topology, to the FortiGate devices. Then, you enable ADVPN on the VPNs. ADVPN dynamically negotiates tunnels between spokes (without having them preconfigured) to get the benefits of a full-mesh topology.

You can use dynamic routing and static routing to deploy ADVPN. A dynamic routing protocol, such as BGP, is usually deployed in large networks because it enables you to exchange routing information between spokes and hub easier, and as a result, to scale up. You can also use static routing to deploy ADVPN, but it is recommended to do so in small networks that are not likely to grow considerably.

Whether you use dynamic routing or not, after a shortcut is negotiated, FortiGate automatically adds routes through the shortcut to redirect spoke-to-spoke traffic through it.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which IPsec protocol is not supported by FortiGate?

- A. IKEv2
- B. AH

2. Which VPN topology is the most fault tolerant?

- A. Full mesh
- B. Hub-and-spoke

DO NOT REPRINT

© FORTINET

Lesson Progress



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

Good job! You have now been introduced to IPsec.

Now, you will learn about IPsec configuration.

DO NOT REPRINT

© FORTINET

IPsec Configuration

Objectives

- Learn about the IPsec wizard
- Identify and understand the phases of IKEv1
- Understand IPsec phase 1 and phase 2 settings

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

By demonstrating competence in IPsec configuration, you will be able to successfully determine the settings required for your IPsec VPN deployment.

DO NOT REPRINT

© FORTINET

IPsec Wizard

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Name: ToRemoteBackup

Template type: Site to Site | Hub-and-Spoke | Remote Access | Custom

NAT configuration: No NAT between sites
This site is behind NAT
The remote site is behind NAT

Remote device type: FortiGate | Cisco

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

VPN Creation Wizard

1. The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	ToRemoteBackup
Local address group	ToRemoteBackup_local
Remote address group	ToRemoteBackup_remote
Phase 2 interface	ToRemoteBackup
Static route	static
Blackhole route	static
Local to remote policies	vpn_ToRemoteBackup_local
Remote to local policies	vpn_ToRemoteBackup_remote

© Fortinet Inc. All Rights Reserved.

18

When you create an IPsec tunnel on the GUI, FortiGate redirects you to the **IPsec Wizard**. The wizard simplifies the creation of the new VPN by walking you through a four to five-step process. The first step is to select a template type. If you want to manually configure your VPN, you can select **Custom** as **Template type**, upon which FortiGate takes you directly to the phase 1 and phase 2 settings of the new VPN.

If you want the wizard to configure the VPN for you, then select the template type (**Site to Site**, **Hub-and-Spoke**, or **Remote Access**) that best matches your VPN. After that, the wizard asks you for key information such as the remote gateway information, authentication method, interfaces involved, and subnets. Based on the input you provide, the wizard applies one of the preconfigured IPsec tunnel templates comprising IPsec phase 1 and 2 settings and other related firewall address objects, routing settings, and firewall policies needed for the new tunnel to work.

In addition, the wizard shows a network diagram that changes based on the input provided. The purpose of the diagram is for the administrator to have a visual understanding of the IPsec VPN deployment that the wizard configures based on the input received.

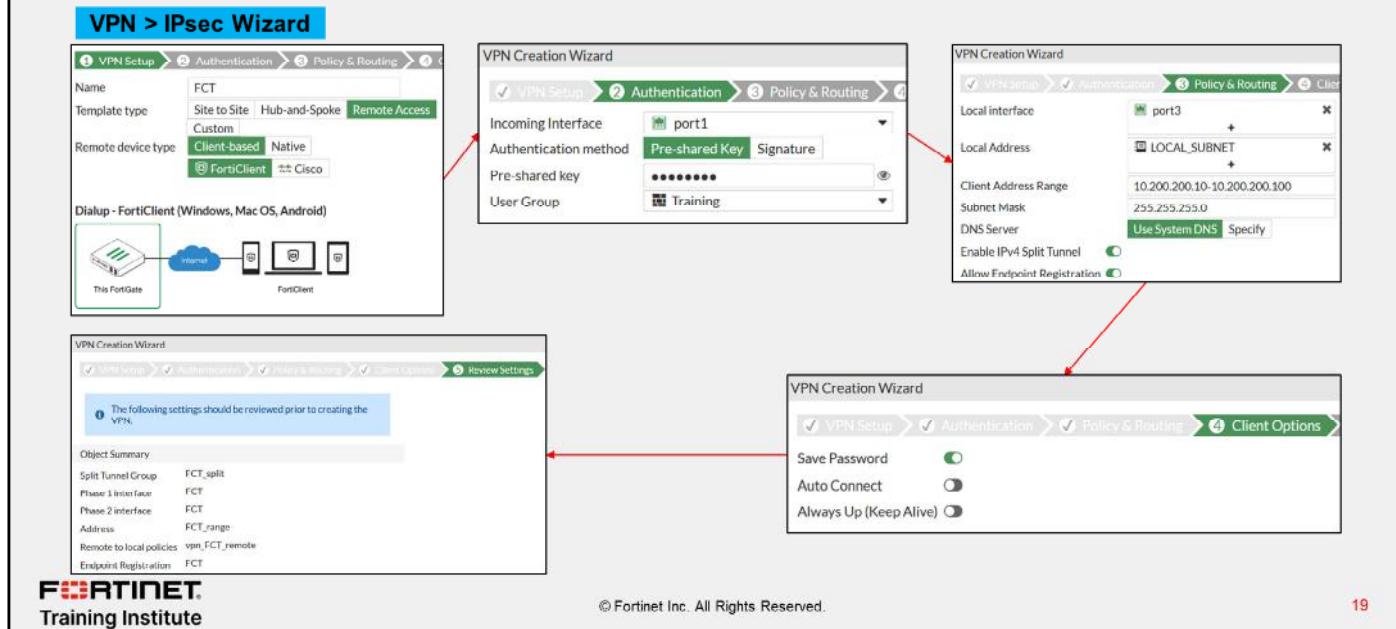
At the end of the wizard, the wizard provides a summary of the configuration changes made in the system, and that the administrator can review if needed.

If you are new to FortiGate, or don't have much experience with IPsec VPNs, using the IPsec wizard is recommended. You can later adjust the configuration applied by the wizard to match your specific needs.

DO NOT REPRINT
© FORTINET

Using the IPsec Wizard for a FortiClient VPN

- Simplifies IPsec configuration for a FortiClient VPN



A common use of the IPsec wizard is for configuring a remote access VPN for FortiClient users. The wizard enables IKE mode config, XAuth, and other appropriate settings for FortiClient users. You will learn more about IKE mode config and XAuth in this lesson.

The images on this slide show the four-step process used by the IPsec wizard for assisting the administrator on the FortiClient VPN configuration.

DO NOT REPRINT
© FORTINET

IPsec Tunnel Templates

VPN > IPsec Tunnel Template

Template	Description
Site to Site - FortiGate	Static tunnel between this FortiGate and a remote FortiGate.
Site to Site - FortiGate (SD-WAN)	Static tunnel between this FortiGate using SD-WAN and a remote FortiGate.
Dialup - FortiGate	On-demand tunnel between two FortiGate devices.
Site to Site - Cisco	Static tunnel between this FortiGate and a remote Cisco firewall.
Dialup - Cisco Firewall	On-demand tunnel between a FortiGate device and a Cisco Firewall.
Dialup - FortiClient (Windows, Mac OS, Android)	On-demand tunnel for users using the FortiClient software.
Dialup - iOS (Native)	On-demand tunnel for iPhone/iPad users using the native iOS IPsec client.
Dialup - Android (Native L2TP/IPsec)	On-demand tunnel for Android users using the native L2TP/IPsec client.
Dialup - Windows (Native L2TP/IPsec)	On-demand tunnel for Windows users using the native L2TP/IPsec client.
Dialup - Cisco IPsec Client	On-demand tunnel for users using the Cisco IPsec client.
Hub-and-Spoke - FortiGate (Spoke)	Spoke role in a Hub-and-Spoke auto-discovery VPN configuration.
Hub-and-Spoke - FortiGate (Hub)	Hub role in a Hub-and-Spoke auto-discovery VPN configuration.

Click **View** to review the template details

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

20

The IPsec wizard uses one of the templates shown on this slide when applying the configuration for the new IPsec tunnel. You can review the settings of a template by selecting the template, and then clicking **View**. You cannot change the template settings.

DO NOT REPRINT**© FORTINET**

Phase 1—Overview

- Each peer of the tunnel—the initiator and the responder—connects and begins to set up the VPN
- On the first connection, the channel is not secure
 - Unencrypted keys can be intercepted
- To exchange sensitive private keys, both peers create a secure channel
 - Both peers negotiate the real keys for the tunnel later

Phase 1 takes place when each peer of the tunnel—the initiator and the responder—connects and begins to set up the VPN. The initiator is the peer that starts the phase 1 negotiation, while the responder is the peer that responds to the initiator request.

When the peers first connect, the channel is not secure. An attacker in the middle could intercept unencrypted keys. Neither peer has a strong guarantee of the other peer's identity, so how can they exchange sensitive private keys? They can't. First, both peers create a secure tunnel. Then, they use this secure tunnel to negotiate the real keys for the tunnel later.

DO NOT REPRINT**© FORTINET**

Phase 1—How it Works

1. Authenticate peers
 - PSK or digital signature
 - XAuth
2. Negotiate one bidirectional SA (called IKE SA)
 - In IKE v1, two possible ways:
 - Main mode
 - Aggressive mode
 - Not the same as IPsec SA
 - Encrypted tunnel for Diffie-Hellman (DH)
3. DH exchange for secret keys



© Fortinet Inc. All Rights Reserved.

22

Now you'll examine how phase 1 works.

The purpose of phase 1 is to authenticate peers and set up a secure channel for negotiating the phase 2 SAs (or IPsec SAs) that are later used to encrypt and decrypt traffic between the peers. To establish this secure channel, the peers negotiate a phase 1 SA. This SA is called the IKE SA and is bidirectional.

To authenticate each other, the peers use two methods: pre-shared key or digital signature. You can also enable an additional authentication method, XAuth, to enhance authentication.

In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel.

At the end of phase 1, the negotiated IKE SA is used to negotiate the DH keys that are used in phase 2. DH uses the public key (that both ends know) plus a mathematical factor called a nonce, in order to generate a common private key. With DH, even if an attacker can listen to the messages containing the public keys, they cannot determine the secret key.

DO NOT REPRINT

© FORTINET

Phase 1—Network

Network

- IP Version: IPv4 (selected)
- Remote Gateway: Static IP Address (selected, value: 10.200.3.1)
- IP Address: port1
- Interface: port1
- Local Gateway:
- Mode Config:
- NAT Traversal:
- Keepalive Frequency: 10
- Dead Peer Detection:
- DPD retry count: 3
- DPD retry interval: 20 s
- Forward Error Correction:

Local Gateway

- Remote Gateway: Static IP Address
- IP Address: Static IP Address
- Interface: Dialup User
- Local Gateway:
- Local Gateway: Primary IP (selected, value: 10.200.10.1)

FOURINET
Training Institute

© Fortinet Inc. All Rights Reserved.

23

Phase 1 configuration is broken down on the GUI into four sections: **Network**, **Authentication**, **Phase 1 Proposal**, and **XAUTH**. You will learn about the settings available on each section. You will learn about some of these settings in more detail on separate slides.

The section shown on this slide corresponds to the **Network** settings. The section includes the settings related to the connectivity of the IPsec tunnel:

- IP Version:** select the IP version to use for the IPsec tunnel. Note that this defines only the IP version of the outer layer of the tunnel (after encapsulation). The packets being encapsulated (protected traffic) can be IPv4 or IPv6, and their IP version is defined in the phase 2 selectors.
- Remote Gateway:** defines the type of the remote gateway. There are three types: **Static IP Address**, **Dialup User**, and **Dynamic DNS**. You will learn more about these types later in this lesson.
- IP Address:** the IP address of the remote gateway. This field appears only when you select **Static IP Address** as **Remote Gateway**.
- Interface:** refers to the interface where the IPsec tunnel terminates on the local FortiGate. Usually, this is the interface connected to the internet or the WAN. You need to make sure there is an active route to the remote gateway through this interface, otherwise the tunnel won't come up.
- Local Gateway:** enable this setting when the interface where the tunnel terminates has multiple addresses assigned, and you want to specify which address to use for the tunnel. When you enable this setting, you see three options: **Primary IP**, **Secondary IP**, and **Specify**. Select **Specify** if you want to use an IP address different from the primary or secondary IP address.
- Mode Config:** Enables automatic configuration through IKE. FortiGate acts as an *IKE mode config client* when you enable **Mode Config** and you set **Remote Gateway** to either **Static IP address** or **Dynamic DNS**. If you set **Remote Gateway** to **Dialup User**, FortiGate acts as an *IKE mode config server*, and more configuration options appear on the GUI. You will learn more about **Mode Config** in this lesson.

DO NOT REPRINT

© FORTINET

Phase 1—Network (Contd)

The screenshot shows the 'New VPN Tunnel' configuration screen. The 'Network' section is highlighted in yellow, containing fields for Name (ToRemote), IP Version (IPv4 selected), Remote Gateway (Static IP Address 10.200.3.1), IP Address (10.200.3.1), Interface (port1), Local Gateway (disabled), Mode Config (disabled), NAT Traversal (Enable selected), Keepalive Frequency (10), Dead Peer Detection (On Demand selected), DPD retry count (3), DPD retry interval (20), and Forward Error Correction (Egress selected). A red box highlights the 'Advanced...' button. A red arrow points from this button to the 'Advanced...' section on the right, which contains options for Add route, Auto discovery sender, Auto discovery receiver, Exchange interface IP, Device creation, and Aggregate member, each with an 'Enabled' or 'Disabled' checkbox.

Advanced...

Add route	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Auto discovery sender	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Auto discovery receiver	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Exchange interface IP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Device creation	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Aggregate member	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

24

The following are the other options available on the GUI in the **Network** section:

- **NAT Traversal:** The option controls the behavior for NAT traversal. You will learn more about NAT traversal later in this lesson.
- **Keepalive Frequency:** When you enable NAT traversal, FortiGate sends keepalive probes at the configured frequency.
- **Dead Peer Detection:** Use dead peer detection (DPD) to detect dead tunnels. There are three DPD modes. **On Demand** is the default mode. You will learn more about DPD later in this lesson.
- **Forward Error Correction:** Forward error correction (FEC) is a technique that you can use to reduce the number of retransmissions in IPsec tunnels established over noisy links, at the expense of using more bandwidth. You can enable FEC on egress and ingress, and it is only supported when you disable IPsec hardware offloading. You will learn more about IPsec hardware offloading later in this lesson.
- **Advanced:**
 - **Add route:** Disable this setting if you are using a dynamic routing protocol over IPsec and do not want FortiGate to automatically add static routes.
 - **Auto discovery sender:** Enable this setting on a hub if you want the hub to facilitate ADVPN shortcut negotiation for spokes. When enabled, the hub sends a shortcut offer to the spoke to indicate that it can establish a shortcut to the remote spoke.
 - **Auto discovery receiver:** Enable this setting on a spoke if you want the spoke to negotiate an ADVPN shortcut.
 - **Exchange interface IP:** Enable this setting to allow the exchange of IPsec interface IP addresses. This allows a point-to-multipoint connection between the hub and spokes..
 - **Device creation:** Enable this setting to instruct FortiOS to create an interface for every dial-up client. To increase performance, disable this setting in dial-up servers with many dial-up clients.
 - **Aggregate member:** FortiGate allows you to aggregate multiple IPsec tunnels into a single interface. Enable this option if you want the tunnel to become an aggregate member.

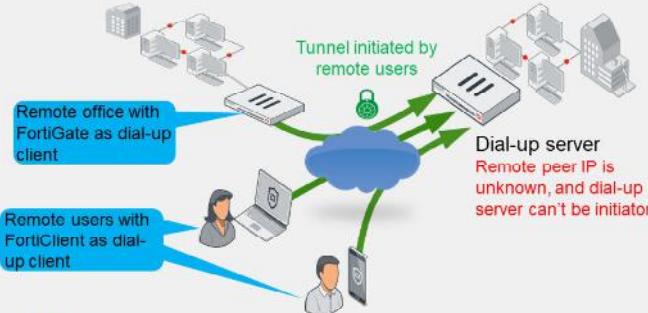
DO NOT REPRINT

© FORTINET

Phase 1—Network—Remote Gateway

Dial-up user

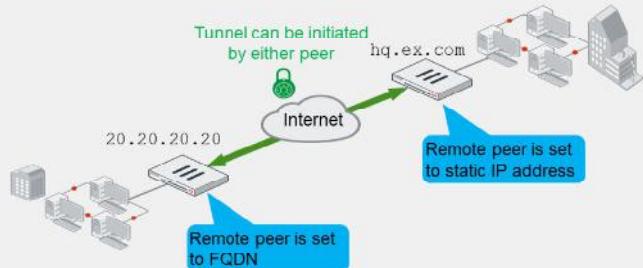
- Two roles: dial-up server and client
- Dial-up server doesn't know client address
 - Dial-up client is always the initiator
- VPN peers:
 - FortiGate to FortiClient (or third-party client)
 - FortiGate to FortiGate (or third-party gateway)



FORTINET
Training Institute

Static IP address / dynamic DNS

- Dynamic DNS uses FQDN
- The address of the remote peer is known
 - Local peer can be initiator or responder
- VPN peers:
 - FortiGate to FortiGate (or third-party gateway)



© Fortinet Inc. All Rights Reserved.

25

You have three options when configuring the remote gateway type of your VPN: **Dialup User**, **Static IP Address**, and **Dynamic DNS**.

Use **Dialup User** when the remote peer IP address is unknown. The remote peer whose IP address is unknown acts as the dial-up client, and this is often the case for branch offices and mobile VPN clients that use dynamic IP addresses, and no dynamic DNS. The dial-up client must know the IP address or FQDN of the remote gateway, which acts as the dial-up server. Because the dial-up server doesn't know the remote peer address, only the dial-up client can initiate the VPN tunnel.

Usually, dial-up clients are remote and mobile employees with FortiClient on their computer or handheld devices. You can also have a FortiGate device acting as a dial-up client for a remote office. One dial-up server configuration on FortiGate can be used for multiple IPsec tunnels from many remote offices or users.

Use **Static IP Address** or **Dynamic DNS** when you know the remote peer address. If you select **Static IP Address**, then you need to provide an IP address. If you select **Dynamic DNS**, then you need to provide a fully qualified domain name (FQDN), and make sure FortiGate can resolve that FQDN. When both peers know the remote peer address, that is, the remote gateway on both peers is set to **Static IP Address** or **Dynamic DNS**, then any peer can initiate the VPN tunnel.

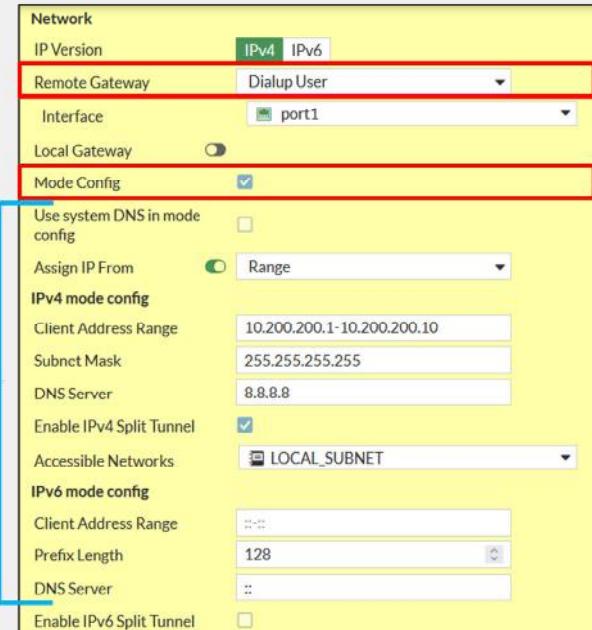
Note that in a dial-up setup, the dial-up client is just a VPN peer with the remote gateway set to **static IP address** or **dynamic DNS**. When setting your VPN, you can combine different types of remote gateways. For obvious reasons, a tunnel in which both peers has the remote gateway set to **Dialup user** won't work.

DO NOT REPRINT
© FORTINET

Phase 1—Network—IKE Mode Config

- Like DHCP, automatically configures VPN clients' virtual network settings
- By default, FortiClient VPNs use it to retrieve their VPN IP address settings from FortiGate
- You must enable **Mode Config** on both peers

IKE mode config settings are only displayed if **Remote Gateway** is set to **Dialup User**



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

26

IKE Mode Config is similar to DHCP because a server assigns network settings such as IP address, netmask, and DNS servers, to clients. This assignment takes place over IKE messages.

When you enable **Mode Config** on a FortiGate device acting as dial-up server, it pushes network settings to dial-up clients. The dial-up clients are usually FortiClient peers, but they can also be FortiGate peers.

For IKE mode config to work, you must enable the feature on both peers. On FortiClient, **Mode Config** is enabled by default, but on FortiGate, you must manually enable it.

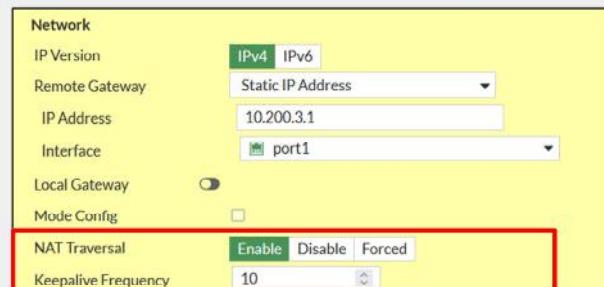
Note that the IKE **Mode Config** settings, are displayed on the GUI only when you set **Remote Gateway** to **Dialup User**. On the FortiGate device acting as dial-up client, you can select **Mode Config** on the GUI, but the additional settings are not displayed.

DO NOT REPRINT

© FORTINET

Phase 1—Network—NAT Traversal (NAT-T)

- ESP can't support NAT because it has no port numbers
- If **NAT Traversal** is set to **Enable**, it detects whether NAT devices exist on the path
 - If yes, both ESP and IKE use UDP port 4500
 - Recommended if the initiator or responder is behind NAT
- If **NAT Traversal** is set to **Forced**:
 - ESP and IKE always use UDP port 4500, even when there are no NAT devices on the path
- Keepalive probes are sent frequently to keep the connection across the routers active



The ESP protocol usually has problems crossing devices that are performing NAT. One of the reasons is that ESP does not use port numbers, like TCP and UDP do, to differentiate one tunnel from another.

To solve this, NAT transversal (NAT-T) was added to the IPsec specifications. When NAT-T is enabled on both ends, peers can detect any NAT device along the path. If NAT is found, then the following occurs on both peers:

- IKE negotiation switches to using UDP port 4500.
- ESP packets are encapsulated in UDP port 4500.

So, if you have two FortiGate devices that are behind, for example, an ISP modem that performs NAT, you will probably need to enable this setting.

When you set the **NAT Traversal** setting to **Forced**, UDP port 4500 is always used, even when there is no NAT device along the path.

When you enable NAT-T, the **Keepalive Frequency** option shows the interval (in seconds) at which FortiGate sends keepalive probes. You need NAT-T when there is one or more routers along the path performing NAT. The purpose of the keepalive probes is to keep the IPsec connection active across those routers along the path.

Phase 1—Network—Dead Peer Detection (DPD)

- Mechanism to detect a dead tunnel
- Useful in redundant VPNs, where multiple paths are available
- Three modes:
 - **On Demand:** DPD probes are sent when there is no inbound traffic
 - **On Idle:** DPD probes are sent when there is no traffic
 - **Disabled:** only reply to DPD probes—don't send probes

Network			
IP Version	IPv4	IPv6	
Remote Gateway	Static IP Address		
IP Address	10.200.3.1		
Interface	port1		
Local Gateway	<input checked="" type="checkbox"/>		
Mode Config	<input type="checkbox"/>		
NAT Traversal	Enable	Disable	
Keepalive Frequency	10		
Dead Peer Detection	Disable	On Idle	On Demand
DPD retry count	3		
DPD retry interval	20	s	
Forward Error Correction	Egress	Ingress	

After the peers negotiate the IPsec SAs of a tunnel and, therefore, the tunnel is considered up, the peers usually don't negotiate another IPsec SA until it expires. In most cases, the IPsec SA expires every few hours. This means that if there is a network disruption along the path of the tunnel before the IPsec SA expires, the peers will continue to send traffic through the tunnel even though the communication between the sites is disrupted.

When you enable DPD, DPD probes are sent to detect a failed (or dead) tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to fail over to a backup connection when the primary connection fails to keep the connectivity between the sites up.

FortiGate supports three DPD modes:

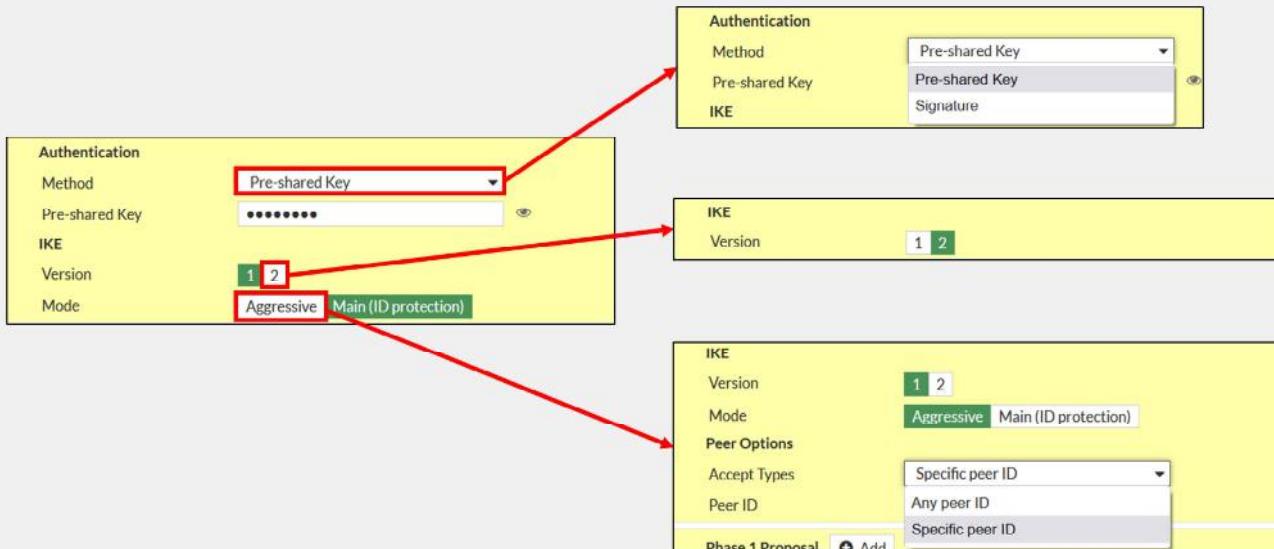
- **On Demand:** FortiGate sends DPD probes if there is only outbound traffic through the tunnel, but no inbound. Because network applications are usually bidirectional, observing only traffic on the outbound direction could be an indication of a network failure.
- **On Idle:** FortiGate sends DPD probes when no traffic is observed in the tunnel. An idle tunnel does not necessarily mean the tunnel is dead. Avoid this mode if you have many tunnels, because the overhead introduced by DPD can be very resource intensive.
- **Disabled:** FortiGate replies only to DPD probes received. FortiGate never sends DPD probes to the remote peer and therefore cannot detect a dead tunnel.

The default DPD mode is **On Demand**. In terms of scalability, **On Demand** is a better option than **On Idle**.

DO NOT REPRINT

© FORTINET

Phase 1—Authentication



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

29

Now, you will learn about the **Authentication** section in phase 1 configuration:

- Method:** FortiGate supports two authentication methods: **Pre-shared Key** and **Signature**. When you select **Pre-shared Key**, you must configure both peers with the same pre-shared key. When you select **Signature**, phase 1 authentication is based on digital certificate signatures. Under this method, the digital signature on one peer is validated by the presence of the CA certificate installed on the other peer. That is, on the local peer, you need to install both the local peer's certificate and the CA certificate that issued the remote peer certificate.
- Version:** allows you to select the IKE version to use. When selecting version **2**, aggressive and main modes disappear because they don't apply to IKEv2.
- Mode:** refers to the IKEv1 mode. Two options are available: **Aggressive** and **Main (ID protection)**. You will learn more about these modes in this lesson.

DO NOT REPRINT**© FORTINET**

Phase 1—Authentication—Modes

Aggressive

- Not as secure as main mode
- Faster negotiation (three packets exchanged)
- Required when peer ID check is needed

Main

- More secure
- Slower negotiation (six packets exchanged)
- Often used when peer ID check is not needed

IKE supports two different negotiation modes: main and aggressive. Which one should you use?

To answer that question, we can analyze three categories: security, performance, and deployment.

Security wise, main mode is considered more secure because the pre-shared key hash is exchanged encrypted, whereas in aggressive mode, the hash is exchanged unencrypted. Although the attacker would still have to guess the cleartext pre-shared key for the attack to be successful, the fact that the pre-shared key hash has been encrypted in main mode reduces considerably the chances of a successful attack.

In terms of performance, aggressive mode may be a better option. This is because the negotiation is completed after only three packets are exchanged, whereas in main mode, six packets are exchanged. For this reason, you may want to use aggressive mode when a great number of tunnels terminate on the same FortiGate device, and performance is a concern.

Another use case for aggressive mode, is when there is more than one dial-up tunnel terminating on the same FortiGate IP address, and the remote peer is authenticated using a peer ID because its IP address is dynamic. Because peer ID information is sent in the first packet in an aggressive mode negotiation, then FortiGate can match the remote peer with the correct dial-up tunnel. The latter is not possible in main mode because the peer ID information is sent in the last packet, and after the tunnel has been identified.

When both peers know each other's IP address or FQDN, you may want to use main mode to take advantage of its more secure negotiation. In this case, FortiGate can identify the remote peer by its IP address and, as a result, associate it with the correct IPsec tunnel.

DO NOT REPRINT

© FORTINET

Phase 1—Phase 1 Proposal

Encryption	Authentication
AES128	SHA256
AES256	SHA256
AES128	SHA1
AES256	SHA1

Diffie-Hellman Groups: 32, 31, 30, 29, 28, 27, 21, 20, 19, 18, 17, 16, 15, 14, 5, 2, 1

Key Lifetime (seconds): 86400

Local ID: []

Encryption
AES128
DES
3DES
AES128
AES192
AES256

Authentication
SHA256
MD5
SHA256
SHA384
SHA512

Now, you will learn about the **Phase 1 Proposal** section of phase 1 configuration. This section allows you to enable the different proposals that FortiGate supports when negotiating the IKE SA (or phase 1 SA). You can combine different parameters to suit your security needs. You must at least configure one combination of encryption and authentication algorithms, or several.

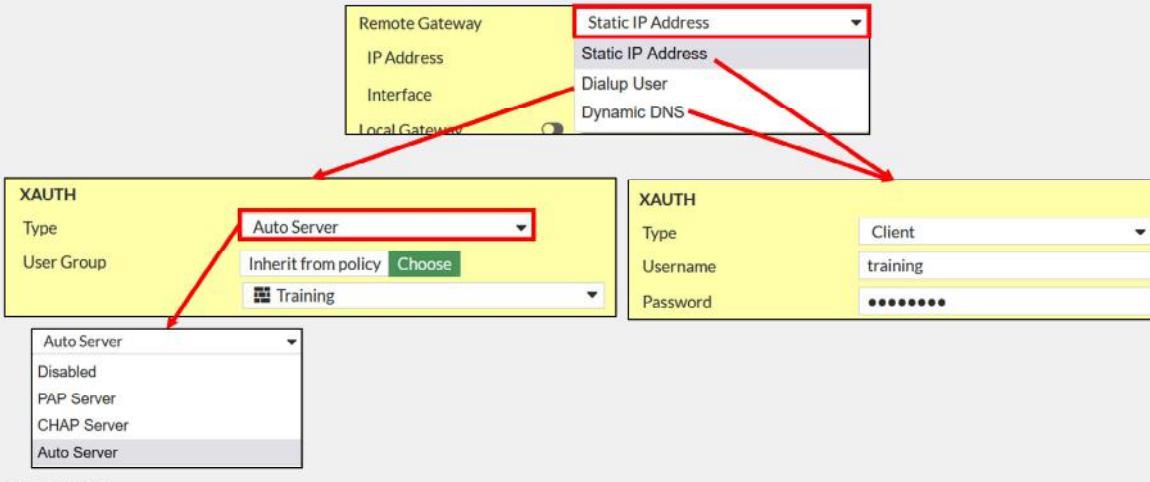
- **Encryption:** select the algorithm to use for encrypting and decrypting the data.
- **Authentication:** select the authentication algorithm to use for verifying the integrity and authenticity of the data.
- **Diffie-Hellman Groups:** The Diffie-Hellman (DH) algorithm is used during IKE SA negotiation. The use of DH in phase 1 is mandatory and can't be disabled. You must select at least one DH group. The higher the DH group number, the more secure the phase 1 negotiation is. However, a higher DH group number also results in a longer compute time.
- **Key Lifetime:** defines the lifetime of the IKE SA. At the end of the lifetime, a new IKE SA is negotiated.
- **Local ID:** if the peer accepts a specific peer ID, type that same peer ID in this field.

DO NOT REPRINT

© FORTINET

Phase 1—Extended Authentication (XAuth)

- XAuth adds stronger authentication: username + password
- You can authorize all users who belong to a specific user group or inherit it from the matching policy



Phase 1 supports two types of authentication: pre-shared keys and digital signatures. The XAuth extension, sometimes called phase 1.5, forces remote users to authenticate additionally with their credentials (username and password). So, additional authentication packets are exchanged if you enable it. What is the benefit? Stronger authentication.

When you set **Remote Gateway** to **Dialup User**, FortiGate acts as the authentication server. The **XAUTH** section shows the authentication server type options: **PAP Server**, **CHAP Server**, and **Auto Server**. In the example shown on this slide, **Auto Server** is selected, which means that FortiGate automatically detects the authentication protocol used by the client.

After you select the authentication server type, you configure how user group matching is performed. There are two options: **Inherit from policy** and **Choose**. The latter is used in the example on this slide, and allows you to select one of the user groups available on FortiGate. Note that, when you select **Choose**, you must configure a separate dial-up VPN for every group of users that require a different network access policy.

The other way to authenticate VPN users with XAuth is by selecting **Inherit from policy**. When you select this option, FortiGate authenticates users based on their matching IPsec policy and, as a result, the configuration for controlling network access is simpler. That is, you control network access by configuring multiple policies for different user groups, instead of configuring multiple tunnels for different user groups. The **Inherit from policy** option follows a similar authentication approach used for SSL VPN remote users. You will learn more about SSL VPN in another lesson.

When **Remote Gateway** is set to **Static IP Address** or **Dynamic DNS**, FortiGate acts as the client, and the **XAUTH** section shows the **Client** option as **Type**. You can then set the credentials that FortiGate uses to authenticate against the remote peer through XAuth.

DO NOT REPRINT**© FORTINET**

Phase 2—How it Works

- Negotiates two unidirectional IPsec SAs for ESP
 - Protected by phase 1 IKE SA
- When IPsec SAs are about to expire, it renegotiates
 - Optionally, if **Perfect Forward Secrecy** is enabled, FortiGate uses DH to generate new keys each time phase 2 expires
- Each phase 1 can have multiple phase 2s
 - High security subnets can have stronger ESP

After phase 1 has established a secure channel to exchange data, phase 2 begins.

Phase 2 negotiates security parameters for two IPsec SAs over the secure channel established during phase 1. ESP uses IPsec SAs to encrypt and decrypt the traffic exchanged between sites.

Phase 2 does not end when ESP begins. Phase 2 periodically renegotiates IPsec SAs to maintain security. If you enable **Perfect Forward Secrecy**, each time phase 2 expires, FortiGate uses DH to recalculate new secret keys. In this way, new keys are not derived from older keys, making it much harder for an attacker to crack the tunnel.

Each phase 1 can have multiple phase 2s. When would this happen? For example, you may want to use different encryption keys for each subnet whose traffic is crossing the tunnel. How does FortiGate select which phase 2 to use? By checking which phase 2 selector (or quick mode selector) matches the traffic.

DO NOT REPRINT

© FORTINET

Phase 2—Phase 2 Selectors

- Determines the encryption domain
 - You can configure multiple selectors for granular control
 - If traffic does not match a selector, it is dropped
 - In point-to-point VPNs, selectors must match
 - The source on one FortiGate is the destination setting on the other
- Select which selector to use using:
 - **Local Address** and **Remote Address**
 - **Protocol** number
 - **Local Port** and **Remote Port**

In phase 2, you must define the encryption domain (or interesting traffic) of your IPsec tunnel. The encryption domain refers to the traffic that you want to protect with IPsec, and it is determined by your phase 2 selector configuration.

You can configure multiple selectors to have more granular control over traffic. When you configure a phase 2 selector, you specify the encryption domain by indicating the following network parameters:

- **Local Address** and **Remote Address**: as seen in the example shown on this slide, you can define IPv4 or IPv6 addresses using different address scopes. When selecting **Named Address** or **Named IPv6 Address**, FortiGate allows you to select an IPv4 or IPv6 firewall address object, respectively, configured in the system.
- **Protocol**: is in the **Advanced** section, and is set to **All** by default.
- **Local Port** and **Remote Port**: are also shown in the **Advanced** section, and are set to **All** by default. This applies only to port-based traffic such as TCP or UDP. You will learn more about the **Advanced** section later in this lesson.

Note that after the traffic is accepted by a firewall policy, traffic is dropped before entering the IPsec tunnel if the traffic does not match any of the phase 2 selectors configured. For this reason, usually, it's more intuitive to filter traffic with firewall policies. So, if you don't want to use phase 2 selector filtering, you can just create one phase 2 selector with both the local and remote addresses set to any subnet, like in the example shown on this slide, and then use firewall policies to control which traffic is accepted on the IPsec tunnel.

In addition, the phase 2 selector network parameters on both peers must match if the tunnel is point-to-point, that is, when the remote gateway is *not* set to dial-up user.

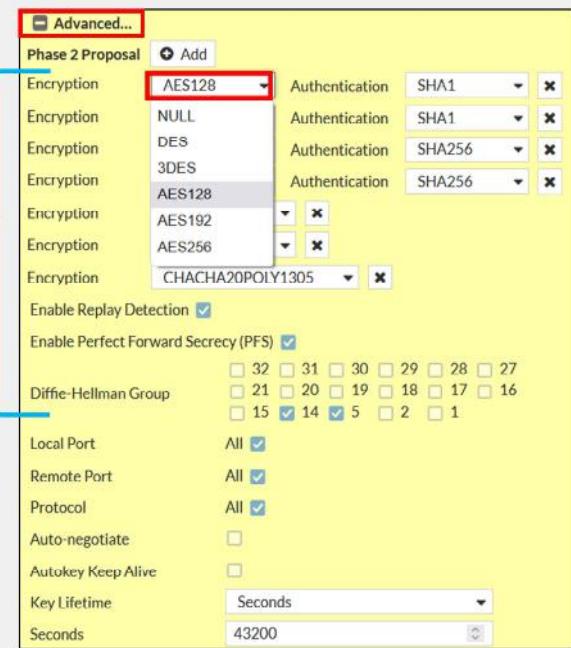
DO NOT REPRINT

© FORTINET

Phase 2—Phase 2 Proposal

- Determines the encryption algorithms
 - You can configure multiple proposals for added flexibility
 - Impacts performance and hardware offloading
- You can enable replay detection to protect against ESP replay attacks
 - Local setting

Encryption and authentication algorithms for IPsec encryption



For every phase 2 selector, you need to configure one or more phase 2 proposals. A phase 2 proposal defines the algorithms supported by the peer for encrypting and decrypting the data over the tunnel. You can configure multiple proposals to offer more options to the remote peer when negotiating the IPsec SAs.

Like in phase 1, you need to select a combination of encryption and authentication algorithms. Some algorithms are considered more secure than others, so make sure to select the algorithms that conform with your security policy. However, note that the selection of the algorithms has a direct impact on FortiGate IPsec performance. For example, **3DES** is known to be a much more resource-intensive encryption algorithm than **DES** and **AES**, which means that your IPsec throughput could be negatively impacted if you select **3DES** as the encryption algorithm. Also, note that if you select **NULL** as the encryption algorithm, traffic is not encrypted.

In addition, some encryption algorithms, such as **CHACHA20POLY1305**, are not supported for hardware offload. That is, if you have a FortiGate device that contains network processor (NP) units, you can achieve higher IPsec performance if you select an algorithm that is supported for IPsec offload by your NP unit model, such as AES or DES. For a list of supported encryption algorithms for IPsec hardware offloading, refer to <https://docs.fortinet.com>.

When configuring the phase 2 proposal, you can select **Enable Replay Detection** to detect antireplay attacks on ESP packets. Note that this is a local setting and, therefore, it is not included as part of the proposals presented by the peer during phase 2 negotiation.

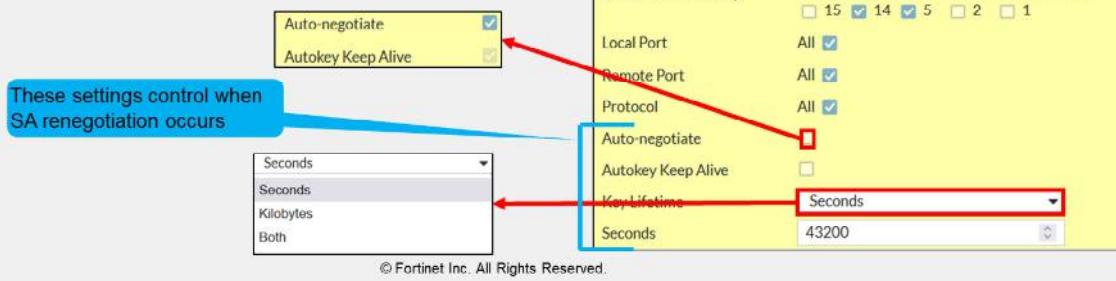
Also, if you enable **Perfect Forward Secrecy**, FortiGate uses DH to enhance security during the negotiation of IPsec SAs.

DO NOT REPRINT

© FORTINET

Phase 2—Phase 2 Proposal (Contd)

- IPsec SA expires based on the number of:
 - Seconds** (time-based)
 - Kilobytes** (volume-based)
 - Both** (whichever expires first)
- Key lifetime thresholds do not have to match for tunnel to come up
- Auto-negotiate** prevents disruption caused by SA renegotiation
- Autokey Keep Alive** keeps the tunnel up



FORTINET
Training Institute

36

IPsec SAs are periodically renegotiated to improve security, but when does that happen? It depends on the key lifetime settings configured on the phase 2 proposal.

The expiration of an IPsec SA is determined by the lifetime type and threshold configured. By default, **Key Lifetime** is set to **Seconds** (time-based). This means that when the SA duration reaches the number of seconds set as **Seconds**, the SA is considered expired. You can also set the key lifetime to **Kilobytes** (volume-based), upon which the SA expires after the amount of traffic encrypted and decrypted using that SA reaches the threshold set. Alternatively, you can select **Both** as the key lifetime type, upon which FortiGate tracks both the duration of the SA and the amount of traffic. Then, when any of the two thresholds is reached, the SA is considered expired. Note that the key lifetime thresholds do not have to match for the tunnel to come up. When thresholds are different, the peers agree on using the lowest threshold value offered between the two.

When IPsec SAs expire, FortiGate needs to negotiate new SAs to continue sending and receiving traffic over the IPsec tunnel. Technically, FortiGate deletes the expired SAs from the respective phase 2 selectors, and installs new ones. If IPsec SA renegotiation takes too much time, then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable **Auto-negotiate**. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away. The latter prevents traffic disruption by IPsec SA renegotiation.

Another benefit of enabling **Auto-negotiate** is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable **Autokey Keep Alive** and keep **Auto-negotiate** disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable **Auto-negotiate**, **Autokey Keep Alive** is implicitly enabled.

DO NOT REPRINT

© FORTINET

IPsec Hardware Offloading

- On some FortiGate models, you can offload IPsec encryption and decryption to hardware
- Hardware offloading capabilities and supported algorithms vary by processor type and model
- By default, offloading is enabled for supported algorithms
 - You can manually disable offloading:

```
config vpn ipsec phasel-interface
    edit ToRemote
        set npu-offload disable
    next
end
```

On some FortiGate models, you can offload the encryption and decryption of IPsec traffic to hardware. The algorithms that are supported depend on the NP unit model present on FortiGate. For a list of supported encryption algorithms for IPsec hardware offloading, refer to <https://docs.fortinet.com>.

By default, hardware offloading is enabled for the supported algorithms. This slide shows the commands you can use to disable hardware offloading per tunnel, if necessary.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which type of VPN peer can initiate a VPN tunnel?
 A. Dial-up server
 B. Dial-up client

2. On which phase do you configure the algorithms used for traffic encryption?
 A. Phase 1
 B. Phase 2

3. Which IKEv1 negotiation mode is faster?
 A. Aggressive
 B. Main

DO NOT REPRINT

© FORTINET

Lesson Progress



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

39

Good job! You now understand IPsec configuration.

Now, you will learn about routing and firewall policies for IPsec traffic.

DO NOT REPRINT

© FORTINET

Routing and Firewall Policies

Objectives

- Understand route-based IPsec VPNs
- Learn how to configure routing and firewall policies for IPsec traffic

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

By demonstrating competence in routing and firewall policies for IPsec VPNs, you will be able to set up appropriate routing and firewall policies for your IPsec VPN deployment.

DO NOT REPRINT**© FORTINET**

Route-Based IPsec VPNs

- Types of IPsec VPNs:
 - Route-based
 - Virtual interface for each VPN: VPN matching based on routing
 - Policy-based
 - Legacy: VPN matching based on policy. Not recommended.
- Route-based VPNs benefits:
 - Simpler operation and configuration
 - Redundancy
 - Support for:
 - L2TP-over-IPsec
 - GRE-over-IPsec
 - Dynamic routing protocols



© Fortinet Inc. All Rights Reserved.

41

FortiGate supports two types of IPsec VPNs: route-based and policy-based. Policy-based is a legacy IPsec VPN that is supported only for backward compatibility reasons, and its use *is not recommended* for new deployments. Unless otherwise stated, all IPsec VPN references in this lesson are for route-based IPsec VPNs.

In a route-based IPsec VPN, FortiGate automatically adds a virtual interface with the VPN name. This means that not only can you configure routing and firewall policies for IPsec traffic in the same way you do for non-IPsec traffic, but you also can leverage the presence of multiple connections to the same destination to achieve redundancy.

Another benefit of route-based IPsec VPNs is that you can deploy variations of IPsec VPNs such as L2TP-over-IPsec and GRE-over-IPsec. In addition, you can also enable dynamic routing protocols for scalability purposes and best path selection.

DO NOT REPRINT

© FORTINET

Routes for IPsec VPNs

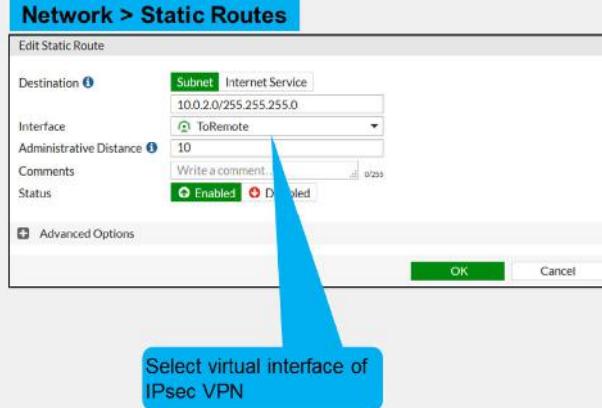
Dial-up user

```
config vpn ipsec phasel-interface
    edit "Dialup"
        set add-route enable | disable
    next
end
```

- **add-route is enabled (default)**
 - No need to configure static routes
 - Static routes are added after phase 2 is up
 - The destination is the local network presented by the dial-up client during phase 2 negotiation
 - The default route distance is 15
 - Static routes are deleted after phase 2 is down
- **add-route is disabled**
 - Useful when dynamic routing protocol is used
 - Dynamic routing protocol takes care of routing updates

Static IP address / dynamic DNS

- Static routes are needed



Although you can use dynamic routing protocols for IPsec VPNs, this lesson covers only the use of static routes.

The routing configuration needed for your IPsec VPN depends on the type of remote gateway configured. When you set the remote gateway to **Dialup User** and enable `add-route`, FortiGate automatically adds a static route for the local network presented by the remote peer during phase 2 negotiation. In addition, the route is added to the routing table only after phase 2 is up. If phase 2 goes down, the static route is removed from the routing table.

When you set the remote gateway to **Dialup User** and disable `add-route`, FortiGate does not add static routes automatically. In this case, a dynamic routing protocol is used between the remote peers to exchange routing information.

When the remote gateway is set to **Static IP Address** or **Dynamic DNS**, you must configure static routes. When you configure a static route, you select the virtual interface of the IPsec tunnel as the outgoing interface.

DO NOT REPRINT

© FORTINET

Firewall Policies for IPsec VPNs

- At least one firewall policy is needed for a tunnel to come up
- Usually two firewall policies are configured for every tunnel

Policy & Objects > Firewall Policy

New Policy

Name: Traffic to Remote

Incoming Interface: port3

Outgoing Interface: ToRemote

Source: LOCAL_SUBNET

Destination: REMOTE_SUBNET

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

NAT: Off

Policy & Objects > Firewall Policy

New Policy

Name: Traffic from Remote

Incoming Interface: ToRemote

Outgoing Interface: port3

Source: REMOTE_SUBNET

Destination: LOCAL_SUBNET

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

NAT: Off

FORTINET
Training Institute
© Fortinet Inc. All Rights Reserved.
43

You must configure at least one firewall policy that accepts traffic on your IPsec tunnel. Otherwise, the tunnel will not come up.

When you configure firewall policies for non-IPsec traffic, the policy determines the direction of the traffic that initiates sessions. The same applies to IPsec traffic. For this reason, you usually want to configure at least two firewall policies for your IPsec VPN: one incoming policy and one outgoing policy. The incoming policy allows traffic initiated from the remote site, while the outgoing policy allows traffic to be initiated from the local network.

Note that the policies are configured with the virtual tunnel interface (or phase 1 name) as the incoming or outgoing interface.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which IPsec VPN type is legacy and not recommended for new deployments?
 - A. Route-based IPsec VPN
 - B. Policy-based IPsec VPN

2. What is a configuration requirement for an IPsec tunnel to come up?
 - A. A firewall policy accepting traffic on the IPsec tunnel
 - B. A route for IPsec traffic

DO NOT REPRINT

© FORTINET

Lesson Progress



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

45

Good job! You now understand routing and firewall policies for IPsec traffic.

Now, you will learn about redundant VPNs.

DO NOT REPRINT

© FORTINET

Redundant VPNs

Objectives

- Learn about redundant VPNs
- Understand redundant VPN configuration between two FortiGate devices

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

By demonstrating competence in redundant VPNs, you will be able to add redundancy to your IPsec VPN deployment.

DO NOT REPRINT**© FORTINET**

Redundant VPNs

- If the primary VPN tunnel fails, FortiGate then routes traffic through the backup VPN
- *Partially redundant*: one peer has two connections



- *Fully redundant*: both peers have two connections



How can you make your IPsec VPN deployment more resilient? Provide a second ISP connection to your site and configure two IPsec VPNs. If the primary IPsec VPN fails, another tunnel can be used instead.

There are two types of redundant VPNs:

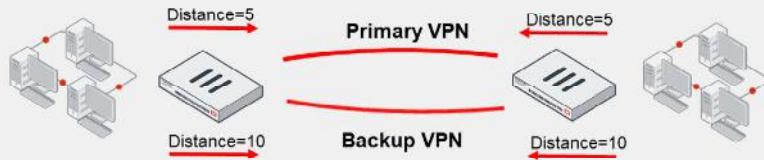
- Partially redundant: on one peer (usually the hub, where a backup ISP is available if the main ISP is down), each VPN terminates on *different* physical ports. That way, FortiGate can use an alternative VPN. On the other peer, each VPN terminates on the *same* physical port—so the spoke is not fault tolerant.
- Fully-redundant: both peers terminate their VPNs on different physical ports, so they are both fault tolerant.

DO NOT REPRINT

© FORTINET

Redundant VPN Configuration

- Add one phase 1 configuration for each tunnel. You should enable DPD on both ends.
- Add at least one phase 2 definition for each phase 1
- Add one static route for each path
 - Use distance or priority to select primary routes over backup routes
 - Alternatively, use dynamic routing
- Configure firewall policies for each IPsec interface



So, how do you configure a partially or fully redundant VPN?

First, create one phase 1 for each path—one phase 1 for the primary VPN and one for the backup VPN. You should also enable DPD on both ends.

Second, create at least one phase 2 definition for each phase 1.

Third, you must add at least one static route for each VPN. Routes for the primary VPN must have a lower distance (or lower priority) than the backup. This causes FortiGate to use the primary VPN while it's available. If the primary VPN fails, then FortiGate automatically uses the backup route. Alternatively, you could use a dynamic routing protocol, such as OSPF or BGP.

Finally, configure firewall policies to allow traffic through both the primary and backup VPNs.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which feature should be enabled in a redundant IPsec VPN deployment?

- A. DPD
- B. XAuth

2. Which setting determines whether a tunnel is used as primary or backup?

- A. Routing
- B. Firewall policies

DO NOT REPRINT

© FORTINET

Lesson Progress



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

Good job! You now understand redundant VPNs.

Now, you will learn about monitoring IPsec VPNs and reviewing their logs.

DO NOT REPRINT

© FORTINET

Monitoring and Logs

Objectives

- Learn how to monitor an IPsec VPN status
- Check IPsec VPN logs

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

By demonstrating competence in monitoring and logs, you will be able to monitor IPsec VPN and review past events.

DO NOT REPRINT

© FORTINET

IPsec VPN Status—IPsec Monitor Widget

- Monitor IPsec VPN tunnels
 - Display status and statistics
 - Bring up or bring down VPNs

Dashboard > Network > IPsec

IPsec

Name Remote Gateway Peer ID Incoming Data Outgoing Data Phase 1 Phase 2 Selectors

Custom 1

ToRemote 10.200.1.1

Reset Statistics

Bring Up

Bring Down

Locate on VPN Map

Show Matching Logs

Entire Tunnel

Phase 2 Selector: ToRemote

All Phase 2 Selectors

2.18 kB

2.18 kB

ToRemote ToRemote1 ToRemote2

Data received Data sent

Phase 1 name and status

Phase 2 name and status

Comments

Created

Phase 2 Protocols

Proxy Destination Ports

Proxy ID Destination

Proxy ID Source

Proxy Source Ports

Remote Port

Status

Timeout

XAUTH User

Apply Cancel

VPN status

Bring down the entire tunnel or the phase 2 only

More columns available

© Fortinet Inc. All Rights Reserved.

52

On the GUI dashboard, you can use the IPsec widget to monitor the status of your IPsec VPNs. The widget shows the phase 1 and phase 2 status of an IPsec VPN.

You can also bring up or bring down individual VPNs, and get additional details. When you bring up an IPsec VPN using the IPsec widget, you can choose between bringing up a particular phase 2 selector or all phase 2 selectors in that VPN. Because bringing up a phase 2 selector requires bringing up its phase 1 first, then bringing up a phase 2 selector results in its phase 1 also coming up.

To bring down the VPN, you can choose between bringing down a particular phase 2 selector, all selectors, or the entire tunnel. When you bring down the entire tunnel, you bring down all phase 2 selectors as well as the phase 1.

The **Name** column indicates the VPN status. The VPN is up when at least one of its phase 2 selectors is up. If all phase 2 selectors are down, the VPN status is also down. The **Phase 1** and **Phase 2 Selectors** columns indicate the status of phase 1 and phase 2 selectors, respectively.

The IPsec widget also displays the amount of data sent and received through the tunnel. When you right-click any of the columns, a menu opens with a list of all the columns available. You can enable additional columns to get further details about the IPsec tunnels.

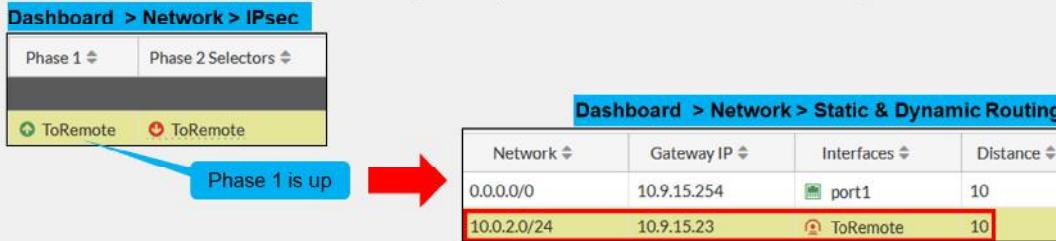
In the example shown on this slide, the **ToRemote** VPN is up because at least one of its phase 2 selectors (**ToRemote1**) is up.

DO NOT REPRINT

© FORTINET

Monitor IPsec Routes

- IPsec routes appear in the routing table after:
 - Phase 1 comes up, if the remote gateway is set to static IP address or dynamic DNS



- Phase 2 comes up, if the remote gateway is set to dial-up user



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

53

If you set the remote gateway to **Static IP Address** or **Dynamic DNS**, the static routes for these tunnels become active in the routing table after phase 1 comes up. Phase 1 negotiation is started automatically because automatic negotiation is enabled on phase 1 by default. This behavior allows FortiGate to match interesting traffic to the right tunnel. Moreover, if phase 2 is not up, traffic matching the static route triggers a phase 2 negotiation, which eventually results in the tunnel (or phase 2) to come up.

When you set the remote gateway to **Dialup User**, by default, a static route for the destination network is added after phase 2 comes up. The distance set for the static route is 15. If phase 2 goes down, the route is removed from the routing table.

DO NOT REPRINT

© FORTINET

IPsec Logs

Log & Report > System Events > VPN Events

Date/Time	Level	Action	Message	VPN Tunnel
Yesterday	INFO	negotiate	success	progress IPsec phase 2
Yesterday	INFO	negotiate	success	progress IPsec phase 2
Yesterday	INFO	phase2-up		IPsec phase 2 status change
Yesterday	INFO	install_sa		install IPsec SA
Yesterday	INFO	phase2-down		IPsec phase 2 status change
Yesterday	INFO	tunnel-stats		IPsec tunnel statistics
Yesterday	INFO	negotiate	success	negotiate IPsec phase 2
Yesterday	INFO	negotiate	success	progress IPsec phase 2
Yesterday	INFO	tunnel-up		IPsec connection status change
Yesterday	INFO	phase2-up		IPsec phase 2 status change
Yesterday	INFO	Install_sa		Install IPsec SA
Yesterday	INFO	negotiate	success	progress IPsec phase 2
Yesterday	INFO	negotiate	success	progress IPsec phase 1
Yesterday	INFO	negotiate	success	progress IPsec phase 1
Yesterday	INFO	negotiate	success	progress IPsec phase 1
Yesterday	INFO	negotiate	success	progress IPsec phase 1
Yesterday	INFO	negotiate	failure	progress IPsec phase 1

Double-click any log to get more details

Phase 1 is DONE (up)

FortiGate logs IPsec VPN events by default. To view IPsec VPN event logs, click **Log & Report > System Events > VPN Events**.

The logs track the progress of phase 1 and phase 2 negotiations, and report on tunnel up and down events and DPD failures, among other events. For more information about IPsec logs, visit <https://docs.fortinet.com>.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. The IPsec monitor widget enables you to bring down the _____ of an IPsec VPN.
A. Phase 1
 B. Entire tunnel

2. When the remote gateway is set to dial-up user, a static route to the remote network is added to the routing table after _____.
A. Phase 1 comes up
 B. Phase 2 comes up

DO NOT REPRINT

© FORTINET

Lesson Progress



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe the benefits of IPsec VPN
- ✓ Understand how IPsec works
- ✓ Learn about the IPsec wizard
- ✓ Identify and understand the phases of IKEv1
- ✓ Understand phase 1 and phase 2 settings
- ✓ Understand redundant VPN configuration between two FortiGate devices
- ✓ Monitor IPsec VPNs and review logs



© Fortinet Inc. All Rights Reserved.

57

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

By mastering the objectives covered in this lesson, you learned how the IPsec protocol works, and how to configure and monitor IPsec VPNs on FortiGate.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

High Availability

FortiOS 7.2

Last Modified: 30 August 2022

In this lesson, you will learn about the fundamentals of FortiGate high availability (HA) and how to configure it. FortiGate HA provides a solution for enhanced reliability and increased performance.

DO NOT REPRINT

© FORTINET

Lesson Overview



HA Operation Modes



HA Cluster Synchronization



HA Failover and Workload



Monitoring and Troubleshooting

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

DO NOT REPRINT**© FORTINET**

HA Operation Modes

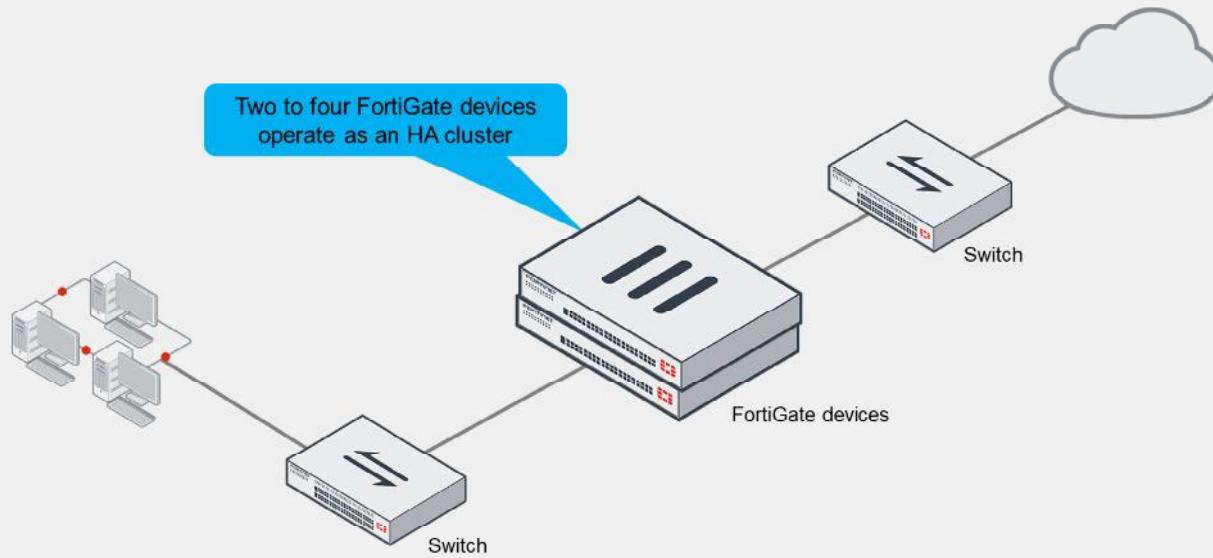
Objectives

- Identify the different operation modes for HA
- Understand the primary FortiGate election in an HA cluster

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

By demonstrating competence in HA operation modes and primary FortiGate election, you will be able to choose and implement the right HA operation mode in your network based on your requirements. You will be able to use FortiGate devices effectively in your network.

What Is FortiGate HA?



The idea of HA is simple. HA links and synchronizes two to four FortiGate devices to form a cluster for redundancy and performance purposes.

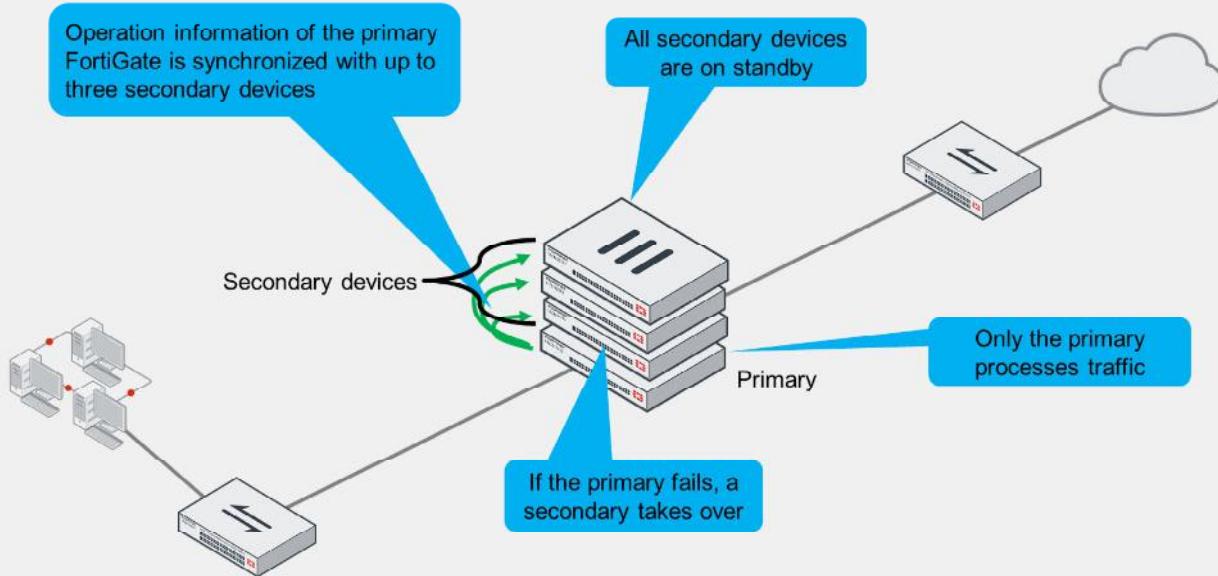
A cluster includes one device that acts as the primary FortiGate (also called the active FortiGate). The primary synchronizes its configuration, session information, FIB entries, FortiGuard definitions, and other operation-related information to the secondary devices, which are also known as standby devices.

The cluster shares one or more heartbeat interfaces among all devices—also known as members—for synchronizing data and monitoring the health of each member.

There are currently two HA operation modes available: active-active (A-A) and active-passive (A-P). Now, you will examine the differences.

DO NOT REPRINT**© FORTINET**

Active-Passive HA

**FORTINET**
Training Institute

© Fortinet Inc. All Rights Reserved.

5

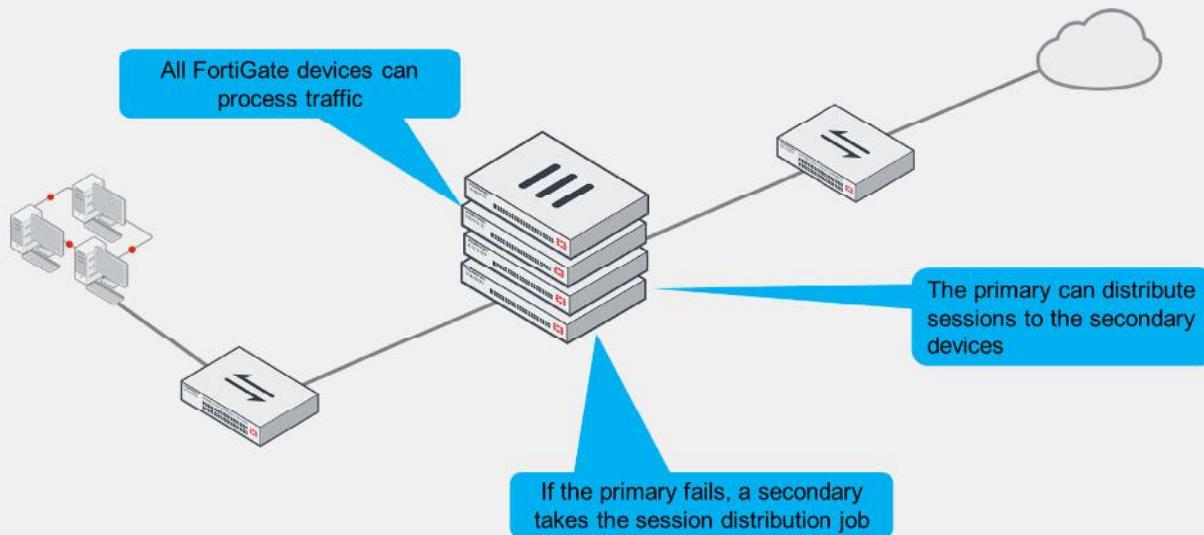
First, take a look at active-passive mode. In either of the two HA operation modes, the operation information (configuration, sessions, FIB entries, and so on) of the primary FortiGate is synchronized with secondary devices.

In active-passive mode, the primary FortiGate is the only FortiGate that actively processes traffic. Secondary FortiGate devices remain in passive mode, monitoring the status of the primary device.

If a problem is detected on the primary FortiGate, one of the secondary devices takes over the primary role. This event is called an *HA failover*.

DO NOT REPRINT**© FORTINET**

Active-Active HA

**FORTINET**
Training Institute

© Fortinet Inc. All Rights Reserved.

6

The other HA mode is active-active.

Like active-passive HA, in active-active HA, the operation-related data of the primary FortiGate is synchronized to the secondary FortiGate devices. Also, if a problem is detected on the primary device, one of the secondary devices takes over the role of the primary, to process the traffic.

However, one of the main differences from active-passive mode is that in active-active mode, all cluster members can process traffic. That is, based on the HA settings and traffic type, the primary FortiGate can distribute sessions to the secondary devices.

FortiGate Clustering Protocol

- Used for:
 - Member discovery
 - Primary election
 - Data synchronization
 - Member health monitoring
- Failover trigger events:
 - Dead member
 - Failed link
 - Failed remote link (link health monitoring)
 - High memory usage
 - Failed solid state disk (SSD)
 - Admin-triggered
- Ethernet types and ports:
 - Heartbeat:
 - Ethernet type 0x8890 (NAT mode)
 - Ethernet type 0x8891 (Transparent mode)
 - Data synchronization, logging, and CLI management:
 - Frame: Ethernet type 0x8893
 - Inner packet:
 - TCP/703 and UDP/703 (data sync)
 - TCP/700 (logging and alert emails)
 - TCP/22 (CLI management)
 - A-A load balancing (first packet only):
 - Frame: Ethernet type 0x8891
 - Inner packet: Original packet (MAC rewrite)

FortiGate HA uses the Fortinet-proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members.

To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces. If the cluster operates in NAT mode, the heartbeat frames are type 8890. In transparent mode, the heartbeat frames are type 8891. If the cluster operates in active-active mode, the first packet of a session distributed to the secondary is encapsulated in Ethernet frames type 8891.

The members also exchange frames type 8893 for data synchronization, local CLI management, and logging purposes. For data synchronization, the inner packet can be TCP port 703 or UDP port 703, depending on the type of data to synchronize. The primary also relays logs and alert emails from secondary devices over TCP port 700. For local HA management using the CLI, the inner packet is SSH.

You can configure the cluster to perform HA failover based on the following events:

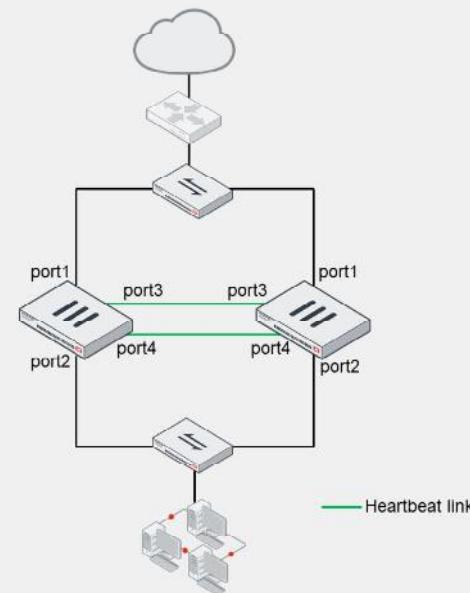
- Dead member: The primary FortiGate is unresponsive.
- Failed link: The link of one or more monitored interfaces on the primary FortiGate goes down.
- Failed remote link: FortiGate uses the link health monitor feature to monitor the health of one or more interfaces. The primary fails if the accumulated penalty of all failed interfaces reaches the set threshold.
- High memory usage: The primary fails if its memory utilization reaches the configured threshold.
- Failed SSD: FortiOS detects a failure in an SSD. Only available for devices with SSDs.
- Admin-triggered: The administrator issues a manual failover.

For any of the failover trigger events, the result is that the cluster promotes one of the secondary devices to the new primary FortiGate role.

DO NOT REPRINT**© FORTINET**

HA Requirements

- All members must have the same:
 - Firmware version
 - Model
 - Licensing
 - If different, the cluster uses the lowest-level license
 - Hard drive configuration
 - Operating mode (management VDOM)
- Setup:
 - Same HA group ID, group name, password, and heartbeat interface settings
 - Heartbeat interfaces can see each other
- Best practice:
 - Use at least two heartbeat interfaces (maximum 8)
 - Initially, switch DHCP and PPPoE interfaces to static configuration



To successfully form an HA cluster, you must ensure that the members have the same:

- Firmware version
- Model: the same hardware model or VM model
- Licensing: includes the FortiGuard license, VDOM license, FortiClient license, and so on
- Hard drive configuration: the same number and size of drives and partitions
- Operating mode: the operating mode—NAT mode or transparent mode—of the management VDOM

If the licensing level among members isn't the same, the cluster resolves to use the lowest licensing level among all members. For example, if you purchase FortiGuard Web Filtering for only one of the members in a cluster, none of the members will support FortiGuard Web Filtering when they form the cluster.

From a configuration and setup point of view, you must also make sure that:

- The HA settings on each member have the same group ID, group name, password, and heartbeat interface settings.
- The heartbeat interfaces on each member can see each other. This usually means placing all heartbeat interfaces in the same broadcast domain, or for two-member clusters, connecting them directly.

It's also a best practice to:

- Configure at least two heartbeat interfaces for redundancy purposes. This way, if one heartbeat link fails, the cluster uses the next one, as indicated by the priority and position in the heartbeat interface list.
- If using DHCP or PPPoE interfaces, use static configuration during the cluster initial setup to prevent incorrect address assignment. After the cluster is formed, you can put back the original interface settings.

DO NOT REPRINT

© FORTINET

Primary FortiGate Election—Override Disabled

- Override disabled (default)
- Force a failover

```
# diagnose sys ha reset-uptime
```

- Check the HA uptime difference:

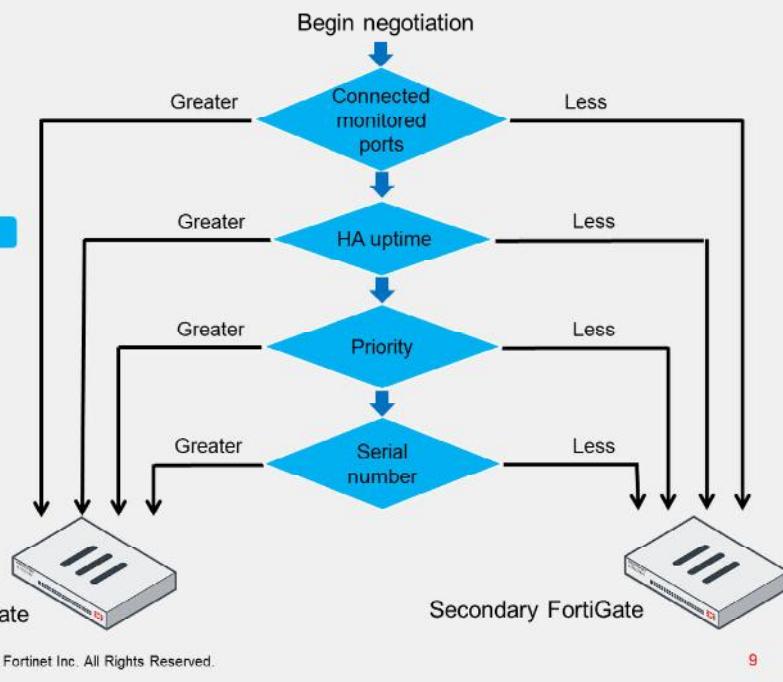
Difference measured in seconds

```
# diagnose sys ha dump-by vcluster
...
FGVMxxxx92:...uptime/reset_cnt=7814/0
FGVMxxxx36:...uptime/reset_cnt=0/1
```

0 is for the device with the lowest HA uptime

Number of times HA uptime has been reset for this device

FORTINET
Training Institute



© Fortinet Inc. All Rights Reserved.

9

This slide shows the different criteria that a cluster considers during the primary FortiGate election process. The criteria order evaluation depends on the HA override setting. This slide shows the order when the HA override setting is disabled, which is the default behavior. Note that the election process stops at the first matching criteria that successfully selects a primary FortiGate in a cluster.

1. The cluster compares the number of monitored interfaces that have a status of up. The member with the most available monitored interfaces becomes the primary.
2. The cluster compares the HA uptime of each member. The member with the highest HA uptime, by at least five minutes, becomes the primary.
3. The member with the highest priority becomes the primary.
4. The member with the lowest serial number becomes the primary.

When HA override is disabled, the HA uptime has precedence over the priority setting. This means that if you must manually fail over to a secondary device, you can do so by reducing HA uptime of the primary FortiGate. You can do this by running the `diagnose sys ha reset-uptime` command on the primary FortiGate, which resets its HA uptime to 0.

Note that the `diagnose sys ha reset-uptime` command resets the HA uptime and not the system uptime. Also, note that if a monitoring interface fails, or a member reboots, the HA uptime for that member is reset to 0.

This slide also shows how to identify the HA uptime difference between members. The member with 0 in the `uptime` column indicates the device with the lowest uptime. The example shows that the device with the serial number ending in 92 has an HA uptime that is 7814 seconds higher than the other device in the HA cluster. The `reset_cnt` column indicates the number of times the HA uptime has been reset for that device.

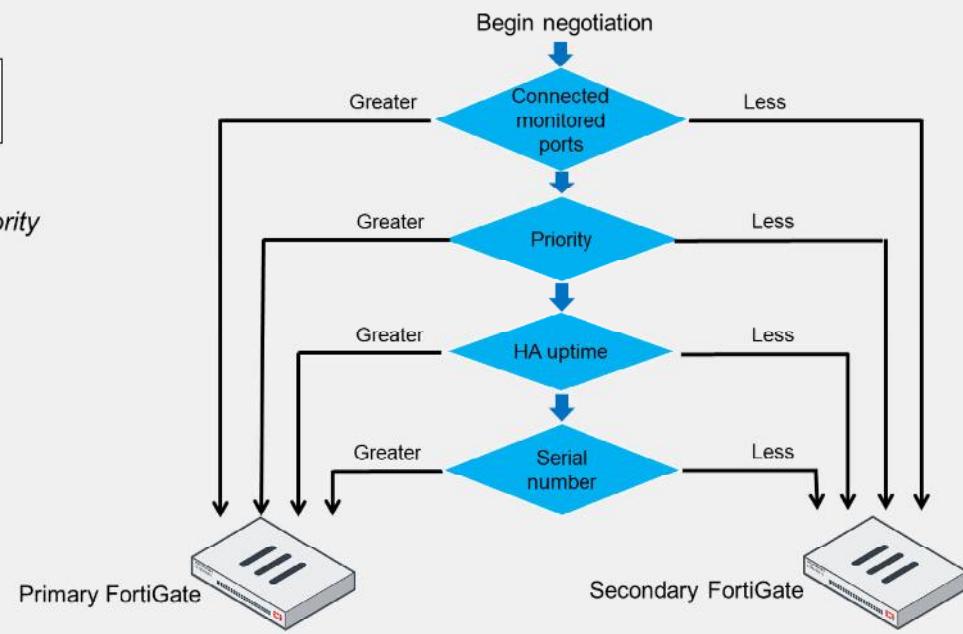
DO NOT REPRINT
© FORTINET

Primary FortiGate Election—Override Enabled

- Override enabled

```
config system ha
  set override enable
end
```

- Force a failover
 - Change the HA priority



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

10

If the HA override setting is enabled, the priority is considered before the HA uptime.

The advantage of this method is that you can specify which device is the preferred primary every time (as long as it is up and running) by configuring it with the highest HA priority value. The disadvantage is that a failover event is triggered not only when the primary fails, but also when the primary is available again. That is, when the primary becomes available again, it takes its primary role back from the secondary FortiGate that temporarily replaced it.

When override is enabled, the easiest way of triggering a failover is to change the HA priorities. For example, you can either increase the priority of one of the secondary devices, or decrease the priority of the primary.

The override setting and device priority values are not synchronized to cluster members. That is, on each member, you must manually enable override and adjust the priority.

DO NOT REPRINT**© FORTINET**

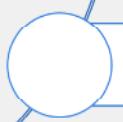
Knowledge Check

1. What is a requirement for members to form an HA cluster?
 - A. They must have same host name
 - B. They must run the same firmware version

2. What is the default order criteria (override disabled) for selecting the primary in an HA cluster?
 - A. Connected monitored ports > HA uptime > priority > serial number
 - B. Priority > HA uptime > connected monitored ports > serial number

DO NOT REPRINT**© FORTINET**

Lesson Progress

**HA Operation Modes****HA Cluster Synchronization****HA Failover and Workload****Monitoring and Troubleshooting**

Good job! You now understand HA operation modes and the election of the primary FortiGate in an HA cluster.

Now, you will learn about HA cluster synchronization.

DO NOT REPRINT**© FORTINET**

HA Cluster Synchronization

Objectives

- Identify the primary and secondary device tasks in an HA cluster
- Identify what is synchronized between HA cluster members
- Configure session synchronization for seamless failover

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

By demonstrating competence in cluster synchronization, you will be able to identify the tasks assigned to members based on their roles, as well as what information is synchronized between members. You will also learn how to configure session synchronization to perform session failover to specific types of traffic.

DO NOT REPRINT**© FORTINET**

Primary FortiGate Tasks

- Broadcasts hello packets for member discovery and monitoring
- Synchronizes operation-related data such as:
 - Configuration (some settings are not synchronized)
 - FIB entries
 - DHCP leases
 - ARP table
 - FortiGuard definitions
 - IPsec tunnel SAs
 - Sessions (must be enabled)
- In active-active mode only:
 - Distributes sessions to secondary members



© Fortinet Inc. All Rights Reserved.

14

So, what are the tasks of a primary FortiGate?

It monitors the cluster by broadcasting hello packets and listening for hello packets from other members in the cluster. The members use the hello packets to identify if other FortiGate devices are alive and available.

The primary FortiGate also synchronizes its operation-related data to the secondary members. Some of the data synchronized includes its configuration, FIB entries, DHCP leases, ARP table, FortiGuard definitions, and IPsec tunnel security associations (SAs). Note that some parts of the configuration are not synchronized because they are device-specific. For example, the host name, HA priority, and HA override settings are not synchronized.

Optionally, you can configure the primary FortiGate to synchronize qualifying sessions to all the secondary devices. When you enable session synchronization, the new primary can resume communication for sessions after a failover event. The goal is for existing sessions to continue flowing through the new primary FortiGate with minimal or no interruption. You will learn which types of sessions you can enable synchronization for later in the lesson.

In active-active mode only, a primary FortiGate is also responsible for distributing sessions to secondary members.

DO NOT REPRINT**© FORTINET**

Secondary FortiGate Tasks

- Broadcasts hello packets for member discovery and monitoring
- Synchronizes data from the primary
- Monitors the health of the primary
 - If the primary fails, the secondary devices elect a new primary
- In active-active mode only:
 - Processes traffic distributed by the primary

Now, take a look at the tasks of secondary FortiGate devices.

Like the primary, secondary members also broadcast hello packets for discovery and monitoring purposes.

In addition, in active-passive mode, the secondary devices act as a standby device, receiving synchronization data but not actually processing any traffic. If the primary FortiGate fails, the secondary devices elect a new primary.

In active-active mode, the secondary devices don't wait passively. They process all traffic assigned to them by the primary device.

DO NOT REPRINT**© FORTINET**

Heartbeat Interface IP Addresses

- The cluster assigns addresses to heartbeat interfaces based on the serial number of each member
 - 169.254.0.1: for the highest serial number
 - 169.254.0.2: for the second highest serial number
 - 169.254.0.3: for the third highest serial number (and so on)
- Members keep their heartbeat IP addresses regardless of any change in their role (primary or secondary)
 - The IP address assignment may change only when a member leaves or joins the cluster
- The cluster uses the heartbeat IP addresses to:
 - Distinguish the members
 - Synchronize data with members

FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number. The IP address 169.254.0.2 is assigned to the device with the second highest serial number, and so on. The IP address assignment does not change when a failover happens. Regardless of the device role at any time (primary or secondary), its heartbeat IP address remains the same.

A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster. In those cases, the cluster renegotiates the heartbeat IP address assignment, this time taking into account the serial number of any new device, or removing the serial number of any device that left the cluster.

The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data.

DO NOT REPRINT**© FORTINET**

Heartbeat and Monitored Interfaces

- Heartbeat interfaces exchange sensitive data and may use a fair amount of bandwidth
 - If using a switch, use a dedicated switch or dedicated VLAN
 - Configure at least one heartbeat interface
 - It's a best practice to configure at least two for redundancy
 - Must be a physical port
- Monitored interfaces
 - Required for link failover
 - Choose interfaces that are critical for user traffic
 - Physical, redundant, and LAG interfaces are supported
 - Don't monitor heartbeat interfaces
 - Configure link failover after the cluster is formed
 - Prevents unwanted failover events during initial setup

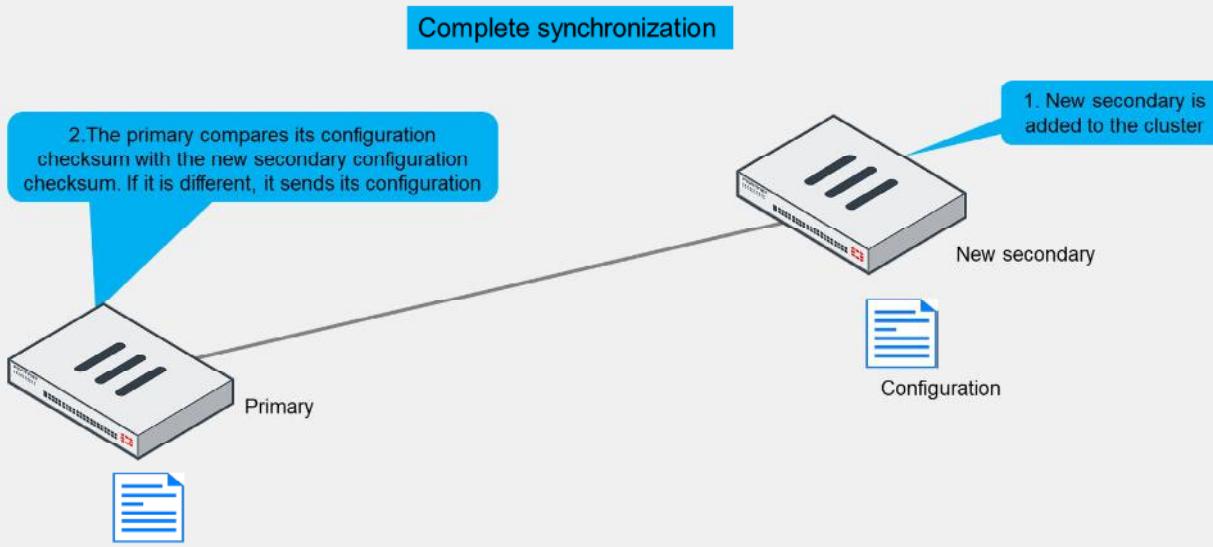
Heartbeat interfaces exchange sensitive information about the cluster operation and may require a fair amount of bandwidth for data synchronization. For this reason, if you use a switch to connect the heartbeat interfaces, it's recommended that you use a dedicated switch or, at least, that you place the heartbeat traffic on a dedicated VLAN.

In addition, you must configure at least one port as a heartbeat interface, but preferably two for redundancy. For heartbeat interfaces, you can use physical interfaces only. That is, you can't use VLAN, IPsec VPN, redundant, or 802.3ad aggregate interfaces. You cannot use FortiGate switch ports either.

For link failover to work, you must configure one or more monitored interfaces. A monitored interface should be an interface whose failure has a critical impact in the network, and therefore, should trigger a device failover. For example, your LAN or WAN interfaces are usually good choices for monitored interfaces. Heartbeat interfaces, however, should not be configured as monitored interfaces because they are not meant to handle user traffic. Note that you can monitor physical ports, redundant interfaces, and link aggregation group (LAG) interfaces.

As a best practice, wait until a cluster is up and running and all interfaces are connected before configuring link failover. This is because a monitored interface can be disconnected during the initial setup and, as a result, trigger a failover before the cluster is fully configured and tested.

HA Complete Configuration Synchronization



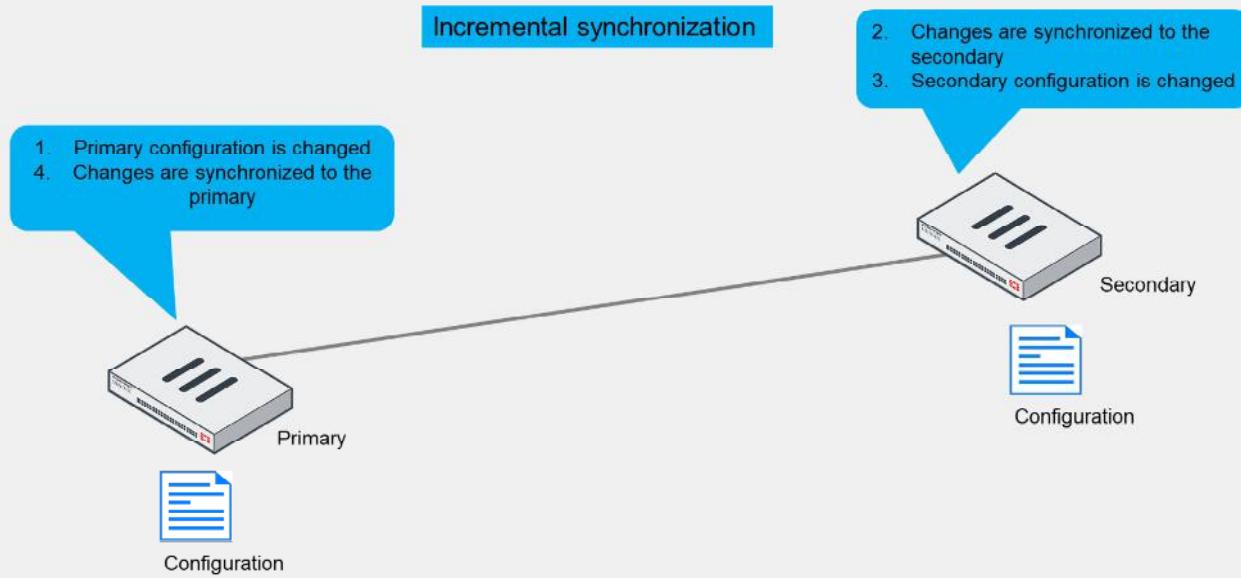
To prepare for a failover, an HA cluster keeps its configurations in sync. You will explore that now.

FortiGate HA uses a combination of both incremental and complete synchronizations.

When you add a new FortiGate to the cluster, the primary FortiGate compares its configuration checksum with the new secondary FortiGate configuration checksum. If the checksums don't match, the primary FortiGate uploads its complete configuration to the secondary FortiGate.

DO NOT REPRINT
© FORTINET

HA Incremental Configuration Synchronization



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

After the initial synchronization is complete, whenever a change is made to an HA cluster device's (primary or secondary) configuration, incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link. An HA synchronization process running on each cluster device receives the configuration change and applies it to the cluster device. For example, if you create a firewall address object, the primary doesn't resend its complete configuration—it sends only the new object.

Another example is in an HA setup with multiple VDOMs and virtual clustering, where the secondary device is acting as the primary FortiGate for VDOM2. Any changes made on VDOM2 are synchronized with the primary FortiGate.

DO NOT REPRINT**© FORTINET**

HA Configuration Synchronization

- Incremental synchronization also includes:
 - Dynamic data such as DHCP leases, FIB entries, IPsec SAs, session information, and so on
- Periodically, HA checks for synchronization
 - If the checksums match, the cluster is in sync
 - If the checksums don't match after five attempts, the secondary downloads the whole configuration from the primary

HA propagates more than just configuration details. Some runtime data, such as DHCP leases and FIB entries, are also synchronized.

By default, the cluster checks every 60 seconds to ensure that all devices are synchronized. If a secondary device is out of sync, its checksum is checked every 15 seconds. If the checksum of the out-of-sync secondary device doesn't match for five consecutive checks, a complete resynchronization to that secondary device is done.

DO NOT REPRINT**© FORTINET**

What Is Not Synchronized?

- These configuration settings are *not* synchronized between cluster members:
 - HA management interface settings
 - HA default route for the reserved management interface
 - In-band HA management interface
 - HA override
 - HA device priority
 - HA virtual cluster priority
 - FortiGate host name
 - Ping server HA priorities
 - The HA priority (ha-priority) setting for a ping server or dead gateway detection configuration
 - Licenses*
 - FortiGuard, FortiCloud activation, and FortiClient licensing
 - Cache
 - FortiGuard Web Filtering and email filter, web cache, and so on
- The primary FortiGate synchronizes all other configuration settings

Note:

* FortiToken licenses (serial numbers) are synchronized

Not all the configuration settings are synchronized. There are a few that are not, such as:

- System interface settings of the HA reserved management interface and the HA default route for the reserved management interface
- In-band HA management interface
- HA override
- HA device priority
- Virtual cluster priority
- FortiGate host name
- HA priority setting for a ping server (or dead gateway detection) configuration
- All licenses except FortiToken licenses (serial numbers)
- Cache

The primary FortiGate synchronizes all other configuration settings, including all other HA settings.

DO NOT REPRINT

© FORTINET

Session Synchronization

- Provides seamless failover
 - Network applications don't need to restart connections
 - Minimum or no impact
- Firewall sessions
 - TCP sessions are synced by default
 - Unless they are subject to proxy inspection
 - Optionally, sync UDP and ICMP sessions
 - Usually not required
 - Multicast sessions are not synced
 - Multicast routes are
 - SIP sessions inspected by SIP ALG
- Local sessions
 - Not synced, must be restarted

- Configure session synchronization on the CLI:

```
config system ha
  set session-pickup enable
  set session-pickup-connectionless enable
  set multicast-ttl <5 - 3600 sec>
end
```

The time multicast routes remain in multicast forwarding table after failover (recommended = 120 seconds; default = 600 seconds)

Enable UDP and ICMP session synchronization

Enable non-proxy TCP session sync synchronization

Session synchronization provides seamless session failover. When the primary fails, the new primary can resume traffic for synchronized sessions without network applications having to restart the connections.

By default, the feature synchronizes TCP firewall sessions that are not subject to proxy-based inspection. An exception to this rule is TCP SIP sessions inspected by SIP ALG. Even though SIP ALG performs proxy-based inspection on SIP sessions, FortiGate can still synchronize such SIP sessions. Firewall sessions, also known as pass-through sessions, are user traffic sessions that travel across FortiGate. TCP firewall sessions that are subject to flow-based inspection or no inspection at all, are synchronized to secondary members.

You can also enable the synchronization of UDP and ICMP sessions. Although both protocols are connectionless protocols, FortiGate still allocates sessions for UDP and ICMP connections in its session table. Usually, the synchronization of UDP and ICMP sessions is not required because most UDP and ICMP connections can resume communication if their session information is lost.

For multicast traffic, FortiGate synchronizes multicast routes only. That is, FortiGate doesn't synchronize multicast sessions, which should be fine because multicast sessions are mostly UDP-based and, as mentioned before, UDP sessions can usually resume communication if their session information is lost. To ensure the multicast routing information across members is accurate, you can adjust the multicast time to live (TTL) timer. The timer controls how long the new primary keeps the synced multicast routes in the multicast forwarding table. The smaller the timer value, the more often the routes are refreshed, and so the more accurate the multicast forwarding table is. The recommended timer value is 120 seconds.

Local-in and local-out sessions, which are sessions that are terminated at or initiated by FortiGate, respectively, are not synchronized either. For example, BGP peerings, OSPF adjacencies, as well as SSH and HTTPS management connections must be restarted after a failover.

DO NOT REPRINT**© FORTINET**

IPsec and SSL VPN Synchronization

- FortiGate automatically synchronizes data for:
 - IPsec
 - IKE and IPsec SAs
 - Tunnels continue to be up after failover
 - Sessions over IPsec require you to enable session synchronization for session failover
 - SSL VPN web mode
 - Authentication information
 - Web mode users don't have to reauthenticate after failover
 - They must still restart connections over SSL VPN
- FortiGate doesn't synchronize data for SSL VPN tunnel mode users
 - Tunnel mode users must restart the SSL VPN tunnel after failover



© Fortinet Inc. All Rights Reserved.

23

The primary FortiGate automatically synchronizes all IKE and IPsec security associations (SAs) to secondary members. This enables the new primary to resume existing IPsec tunnels after a failover. Note that you must also enable session synchronization if you want the new primary to also resume existing IPsec sessions. Otherwise, after a failover, you must still restart existing TCP connections made over IPsec tunnels, even though the IPsec tunnels continue to be up on the new primary.

For SSL VPN, the primary FortiGate synchronizes the authentication information for SSL VPN web mode users only. That is, they are using SSL VPN web mode, the SSL VPN users don't have to authenticate again after a failover. However, the users must still restart the connections made using SSL VPN web mode to regain access to protected resources. Note that FortiGate doesn't synchronize any information for SSL VPN tunnel mode. That is, after a failover, SSL VPN tunnel mode users must restart their SSL VPN tunnel connection, as well as any connection made through the tunnel.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which information is synchronized in an HA cluster?
 A. Firewall policies and objects
 B. FortiGate host name

2. Which one of the following session types can be synchronized in an HA cluster?
 A. BGP peerings
 B. Non-proxy TCP sessions

DO NOT REPRINT**© FORTINET**

Lesson Progress

**HA Operation Modes****HA Cluster Synchronization****HA Failover and Workload****Monitoring and Troubleshooting**

Good job! You now understand HA cluster synchronization.

Now, you will learn about HA cluster failover protection types and workload for primary and secondary FortiGate devices in an HA cluster.

DO NOT REPRINT**© FORTINET**

HA Failover and Workload

Objectives

- Identify the HA failover types
- Interpret how an HA cluster in active-active mode distributes traffic
- Implement virtual clustering per VDOM in an HA cluster

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

By demonstrating competence in failover types and workload, you will be able to identify how enhanced reliability is achieved through HA failover protection. You will also learn about the distribution of traffic in an active-active cluster and distributing traffic using virtual clustering.

DO NOT REPRINT

© FORTINET

Failover Protection

- Types:
 - Device failover
 - The secondary devices stop receiving hello packets from the primary
 - Link failover
 - The link of one or more monitored interfaces goes down
 - Remote link failover
 - One or more interfaces are monitored using the link health monitor
 - The primary fails if the accumulated penalty of all failed interfaces reaches the configured threshold
 - Memory-based failover
 - Memory utilization on the primary exceeds the configured threshold and monitoring period
 - SSD failover
 - FortiOS detects extended filesystem (Ext-fs) errors in an SSD
 - Only available for devices with SSDs
- Identify failover protection type by looking at:
 - Event logs, SNMP traps, and alert email record failover events
- Enable session synchronization for seamless session failover



© Fortinet Inc. All Rights Reserved.

27

The most common types of failovers are device failovers and link failovers. However, you can also configure remote link failover and memory-based failover. When a failover event is triggered, the secondary devices elect a new primary.

A device failover is triggered when the secondary devices stop receiving the heartbeat hello packets from the primary.

A link failover occurs when the link status of a monitored interface on the primary FortiGate goes down. You can configure an HA cluster to monitor one or more interfaces. If a monitored interface on the primary FortiGate is unplugged, or its link status goes down, a new primary FortiGate is elected.

When you configure remote link failover, FortiGate uses the link health monitor feature to monitor the health of one or more interfaces against one or more servers that act as beacons. The primary FortiGate fails if the accumulated penalty of all failed interfaces reaches the configured threshold.

If you enable memory-based failover, an HA failover is triggered when the memory utilization on the primary FortiGate reaches the configured threshold for the configured monitoring period. You can also enable SSD failover, which triggers a failover if FortiOS detects Ext-fs errors on an SSD on the primary FortiGate.

There are multiple events that might trigger an HA failover, such as a hardware or software failure on the primary FortiGate or an issue on one of the interfaces on the primary. When a failover occurs, an event log is generated. Optionally, you can configure the device to also generate SNMP traps and alert emails.

Make sure that you enable session pickup for sessions you want to protect from a failover event. This way, the new primary can resume traffic for these sessions.

Failover Protection Configuration

- Device failover
 - Always enabled
 - Adjust the failover time:

```
config system ha
  set hb-interval <1 - 20>
  set hb-interval-in-milliseconds 100ms | 10ms
  set hb-lost-threshold <1 - 60>
end
```

Number of failed heartbeats before device is dead
 Heartbeat interval
 Number of heartbeat interval units

- Default values vary by model
 - FortiGate 2000E:
 - hb-interval: 2
 - hb-interval-in-milliseconds: 100ms
 - hb-lost-threshold: 6
 - Total failover time = $2 \times 100 \text{ ms} \times 6 = 1200 \text{ ms}$

- Link failover

- Configure one or more monitored interfaces:

```
config system ha
  set monitor <interface1> <interface2> ...
end
```

- Supported interfaces:

- Physical
- Redundant
- LAG

When you configure HA, device failover is always enabled. However, you can adjust the settings that dictate the failover time. To speed up failover, you can reduce the values for all three settings shown on this slide. To reduce false positives, increase their values.

The default values for the three settings vary by model. For example, using the default values on a FortiGate 2000E model results in a device failover time of 1200 milliseconds (1.2 seconds). Note that the 10-millisecond heartbeat interval is supported on NP6 platforms only.

To configure link failover, you must configure one or more monitored interfaces, as shown on this slide. Note that you can configure only physical, redundant, and LAG interfaces as monitored interfaces.

Failover Protection Configuration (Contd)

- Remote link failover

- Configure link health monitor:

```
config system link-monitor
  edit "port1-ha"
    set srcintf "port1"
    set server "4.2.2.1" "4.2.2.2"
    set ha-priority 10
  next
end
```

Dead link nominal penalty—not synchronized

- Configure HA settings:

```
config system ha
  set pingserver-monitor-interface port1
  set pingserver-failover-threshold 5
  set pingserver-secondary-force-reset enable
  set pingserver-flip-timeout 30
end
```

Perform remote link failover on port1

Elect a new primary if the accumulated penalty reaches this threshold (5)

Elect a new primary again at the end of the flip timeout

The next primary election is in 30 minutes

This slide shows a configuration example for remote link failover.

First, you configure link health monitor, as shown in the *Routing* lesson. The `ha-priority` setting in the link health monitor configuration defines the penalty applied to the member after the link is detected as dead. Note that the `ha-priority` setting has local significance only, and therefore, is not synchronized to other members.

The next step is to configure the HA settings related to remote link failover. The configuration on this slide instructs FortiGate to perform remote link failover on port1 as follows:

- When port1 is detected as dead, the nominal penalty (10) is added to the global penalty, which is initially set to 0.
- If the accumulated penalty reaches the penalty threshold (5), then the cluster elects a new primary. A failover occurs when a secondary member has a lower accumulated penalty than the primary. If so, the secondary member with the lowest accumulated penalty becomes the new primary.
- The cluster doesn't elect a new primary again until the flip timeout (30 minutes) has passed.

If during the primary election, the accumulated penalty of all members is the same, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect the new primary.

Failover Protection Configuration (Contd)

- Memory-based failover

- Configure HA settings:

```
config system ha
  set memory-based-failover enable
  set memory-failover-threshold 70
  set memory-failover-monitor-period 30
  set memory-failover-sample-rate 2
  set memory-failover-flip-timeout 20
end
```

Enable memory-based failover

The memory usage threshold is 70%

Elect a new primary when the memory usage exceeds 70% for 30 seconds

Check memory usage every 2 seconds

The next primary election is in 20 minutes

The HA configuration shown on this slide instructs FortiGate to perform memory-based failover as follows:

- When the memory on the primary reaches the threshold (70%) and stays like that for 30 seconds, then the cluster elects a new primary.
- During primary election, a failover occurs when the memory usage on a secondary member is lower than the configured memory threshold (70%). If so, the secondary member becomes the new primary.
- The cluster doesn't elect a new primary again until the flip timeout (20 minutes) has passed.
- Each member in the cluster checks its memory usage every 2 seconds.

If during the primary election, the memory usage of all members are below or above the threshold, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect the new primary.

DO NOT REPRINT**© FORTINET**

Failover Protection Configuration (Contd)

- SSD failover

- Configure HA settings:

```
config system ha
  set ssd-failover enable
end
```

Enable memory-based failover



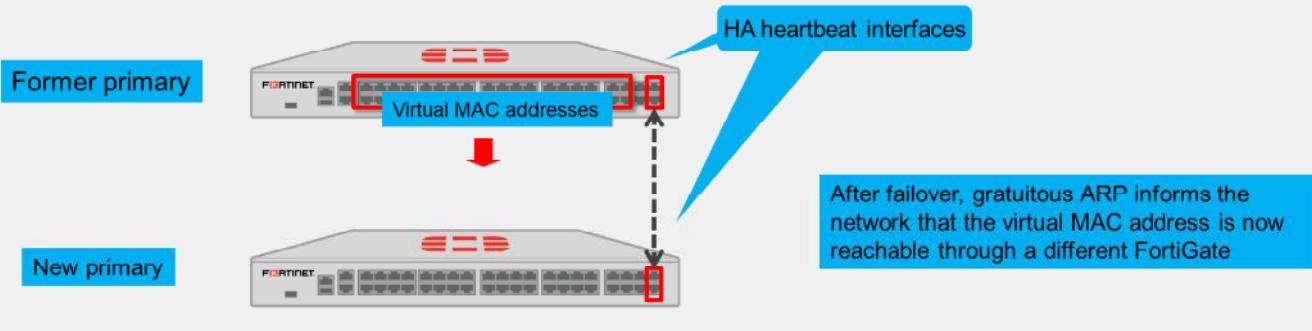
© Fortinet Inc. All Rights Reserved.

31

The HA configuration shown on this slide instructs FortiGate to perform a failover when any of the SSD disks on the primary FortiGate report Ext-fs errors. Note that this feature is supported only on FortiGate models with SSD disks.

Virtual MAC Addresses and Failover

- On the primary, each interface is assigned a virtual MAC address
 - HA heartbeat interfaces are not assigned a virtual MAC address
- Upon failover, the newly elected primary adopts the same virtual MAC addresses as the former primary



To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses. When a primary joins an HA cluster, each interface is assigned a virtual MAC address. The HA group ID is used in the creation of virtual MAC addresses assigned to each interface. So, if you have two or more HA clusters in the same broadcast domain, and using the same HA group ID, you might get MAC address conflicts. For those cases, it is strongly recommended that you assign different HA group IDs to each cluster.

Through the heartbeats, the primary informs all secondary devices about the assigned virtual MAC address. Upon failover, a secondary adopts the same virtual MAC addresses for the equivalent interfaces.

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

Note that the MAC address of a reserved HA management interface is not changed to a virtual MAC address. Instead, the reserved management interface keeps its original MAC address.

DO NOT REPRINT**© FORTINET**

Failure of a Secondary FortiGate

- Active-passive HA cluster
 - The primary updates the list of available secondary FortiGate devices
- Active-active HA cluster
 - The primary updates the list of available secondary FortiGate devices and redistributes sessions to prevent failed secondary devices

As you learned earlier in this lesson, if a primary fails, a new primary is elected. But what happens if a secondary FortiGate device fails? It depends on the HA mode.

In an active-passive cluster, the primary only updates its list of available secondary FortiGate devices. It also starts monitoring for the failed secondary, waiting for it to come online again.

However, in an active-active cluster, the secondary devices can handle traffic. So, the primary (which tracks and assigns sessions to each secondary) must not only update its list of available secondary FortiGate devices, but also reassign sessions from the failed FortiGate to a different secondary FortiGate.

DO NOT REPRINT**© FORTINET**

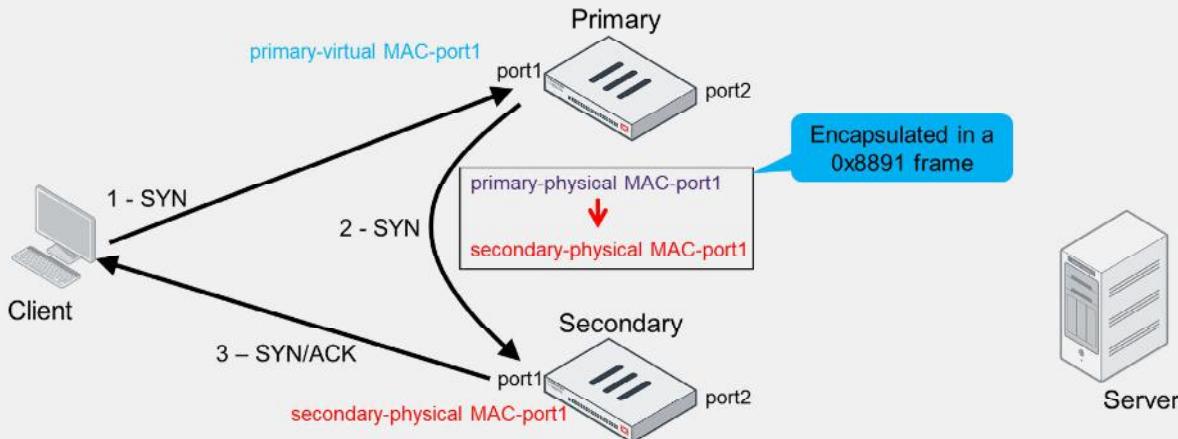
Workload

- Active-passive HA cluster
 - The primary receives and processes all traffic
 - The secondary waits passively
- Active-active HA cluster
 - The primary receives all traffic and redirects some proxy-based sessions to secondary devices
 - Enable `load-balance-all` to force distribution of all sessions

This is how the workload is distributed between roles, depending on the HA mode.

Notice that traffic workload is distributed in active-active mode only. However, keep in mind that by default, only sessions that are subject to proxy inspection are distributed to secondary devices. If you want to force the distribution of sessions that are subject to flow inspection or no inspection at all, then you must enable the `load-balance-all` setting under HA configuration—this setting is disabled by default.

Active-Active Traffic Flow (Proxy Inspection)



1. srcMAC client, dstMAC **primary-virtual MAC-port1**, TCP SYN dport 80
2. srcMAC primary-physical MAC-port1, dstMAC **secondary-physical MAC-port1**, TCP SYN dport 80 (Ethernet frame 0x8891)
3. srcMAC **secondary-physical MAC-port1**, dstMAC client, TCP SYN/ACK sport 80

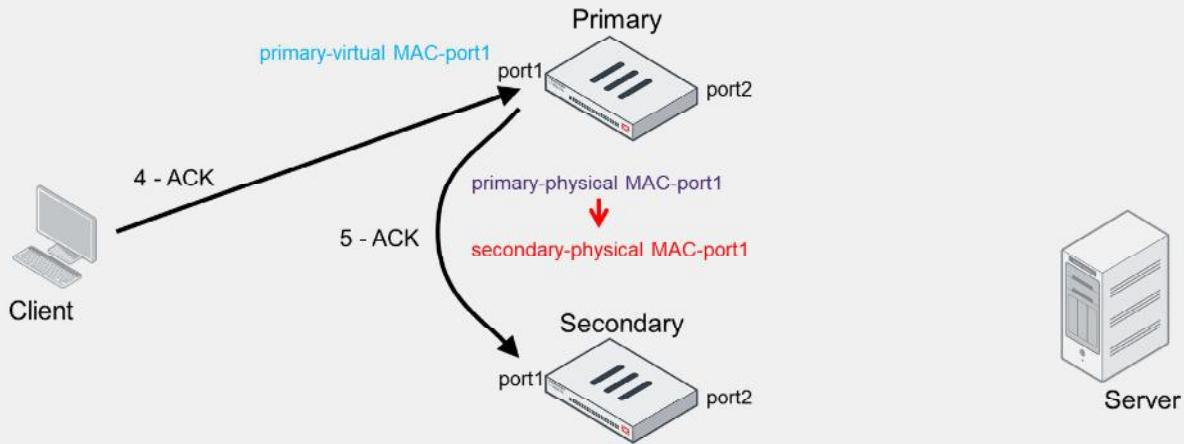
In active-active mode, the following occurs:

- The traffic destined to the cluster is sent to the primary. Because all network ports on the primary—except the heartbeat ports—are assigned a virtual MAC address, the traffic is destined to the virtual MAC address of the receiving port on the primary FortiGate.
- For traffic that is distributed to the secondary, the traffic destined to the endpoints is sent by the secondary. The traffic is sourced from the physical MAC address of the egressing port on the secondary.

This slide shows the flow for distributed traffic that is subject to proxy inspection:

1. The client sends a SYN packet, which is forwarded to port1 on the primary. The packet destination MAC address is the virtual MAC address on port1.
2. The primary forwards the SYN packet to the selected secondary. In this example, the source MAC address of the packet is changed to the physical MAC address of port1 on the primary and the destination MAC address to the physical MAC address of port1 on the secondary. This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic.
3. The secondary responds to the client with a SYN/ACK packet that contains the physical MAC address of port1 on the secondary as the source and the MAC address of the client as the destination.

Active-Active Traffic Flow (Proxy Inspection) (Contd)

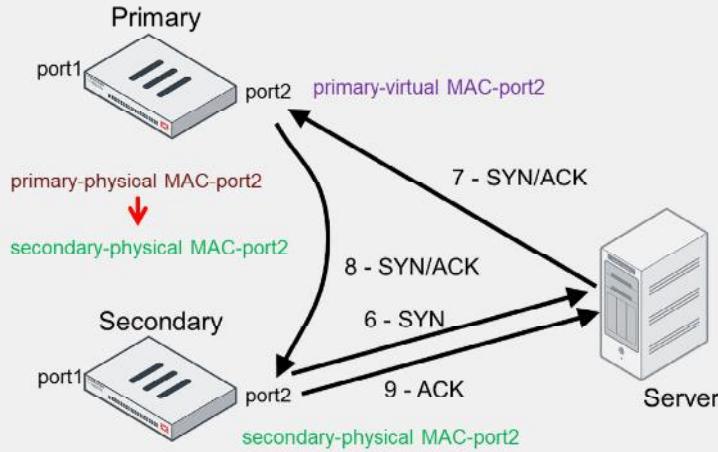


- 4. srcMAC client, dstMAC **primary-virtual MAC-port1**, TCP ACK dport 80
- 5. srcMAC **primary-physical MAC-port1**, dstMAC **secondary-physical MAC-port1**, TCP ACK dport 80

4. The client acknowledges the SYN/ACK by sending an ACK to the cluster. The ACK packet is destined to port1 on the primary.
5. The primary receives the packet and knows that it matches a session that was previously distributed to the secondary. As a result, the primary forwards the ACK packet to the corresponding secondary FortiGate. The packet is sourced from the physical MAC address of port1 on the primary and destined to the physical MAC address of port1 on the secondary. The three-way handshake on the client side is complete.

DO NOT REPRINT
© FORTINET

Active-Active Traffic Flow (Proxy Inspection) (Contd)



- 6. srcMAC **secondary physical MAC-port2**, dstMAC server, TCP SYN dport 80
- 7. srcMAC server, dstMAC **primary-virtual MAC-port2**, TCP SYN/ACK sport 80
- 8. srcMAC **primary-physical MAC-port2**, dstMAC **secondary-physical MAC-port2**, TCP SYN/ACK sport 80
- 9. srcMAC **secondary-physical MAC-port2**, dstMAC server, TCP ACK dport 80

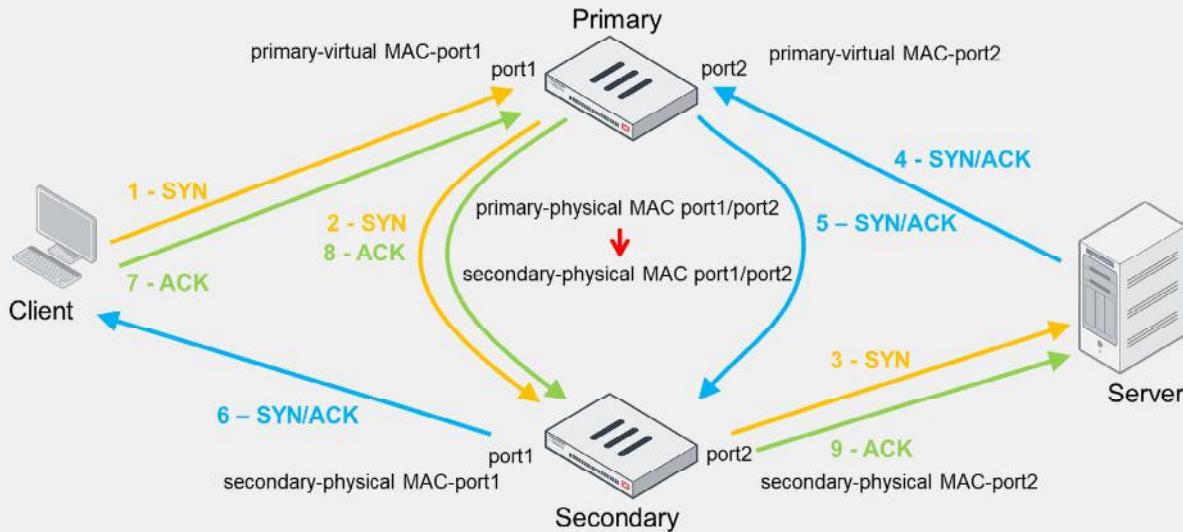
6. The secondary starts the connection with the server by sending a SYN packet using the physical MAC address of port2 as the source. Note that FortiGate contacts the server after it finishes the three-way handshake to the client, not before. The same behavior is seen when FortiGate operates in standalone mode and performs proxy-based inspection.
7. The SYN/ACK packet from the server is sent to port2 on the primary. The destination MAC address is the virtual MAC address of port2.
8. The primary receives the packet and knows that it matches a session that was previously distributed to the secondary. The primary forwards the SYN/ACK packet to the corresponding secondary FortiGate. The packet is sourced from the physical MAC address of port2 on the primary and destined to the physical MAC address of port2 on the secondary.
9. The secondary responds to the server with an ACK packet that contains the physical MAC address of port2 on the secondary as the source and the MAC address of the server as the destination.

The three-way handshake on the server side is also complete. From now on, packets that the client sends follow the same flow. For example, an HTTP GET request packet from the client is first received by the primary, which then forwards it to the secondary for proxy-based inspection. If the packet is allowed, the secondary forwards the packet to the server. Any server response packets to the client HTTP GET request are sent to the primary, which then forwards the packets to the secondary for inspection, and so on.

Note that the goal of active-active mode is to leverage unused CPU and memory resources on secondary devices. The intention is not really to load balance traffic. In fact, because the traffic from endpoints is always sent to the primary, you usually see more traffic on the primary than any secondary devices.

DO NOT REPRINT
© FORTINET

Active-Active Traffic Flow (No Proxy Inspection)



When there is no proxy inspection, that is, when traffic is either subject to flow inspection or no inspection at all, sessions are distributed to the secondary FortiGate only if you enable the `load-balance-all` setting (which is disabled by default) under HA configuration. In addition, as in proxy inspection, you will also see the following behavior:

- Traffic sourced from the client or server and destined to the FortiGate cluster is sent to the primary FortiGate. The source and destination MAC addresses are the endpoint (client or server) and the primary FortiGate virtual MAC address, respectively.
- The primary FortiGate may, in turn, forward the traffic to the secondary if the session is to be load balanced.
- When distributing the traffic to the secondary, FortiGate uses the physical MAC addresses of the primary and secondary devices interfaces as the source and destination MAC addresses, respectively.
- If traffic is load balanced to the secondary FortiGate, any traffic sourced from the cluster and destined to the endpoint is sourced from the secondary FortiGate. This means that the source MAC address is the physical address of the secondary egress interface.

When compared to proxy inspection, the difference is that FortiGate does not reply to packets on behalf of the client or server. For example, instead of replying to the SYN packet that the client sends, FortiGate forwards the packet to the server through the secondary. Similarly, FortiGate forwards packets that the server sends to the client through the secondary.

DO NOT REPRINT

© FORTINET

Unsupported Sessions for Active-Active Load Balancing

- Sessions that can't be load balanced
 - ICMP, multicast, broadcast, SIP ALG, IM, P2P, and IPsec VPN
 - SSL VPN, HTTP multiplexing, SSL offloading, WAN optimization, explicit web proxy, and WCCP
- HTTPS sessions are not load balanced if they are subject to proxy-based inspection
- HTTPS sessions are load balanced only when `load-balance-all` is enabled and:
 - The inspection mode is set to flow mode, or
 - The inspection mode is set to proxy mode and the HTTPS traffic is not inspected
- Session failover and session load balancing
 - Some sessions can be synced, but not necessarily load balanced
 - For example, ICMP sessions can be synced (`session-pickup-connection` must be enabled) but can't be load balanced

In active-active mode, not all sessions qualify for active-active load balancing. This slide shows a list of sessions that can't be load balanced.

Most of the internet traffic nowadays is HTTPS. For this reason, it is important to understand the limitations for HTTPS traffic load balancing. You must know that HTTPS sessions are not load balanced if they are subject to proxy-based inspection. In fact, the only two scenarios in which HTTPS sessions are load balanced is when the `load-balance-all` setting is enabled and:

- The inspection mode is set to flow mode, or
- The inspection mode is set to proxy mode and the HTTPS traffic is not inspected.

Do not confuse session failover with session load balancing. While some sessions can be synchronized to secondary members for session failover protection, those same sessions aren't necessarily supported for active-active load balancing. For example, ICMP sessions can be synchronized to secondary members if you enable the `session-pickup-connectionless` setting, but they cannot be load balanced.

Active-Active Load Balancing Methods

Method	Description
none	The primary handles all sessions
leastconnection	Sessions are sent to the member with the least number of sessions
round-robin	Default method. Sessions are distributed equally across members
weight-round-robin	The more weight a member is assigned, the more sessions it handles
random	Sessions are distributed randomly across members
ip hub	Sessions with the same source and destination IP pair are handled by the same member
ipport	Distribution based on source address, source port, destination address, and destination port information

In active-active mode, when the primary device distributes sessions, it uses one of the following load balancing methods:

- **none:** Load balancing is turned off. The primary handles all sessions.
- **leastconnection:** The primary distributes sessions to the member with the least number of sessions.
- **round-robin:** This is the default method. The primary distributes sessions equally across members.
- **weight-round-robin:** The primary distributes sessions across members based on the member weight. The higher the member weight, the more sessions are distributed to that member.
- **random:** The primary distributes sessions randomly across members.
- **ip and hub:** The primary distributes sessions with the same source and destination IP pair to the same member. Both methods, **ip** and **hub**, work the same way. Both names in the configuration were kept for legacy compatibility purposes. The **hub** schedule will be removed in a future FortiOS version.
- **ipport:** The primary distributes sessions based on the source address, source port, destination address, and destination port information. The more diverse the traffic is, the more evenly the traffic is distributed across members.

DO NOT REPRINT
© FORTINET

Active-Active Load Balancing Methods (Contd)

- Configure link health monitor:

```
config system ha
  set schedule none | hub | leastconnection | round-robin | weight-round-robin | random | ip | ipport
end
```

- If using weight-round-robin, configure the member weight on the primary FortiGate:

```
config system ha
  set weight <id> <weight>
end
```

- Example—33% of sessions to primary and 67% to secondary

```
# get system ha status
...
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1

# config system ha
# set weight 0 1
# set weight 1 2
# end
```

You set the load balancing method by configuring the `schedule` setting, as shown on this slide.

When you select the weight-round-robin method, you must also configure the weight for each member, as shown on this slide. You indicate the member ID followed by its weight. The higher the member weight, the more sessions are distributed to that member. You can obtain the member ID from the output of the `get system ha status` command.

This slide also shows a configuration example for a weight-based distribution of 67% of sessions to the secondary FortiGate and 33% of sessions to the primary device. That is, for every three connections that qualify for load balancing, two of them are distributed to the secondary, and one of them to the primary.

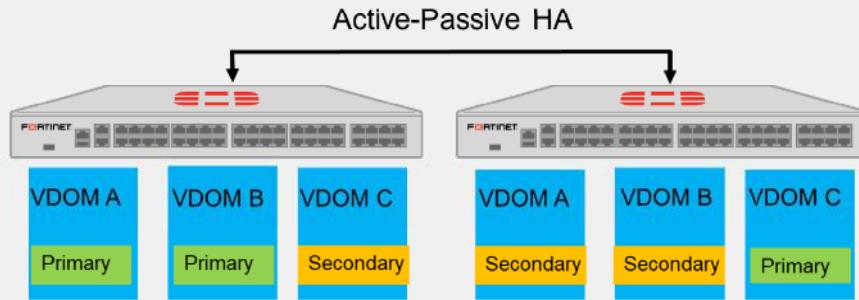
Note that you apply the member weight configuration for all members on the primary device. That is, you don't have to apply the weight on each member individually. The cluster will synchronize the configuration to each member for you.

DO NOT REPRINT

© FORTINET

Virtual Clustering

- Virtual clusters are an extension of FGCP for FortiGate with multiple VDOMs
 - The HA cluster *must* consist of *only* two FortiGate devices
- Allows FortiGate to be the primary for some VDOMs and the secondary for the other VDOMs



So far, you've learned about HA clustering where each FortiGate device acts as a whole security domain.

But, if you have an HA cluster with multiple VDOMs, you can configure *virtual clusters*.

Virtual clusters allow you to have one device acting as the primary for one VDOM, and as the secondary for a different VDOM. Each VDOM has a primary and a secondary FortiGate. Any device can act as the primary for some VDOMs, and the secondary for the other VDOMs, at the same time. Because traffic from different VDOMs can go to different primary FortiGate devices, you can use virtual clustering to manually distribute your traffic between the two cluster devices and allow the failover mechanism for each VDOM between two FortiGate devices.

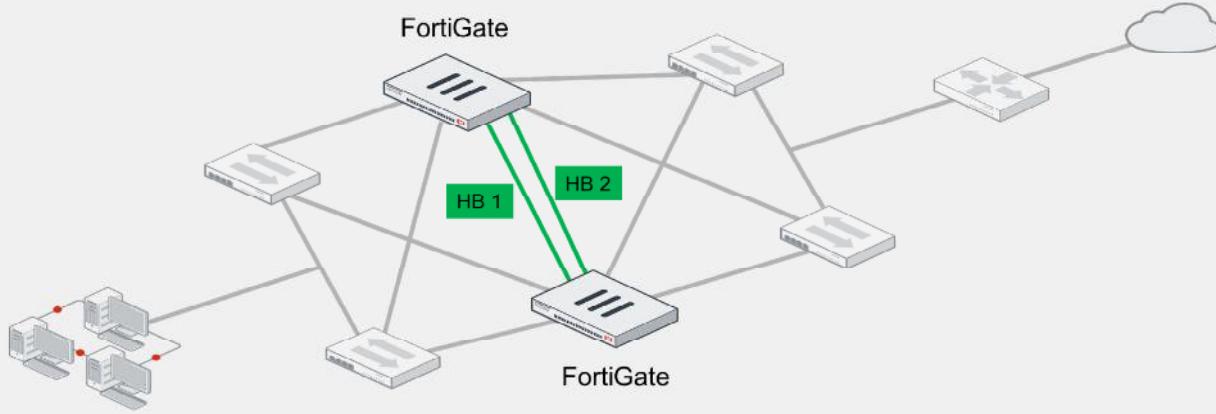
Note that if you deploy virtual clustering with more than two FortiGate devices, only two FortiGate devices will process the traffic.

When you add additional (third or fourth) FortiGate devices to a virtual cluster, the primary FortiGate and first secondary FortiGate handle all traffic, and the remaining FortiGate(s) will be operating in standby mode. In the event of a failure of the primary or first secondary FortiGate, one of the remaining FortiGate devices takes over as the new primary or secondary FortiGate and starts handling the traffic.

FGCP in Active-Active mode cannot load balance any sessions that traverse NPU VDOM links or regular VDOM links. If Active-Active session load balancing between VDOMs is required, use an external router to handle the inter-VDOM routing.

Full Mesh HA

- Eliminates a single point of failure
- Requires redundant or LAG interfaces
 - If using LAG interfaces, the switch must support MCLAG or something similar
 - FortiSwitch supports MCLAG



At the beginning of this lesson, you reviewed a simple HA topology. Now, take a look at a more robust topology. It is called *full mesh HA*.

The goal of a full mesh HA topology is to eliminate a single point of failure, not only by having multiple FortiGate devices forming a cluster, but also by having redundant links to the adjacent switches. The goal is to have two switches for both upstream and downstream links, and then connect the redundant links to different switches. For example, the topology on this slide shows two FortiGate devices forming a cluster, and each FortiGate is connected to two redundant switches, using two different interfaces.

To achieve redundancy with adjacent switches, you must deploy redundant or LAG interfaces. If you use redundant interfaces, only one interface remains active. This avoids a Layer 2 loop and a standard switch should suffice. However, if you want to use LAG interfaces, then you must ensure that the switch supports multichassis link aggregation group (MCLAG) or a similar virtual LAG technology that enables you to form a LAG whose interface members connect to different switches. FortiSwitch, which is a Fortinet Ethernet switch, supports MCLAG. You can use FortiSwitch as the adjacent switch to deploy a full mesh HA topology with FortiGate.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. An HA failover occurs when the link status of a monitored interface on the _____ goes down.
 A. Primary FortiGate
 B. Secondary FortiGate

2. In an active-passive HA cluster, you can configure virtual clustering between only _____ FortiGate devices with multiple VDOMs.
 A. Two
 B. Four

DO NOT REPRINT

© FORTINET

Lesson Progress



HA Operation Modes



HA Cluster Synchronization



HA Failover and Workload



Monitoring and Troubleshooting

Good job! You now understand HA failover and workload.

Now, you will learn about monitoring and troubleshooting an HA cluster.

DO NOT REPRINT**© FORTINET**

Monitoring and Troubleshooting

Objectives

- Verify the normal operation of an HA cluster
- Configure an HA management interface
- Upgrade the HA cluster firmware

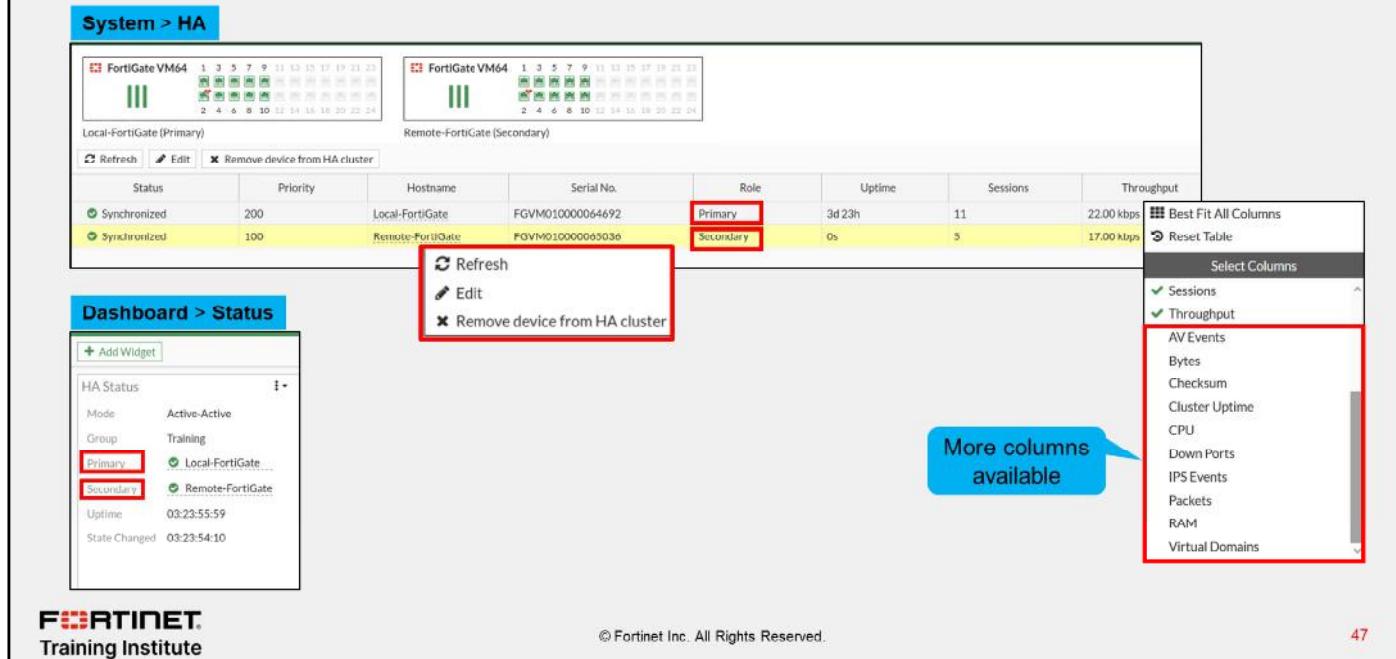
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in monitoring and troubleshooting, you will be able to make sure the cluster is synchronized properly. You will also learn how to configure and access secondary devices in an HA cluster and how to upgrade the firmware on the HA cluster.

DO NOT REPRINT

© FORTINET

Checking the HA Status on the GUI



The screenshot shows the FortiGate GUI with the following interface elements:

- System > HA**: The main table view showing two cluster members:
 - FortiGate VM64 (Local-FortiGate, Primary)**: Status Synchronized, Priority 200, Hostname Local-FortiGate, Serial No. FGVM01000064692, Role Primary, Uptime 3d 23h, Sessions 11, Throughput 22.00 kbps.
 - FortiGate VM64 (Remote-FortiGate, Secondary)**: Status Synchronized, Priority 100, Hostname Remote-FortiGate, Serial No. FGVM01000065036, Role Secondary, Uptime 0s, Sessions 5, Throughput 17.00 kbps.
- Dashboard > Status**: A summary widget showing HA Status (Active-Active), Mode (Training), Group (Primary, Secondary), and Uptime (03:23:55:59).
- Context Menu (over the 'Sessions' column header)**:
 - Refresh
 - Edit
 - Remove device from HA cluster
- Table Column Selection Context Menu** (highlighted with a red box):
 - Best Fit All Columns
 - Reset Table
 - Select Columns
 - Sessions
 - Throughput
 - AV Events
 - Bytes
 - Checksum
 - Cluster Uptime
 - CPU
 - Down Ports
 - IPS Events
 - Packets
 - RAM
 - Virtual Domains
- Text Overlay**: "More columns available" with an arrow pointing to the context menu.
- Page Footer**: FORTINET Training Institute, © Fortinet Inc. All Rights Reserved., 47

The **HA** page on the FortiGate GUI shows important information about the health of your HA cluster. For each cluster member, the page shows whether the member is synchronized or not, and its status, host name, serial number, role, priority, uptime, and active sessions.

On the **HA** page, you can remove a device from a cluster. When you remove a device from HA, the device operation mode is set to standalone. You can also enable more columns that display other important information about each member such as the checksum, CPU, and memory.

You can also add the **HA Status** widget on the **Dashboard** page. The widget provides a summary of the HA status on the device.

DO NOT REPRINT

© FORTINET

Checking the HA Status on the CLI

```
# get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 210
Debug: 0
Cluster Uptime: 2 days 21:28:23
Cluster state change time: 2022-04-20 18:28:23
Primary selected using:
  <2022/04/20 18:28:23> vcluster-1: SN1 is selected as the primary because its uptime is larger than peer member SN2.
  <2022/04/20 16:13:49> vcluster-1: SN2 is selected as the primary because its uptime is larger than peer member SN1.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
Configuration Status:
  SN1(updated 4 seconds ago): in-sync
  SN2(updated 4 seconds ago): in-sync
System Usage stats:
  SN1(updated 4 seconds ago):
    sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=57%
  SN2(updated 4 seconds ago):
    sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=56%
...
...
```

Cluster status, member model, HA mode, and cluster uptime

Latest primary election results and the reason

Configuration sync status

Performance stats of each member

Note: Displayed serial numbers are not real

You can get more information about the HA status on the FortiGate CLI by using the `get system ha status` command.

The command displays comprehensive HA status information in a user-friendly output and is usually executed as the first step when troubleshooting HA. This slide shows the first part of an example output that the command provides. Note that the serial numbers of members have been replaced by fake ones (SN1 and SN2), so the output fits on this slide.

At the beginning of the output, you can see the cluster status, the member model, the HA mode in use, and the cluster uptime. The example output shows that the cluster status is good, the member model is FortiGate-VM64-KVM, and the HA mode is active-passive. The cluster has also been up for almost three days.

Next, you can see the latest primary election events, the result, and the reason. The output indicates that a different member was elected as the primary during the last two election events. In both cases, the member was elected because it had a higher HA uptime.

The configuration status information is displayed next. It indicates the configuration sync status for each member. For both members, the configuration is in sync.

Following the configuration status information, you can see the system usage statistics, which report on performance statistics for each member. They indicate the number of sessions that each member handles, as well as the average CPU and memory usage. Note that the sessions field accounts for any sessions that the member handles, and not only the sessions that are distributed when the HA mode is active-active.

DO NOT REPRINT
© FORTINET

Checking the HA Status on the CLI (Contd)

```
...
HBDEV stats:
  SNI1(updated 4 seconds ago):
    port9: physical/10000full, up, rx-bytes/packets/dropped/errors=154604218/304596/0/0, tx=352015560/498020/0/0
  SNI2(updated 4 seconds ago):
    port9: physical/10000full, up, rx-bytes/packets/dropped/errors=386075683/578563/0/0, tx=269160874/516602/0/0
MONDEV stats:
  SNI1(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0, tx=13209070/157763/0/0
  SNI2(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0, tx=6345393/37126/0/0
PINGSVR stats:
  SNI1(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0, tx=13209070/157763/0/0
    pingsvr: state=up(since 2022/04/20 16:13:50), server=10.9.15.40, ha_prio=5
  SNI2(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0, tx=6345393/37126/0/0
    pingsvr: state=N/A(since 2022/04/20 16:13:54), server=10.9.15.40, ha_prio=5
Primary      : Local-FortiGate , SNI1, HA cluster index = 0
Secondary    : Remote-FortiGate, SNI2, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: SNI1, HA operating index = 0
Secondary: SNI2, HA operating index = 1
```

Heartbeat, monitored, and remote link interfaces status

Member role, host name, serial number, and ID

Note: Displayed serial numbers are not real

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

49

This slide shows the second part of the example output that the `diagnose system ha status` command provides.

The output begins with the status information for the configured heartbeat, monitored, and remote link interfaces. These interfaces enable the cluster to perform device failover, link failover, and remote link failover protection, respectively.

Next, the output shows the role, host name, serial number, and ID information for each member of the cluster. The output indicates that the Local-FortiGate and Remote-FortiGate devices are primary and secondary members, respectively.

Checking the Configuration Synchronization

- Display the member checksum:

```
# diagnose sys ha checksum show

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11
```

Configuration is in sync when all hash values on each member match

- If the checksums don't match, try running:

```
diagnose sys ha checksum recalculate
```

- Display the checksum for all members:

```
# diagnose sys ha checksum cluster

===== FGVM010000112065 =====

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

===== FGVM010000065036 =====

is_manage_primary()=0, is_root_primary()=0
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11
```

The `diagnose sys ha checksum` command tree enables you to check the cluster configuration sync status. In most cases, you want to use the `diagnose sys ha checksum cluster` command to view the cluster checksum. The output includes the checksum of each member in the cluster.

When you run the `diagnose sys ha checksum cluster` command, the checksum is polled from each member using the heartbeat interface. If HA is not working properly, or if there are heartbeat communication issues, then the command may not show the checksum for members other than the one you run the command on. An alternative is to connect to each member individually and run the `diagnose sys ha checksum show` command instead. This command displays only the checksum of the member you are connected to.

After you obtain the checksums of each member, you can identify the configuration sync status by comparing the checksums. If all members show the exact hash values for each configuration scope, then the configuration of all members is in sync.

To calculate checksums, FortiGate computes a hash value for each of the following configuration scopes:

- `global`: global configuration, such as global settings, FortiGuard settings, and so on
- `root`: settings and objects specific to the root VDOM—if you configure multiple VDOMs, FortiGate computes hash values for each VDOM
- `all`: global configuration plus the configuration of all VDOMs

In some cases, the configuration of members is in sync even though the checksums are different. For these cases, try running the `diagnose sys ha checksum recalculate` command to recalculate the HA checksums.

DO NOT REPRINT
© FORTINET

Switching to the CLI of Another Member

- Using the FortiGate CLI, you can connect to the CLI of any member:

```
# execute ha manage <member_id> <admin_username>
```

- To list the ID of each member, use a question mark:

```
# execute ha manage ?  
<id>    please input peer box index.  
<1>    Subsidiary unit FGVM0100000xxxxx
```

- The CLI connection is made over SSH and Ethernet frames type 0x8893

When troubleshooting HA, you may need to connect to the CLI of another member from the CLI of the member you are currently connected to. You do this by using the `execute ha manage` command to connect to the other member.

For example, when you connect to the cluster over SSH using any of the cluster virtual IP addresses, you connect to the primary member. If you then want to connect to another member, you can use the `execute ha manage` command to access its CLI.

This command requires you to indicate the ID of the member you want to connect to and the username you will use to log in. To get the list of member IDs, you can add a question mark to the end of the `execute ha manage` command, as shown on this slide.

Note that when you switch to the CLI of another member, FortiGate establishes an SSH session to that member over the heartbeat interface. The SSH session is then encapsulated in Ethernet frames type 0x8893.

DO NOT REPRINT**© FORTINET**

Force a Permanent Secondary Role on the Primary

- Set the primary to have a permanent secondary:

```
Local-FortiGate # execute ha failover set
Caution: This command will trigger an HA failover.
It is intended for testing purposes.
Do you want to continue? (y/n)
```

- A failover occurs, and the device remains as secondary device
 - *Use the command for testing, demo, or troubleshooting purposes only*
 - Not recommended in production networks

- To view the permanent secondary role status:

```
Local-FortiGate # execute ha failover status
failover status: set
```

- Revert the permanent secondary role state:

```
Local-FortiGate # execute ha failover unset
```

You can set the primary FortiGate to have a permanent secondary role using the `execute ha failover set` command. When you do this, a failover occurs, and the former primary member remains as a secondary member permanently, regardless of the status of other members in the cluster. That is, the impacted member never takes over the cluster even if it's the best candidate for the primary role.

You can revert the permanent secondary role state by running the `execute ha failover unset` command. Note that you should set the primary member to a permanent secondary role for testing, troubleshooting, and demonstration purposes only. Do not use this feature in production networks.

DO NOT REPRINT

© FORTINET

Connect to Any Member Directly

- Reserved HA management interface
 - Out-of-band
 - Up to four dedicated interfaces
 - For local-in traffic and *some* local-out traffic
 - Separate routing table
 - Configuration example (not synchronized):

```
config system ha
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port10"
      set gateway 192.168.100.254
    next
  end
config system interface
  edit "port10"
    set ip 192.168.100.1 255.255.255.0
    set allowaccess ping https ssh snmp
  next
end
```

- In-band HA management interface
 - In-band
 - Use any user-traffic interface
 - For local-in and local-out traffic
 - Shared routing table
 - Configuration example (not synchronized):

```
config system interface
  edit "port1"
    set management-ip 10.0.10.1 255.0.0.0
    set allowaccess ping https ssh snmp
  next
end
```

When you connect to a cluster using any of its virtual IP addresses, you always connect to the primary. You can then switch to the CLI of any member in the cluster by using the `execute ha manage` command. But what if you want to access the GUI of a secondary member or maybe poll data from it using SNMP? For this, you need a way to access each member directly regardless of its role in the cluster.

FortiGate provides two ways for the administrator to connect to a member directly no matter what the member role is. The reserved HA management interface is the out-of-band option. You configure up to four dedicated management interfaces, and you assign them a unique address on each member. You can then use the unique address assigned to each member to connect to them directly. You can also instruct FortiGate to use the dedicated management interface for some outbound management services such as SNMP traps, logs, and authentication requests.

Alternatively, you can configure in-band HA management, which enables you to assign a unique management address to a member without having to set aside an interface for that purpose. You assign the management address to any user-traffic that the member uses, and then connect to the member using that unique management address.

If you have unused interfaces, then it's generally more convenient to use a reserved HA management interface because the user and management traffic don't have to compete. Many FortiGate models come with a management interface that you can use for this purpose. Also, the routing information for a reserved HA management interface is placed in a separate routing table, which means that you don't see the interface routes in the FortiGate routing table. This allows for segmentation between data and management traffic.

This slide also shows configuration examples for both management options. For both options, the configuration you apply on a member is not synchronized to other members in the cluster.

DO NOT REPRINT



Firmware Upgrade

- Apply the new firmware using the GUI or CLI
- Uninterruptible upgrade is enabled by default:

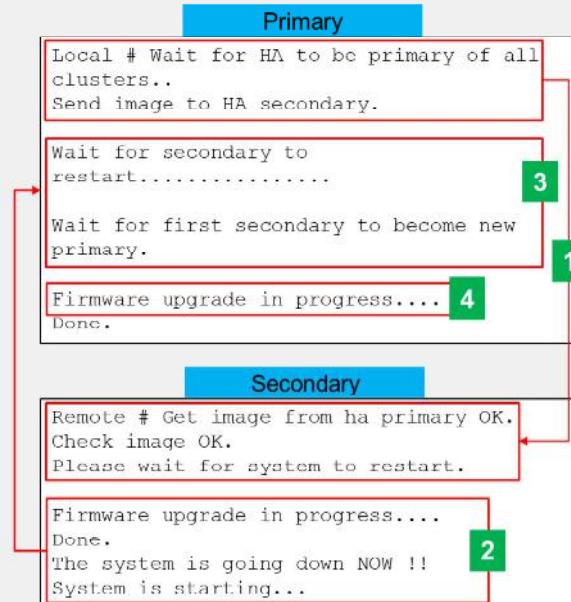
```
config system ha
    set uninterruptible-upgrade enable | disable
end
```

- Firmware upgrade process (uninterruptible upgrade enabled):
 1. The primary sends the firmware image to the secondary devices
 2. The secondary devices upgrade their firmware
 3. The first secondary to finish becomes the primary*
 4. The former primary becomes a secondary device and upgrades its firmware**

Note:

* If HA mode is active-active, the primary temporarily takes over all the traffic.

** Enable the `override` setting on the primary to ensure it takes over the cluster after the firmware upgrade completes.



You upgrade an HA cluster in the same way you do for standalone FortiGate devices. That is, you can apply the new firmware using the GUI firmware upgrade tool. In HA, this usually means connecting to the primary FortiGate GUI to apply the new firmware. You can also use the CLI if you prefer.

Also, like on standalone FortiGate devices, the device must reboot to apply the new firmware. However, by default, members in a cluster are upgraded one at a time to minimize service disruption. This feature is called uninterrupted upgrade and is enabled by default. After the administrator applies the new firmware on the primary, uninterrupted upgrade works as follows:

1. The primary sends the firmware to all secondary members using the heartbeat interface.
2. The secondary devices upgrade their firmware first. If the cluster is operating in active-active mode, the primary temporarily takes over all traffic.
3. The first secondary that finishes upgrading its firmware takes over the cluster.
4. The former primary becomes a secondary device and upgrades its firmware next.

Note that depending on the HA settings and uptime, the original primary may remain as a secondary after the upgrade. Later, if required, you can issue a manual failover. Alternatively, you can enable the `override` setting on the primary FortiGate to ensure it takes over the cluster again after it upgrades its firmware, as long as the device is assigned the higher priority.

If you want the cluster to upgrade all members at the same time to speed up the firmware upgrade process, you can disable uninterrupted upgrade, as shown on this slide. Just keep in mind this will result in a service impact during the firmware upgrade.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which member is the heartbeat interface IP address 169.254.0.1 assigned to?
 A. The member with the highest serial number
 B. The member with the highest priority

2. Which statement about the firmware upgrade process on an HA cluster is true?
 A. You upload the new firmware to the primary FortiGate only.
 B. The members do not reboot.

DO NOT REPRINT**© FORTINET**

Lesson Progress

**HA Operation Modes****HA Cluster Synchronization****HA Failover and Workload****Monitoring and Troubleshooting**

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify the different operation modes for HA
- ✓ Understand the primary FortiGate election in an HA cluster
- ✓ Identify the primary and secondary device tasks in an HA cluster
- ✓ Identify what is synchronized between HA cluster members
- ✓ Configure session synchronization for seamless failover
- ✓ Identify the HA failover types
- ✓ Interpret how an HA cluster in active-active mode distributes traffic
- ✓ Implement virtual clustering per VDOM in an HA cluster
- ✓ Verify the normal operation of an HA cluster
- ✓ Configure an HA management interface
- ✓ Upgrade the HA cluster firmware

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

By mastering the objectives covered in this lesson, you learned about the fundamentals of FortiGate HA and how to configure it.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

Diagnostics

FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn about using diagnostic commands and tools.

DO NOT REPRINT

© FORTINET

Lesson Overview



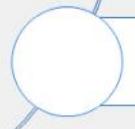
General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

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

DO NOT REPRINT

© FORTINET

General Diagnosis

Objectives

- Identify your network's normal behavior
- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers

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

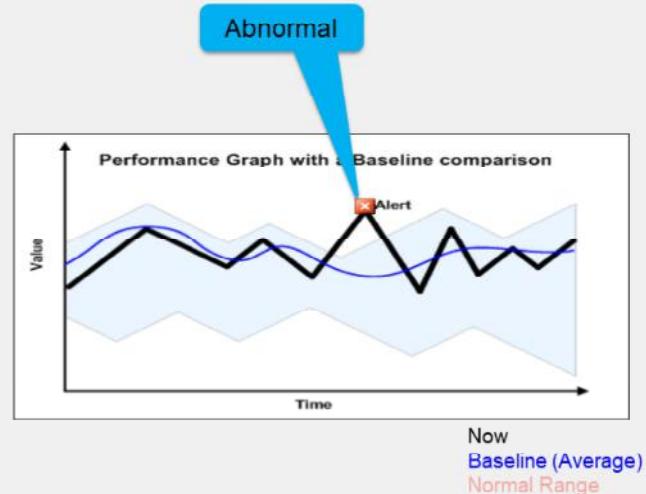
By demonstrating competence in general diagnosis, you will be able to discover general information about the status of FortiGate.

DO NOT REPRINT

© FORTINET

Before a Problem Occurs

- Know what normal is (baseline):
 - CPU usage
 - Memory usage
 - Traffic volume
 - Traffic directions
 - Protocols and port numbers
 - Traffic pattern and distribution
- Why?
 - Abnormal behavior is difficult to identify, *unless* you know, relatively, what normal is



Diagnosis is the process of finding the underlying cause of a problem.

In order to define any problem, first you must know what your network's *normal* behavior is.

In the graph shown on this slide, the range that indicates *normal* is shown in blue. What exactly is this blue line? It indicates the averages—our baseline. What is the thick black line? It's the current behavior. When the current behavior (black line) leaves the normal range, an abnormal event is happening.

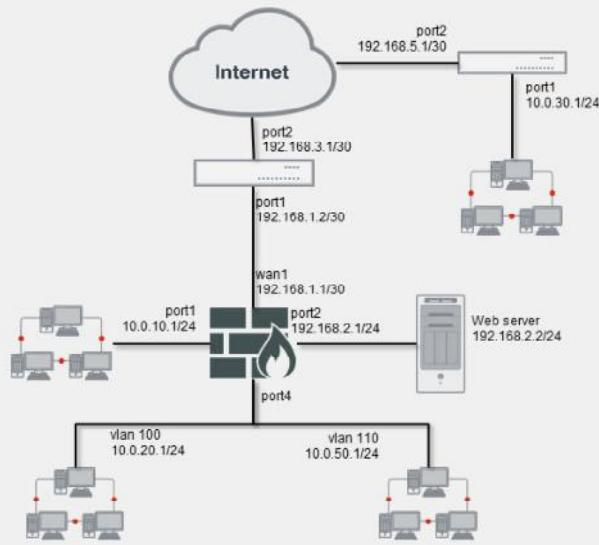
Normal is measured and defined in many ways. It can be performance: the expected CPU and memory utilization, bandwidth, and traffic volumes. But, it can also be your network topology: which devices are normally connected at each node. It is also behavior: traffic flow directions, which protocols are blocked or proxied, and the distribution of protocols and applications used during specific times of the day, week, or year.

DO NOT REPRINT

© FORTINET

Network Diagrams

- Why?
 - Explaining or analyzing complex networks is difficult and time-consuming without them
- Physical diagrams:
 - Include cables, ports, and physical network devices
 - Show relationships at Layer 1 and Layer 2
- Logical diagrams:
 - Include subnets, routers, logical devices
 - Show relationships at Layer 3



What is the first way to define what is *normal* for your network?

Flows and other specifications of *normal* behaviour are derived from topology. So, during troubleshooting, a network diagram is essential. If you create a ticket with Fortinet Technical Support, a network diagram should be the first thing you attach.

Network diagrams sometimes combine the two types of diagrams:

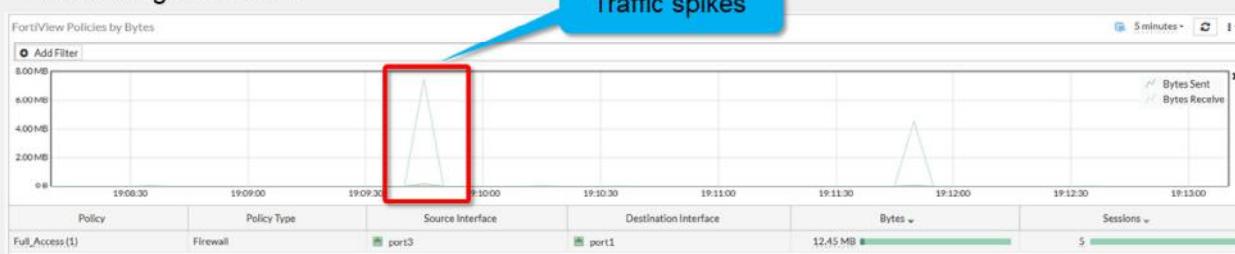
- Physical
- Logical

A physical diagram shows how cables, ports, and devices are connected between buildings and cabinets. A logical diagram shows relationships (usually at OSI Layer 3) between virtual LANs, IP subnets, and routers. It can also show application protocols such as HTTP or DHCP.

DO NOT REPRINT
© FORTINET

Monitoring Traffic Flows and Resource Usage

- Get normal data before problems or complaints
- Tools:
 - Security Fabric
 - Dashboard
 - SNMP
 - Alert email
 - Logging/Syslog/FortiAnalyzer
 - CLI debug commands



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

6

Another way to define normal is to know the average performance range. On an ongoing basis, collect data that shows normal usage.

For example, if traffic processing is suddenly slow, and the FortiGate CPU use is 75%, what does that indicate? If CPU use is usually 60-69%, then 75% is probably still normal. But if normal is 12-15%, there may be a problem.

Get data on both the typical maximum and minimum for the time and date. That is, on a workday or holiday, how many bits per second should ingress or egress each interface in your network diagrams?

DO NOT REPRINT

© FORTINET

System Information

```
FortiGate# set system status
Version: FortiGate-40F-364G v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Virus-DB: 90.01760(2022-04-26 16:26)
Extended DB: 90.01760(2022-04-26 16:26)
AV AI/ML Model: 2.05403(2022-04-26 16:26)
IPS-DB: 20.00304(2022-04-26 00:08)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 20.00304(2022-04-26 00:08)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 3.00331(2022-04-25 16:10)
IoT-Detect: 0.00000(2001-01-01 00:00)
Serial-Number: FG40FITKXXXXXX
BIOS version: 05000004
System Part-Number: P24695-03
Log hard disk: Not available
Hostname: FortiGate
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1157
Release Version Information: GA
System time: Wed Apr 27 12:43:57 2022
Last reboot reason: power cycle
```

```
FortiGate # get system status
Version: FortiGate-VM64-KVM v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Virus-DB: 81.00091(2020-10-14 16:20)
Extended DB: 81.00091(2020-10-14 16:20)
Extreme DB: 1.00000(2018-04-09 16:20)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 2.00797(2020-10-14 05:06)
IoT-Detect: 0.00000(2001-01-01 00:00)
Serial-Number: FGVM010000064692
License Status: Valid
VM Resources: 1 CPU/1 allowed, 2007 MB RAM
Log hard disk: Available
Hostname: FortiGate
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1157
Release Version Information: GA
FortiOS x86-64: Yes
System time: Wed Apr 27 04:16:15 2022
Last reboot reason: shutdown
```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

7

How can we get information about the current status? First, look at CLI commands; you can use them through a local console, even if network issues make GUI access slow or impossible.

A few commands provide system statuses. The `get system status` command provides mostly general-purpose information. The output shows:

- Model
- Serial number
- Firmware version
- Host name
- FortiGuard license status
- System time
- Version of the FortiGuard antivirus, IPS, and IP reputation databases, and others

DO NOT REPRINT
© FORTINET

Hardware Interface Information

```
FortiGate # get hardware nic <interface_name>
Description      :FortiASIC NP6XLITE Adapter
Driver Name     :FortiASIC NP6XLITE Driver
Board          :40Flif
id             :01if
oid            :64
netdev oid     :64
Current_Hwaddr  e0:23:ff:65:19:c8
Permanent_Hwaddr e0:23:ff:65:19:c8
===== Link Status =====
Admin          :up
netdev status   :up
autonego_setting :1
link_setting    :1
speed_setting   :1000
duplex_setting  :0
Speed          :1000
Duplex         :Full
link_status     :Up
```

FortiGate physical interface

```
===== Counters =====
Rx Pkts          :509427
Rx Bytes         :231539694
Tx Pkts          :513489
Tx Bytes         :132128420
Host Rx Pkts    :343935
Host Rx Bytes   :56092804
Host Tx Pkts    :365879
Host Tx Bytes   :51129548
Host Tx dropped  :0
FragTxCreate    :0
FragTxOk        :0
FragTxDrop      :0
```

At the physical layer, troubleshooting analyzes which ports are plugged in, media capacity, and negotiated speed and duplex mode.

At the data link layer, diagnostics often analyze how many frames are being dropped because of CRC errors or collisions.

The get hardware nic command is used to display the FortiGate interface hardware and status information. The output might vary depending on the model and NIC driver version.

DO NOT REPRINT
© FORTINET

Hardware Interface Information (Contd)

```
FortiGate # get hardware nic <interface_name>
```

```
Name: port1
Driver: virtio_net
Version: 1.0.0
Bus: 0000:00:03.0
Hwaddr: 02:09:0f:00:00:00
Permanent Hwaddr: 02:09:0f:00:00:00
State: up
Link: up
Mtu: 1500
Supported: 1000full 10000full
Advertised: 10000full
Speed: 10000full
Auto: disabled
RX Ring: 256
TX Ring: 256
Rx packets: 670785
Rx bytes: 949908714
Rx compressed: 0
Rx dropped: 0
...
```

```
...
Rx errors: 0
Rx Length err: 0
Rx Buf overflow: 0
Rx Crc err: 0
Rx Frame err: 0
Rx Fifo overrun: 0
Rx Missed packets: 0
Tx packets: 57752
Tx bytes: 4993066
Tx compressed: 0
Tx dropped: 0
Tx errors: 0
Tx Aborted err: 0
Tx Carrier err: 0
Tx Fifo overrun: 0
Tx Heartbeat err: 0
Tx Window err: 0
Multicasts: 0
Collisions: 0
```

The output on this slide shows the driver name, hardware address, administrative status, and link status, along with send and receive packets and errors.

DO NOT REPRINT
© FORTINET

ARP Table

```
# get system arp
```

Address	Age (min)	Hardware Addr	Interface
10.0.1.10	0	00:0c:29:e0:c1:87	port3
10.200.1.254	0	00:0c:29:1c:28:d7	port1

Connecting device IP address
and MAC address

FortiGate Interface

If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table. The `get system arp` command is used for that purpose. It shows the FortiGate interface, IP address, and associated MAC address. This command lists the information for all external devices connected to the same LAN segments where FortiGate is connected. The current IP and MAC addresses of FortiGate are not included.

DO NOT REPRINT**© FORTINET**

Network Layer Troubleshooting

```
# execute ping-options
adaptive-ping      Adaptive ping <enable|disable>.
data-size          Integer value to specify datagram size in bytes.
df-bit             Set DF bit in IP header <yes | no>.
interface          Auto | <outgoing interface>.
interval           Integer value to specify seconds between two pings.
pattern            Hex format of pattern, e.g. 00ffaabb.
repeat-count       Integer value to specify how many times to repeat PING.
...
# execute ping <ip> IP address or domain name
# execute traceroute <dest> IP address or hostname
```



© Fortinet Inc. All Rights Reserved.

11

Say that FortiGate can contact some hosts through port1, but not others. Is the problem in the physical layer or the link layer? Neither. Connectivity has been proven with at least part of the network. Instead, you should check the network layer. To test this, as usual, start with ping and traceroute.

The same commands exist for IPv6: execute ping becomes execute ping6, for example.

Remember: location matters. Tests are accurate only if you use the same path as the traffic that you are troubleshooting. To test from FortiGate (to FortiAnalyzer or FortiGuard, for example), use the FortiGate execute ping and execute traceroute CLI commands. But, to test the path through FortiGate, also use ping and tracert or traceroute from the endpoint—from the Windows, Linux, or Mac OS X computer—not only from the FortiGate CLI.

Because of NAT and routing, you might need to specify a different ping source IP address—the default address is the IP of the outgoing interface. If there is no response, verify that the target is configured to reply to ICMP echo requests.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which CLI command can be used to determine the MAC address of a FortiGate default gateway?
 A. get system arp
 B. get hardware nic

2. Which CLI command can be used to diagnose a physical layer problem?
 A. execute traceroute
 B. get hardware nic

DO NOT REPRINT

© FORTINET

Lesson Progress



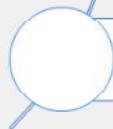
General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Good job! You now understand general diagnostics.

Now, you will learn about debug flow.

DO NOT REPRINT

© FORTINET

Debug Flow

Objectives

- Diagnose connectivity problems using the debug flow

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

By demonstrating competence in the debug flow, you will be able to diagnose connectivity problems.

DO NOT REPRINT**© FORTINET**

Debug Flow

- Shows what the CPU is doing, step-by-step, with the packets
 - If a packet is dropped, it shows the reason
- Multi-step command
 1. Define a filter: `diagnose debug flow filter <filter>`
 2. Enable debug output: `diagnose debug enable`
 3. Start the trace: `diagnose debug flow trace start <xxxx> Repeat number`
 4. Stop the trace: `diagnose debug flow trace stop`

If FortiGate is dropping packets, can a packet capture (sniffer) be used to identify the reason? To find the cause, you should use the debug (packet) flow.

The debug flow shows, step-by-step, how the CPU is handling each packet.

To use the debug flow, follow these steps:

1. Define a filter.
2. Enable debug output.
3. Start the trace.
4. Stop the trace when it's finished.

DO NOT REPRINT
© FORTINET

Debug Flow Example—SYN

```
#diagnose debug flow filter addr 66.171.121.44
#diagnose debug flow filter port 80
#diagnose debug flow trace start 20
#diagnose debug enable

id=2 line=4677 msg="vd-root received a packet(proto=6,
10.0.1.10:49886->66.171.121.44:80) from port3, flag [S], seq 2176715501,
ack 0, win 8192"
id=2 line=4831 msg="allocate a new session-00007fc0"

id=2 line=2582 msg="find a route: flag=04000000
gw-10.200.1.254 via port1"

id=2 line=699 msg="Allowed by Policy-1: SNAT"
id=2 line=2719 msg="SNAT 10.0.1.10->10.200.1.1:49886"
```

IP addresses, port numbers, and incoming interface

Create a new session

Found a matching route. Shows next-hop IP address and outgoing interface

Matching firewall policy

Source NAT

This slide shows an example of a debug flow output of the above `diagnose debug flow` commands, which captures the first packet of a TCP three-way handshake, the SYN packet. It shows:

- The packet arriving at FortiGate, indicating the source and destination IP addresses, port numbers, and incoming interface
- FortiGate creating a session, indicating the session ID
- The route to the destination, indicating the next-hop IP address and outgoing interface
- The ID of the policy that matches and allows this traffic
- How the source NAT is applied

DO NOT REPRINT

© FORTINET

Debug Flow Example—SYN/ACK

```
id=2 line=4677 msg="vd-root received a packet(proto=6,  
66.171.121.44:80->10.200.1.1:49886) from port1. flag [S.],  
seq 3567496940, ack 2176715502, win 5840"
```

IP addresses, port numbers,
and incoming interface

```
id=2 line=4739 msg="Find an existing session,  
id-00007fc0,reply direction"
```

Using an existing session

```
id=2 line=2733 msg="DNAT 10.200.1.1:49886->10.0.1.10:49886"
```

Destination NAT

```
id=2 line=2582 msg="find a route: flag=00000000 gw-10.0.1.10 via port3"
```

Found a matching route.
Shows next-hop IP address
and outgoing interface.

This slide shows the output for the SYN/ACK packet, which is from the same `diagnose debug` command shown on the previous slide. It shows:

- The packet arrival, indicating again the source and destination IP addresses, port numbers, and incoming interface
- The ID of the existing session for this traffic. This number matches the ID of the session created during the SYN packet. The ID is unique for each session, and useful to trace the request/reply packets of the session.
- How the destination NAT is applied
- The route to the destination, indicating again the next-hop IP address and outgoing interface.

If the packet is dropped by FortiGate, this debug shows the reason for that action.

This tool is useful for many other troubleshooting cases, including when you need to understand why a packet is taking a specific route, or why a specific NAT IP address is being applied.

DO NOT REPRINT

© FORTINET

Debug Flow—GUI

- From the GUI:
 - Available on devices with internal storage

Network > Diagnostics > Debug Flow

Packet Capture Debug Flow

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filters

Filter type: Basic Advanced

IP type: IPv4 IPv6

IP address: 8.8.8.8

Port: 80

Protocol: ICMP

Any

Specify

TCP

UDP

SCTP

ICMP

Start debug flow

Network > Diagnostics > Debug Flow

Packet Capture Debug Flow

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filters

Filter type: Basic Advanced

IP type: IPv4 IPv6

Source IP: 10.0.1.10

Source port: 80

Destination IP: 8.8.8.8

Destination port: 80

Protocol: ICMP

Start debug flow

FOR**TI****NET**
Training Institute

© Fortinet Inc. All Rights Reserved.

18

The Debug Flow tool allows you to view debug flow output on the GUI in real time until you stop the debug process.

This tool helps you to examine the packet flow details directly on the GUI.

After you stop the debug flow, you can view the completed output, and filter it by time, message, or function. You can also export the output as a CSV file.

You can set up the Debug Flow tool to use either Basic or Advanced filter options. **Basic** allows you to filter using basic criteria such as host address, port number, and protocol name. **Advanced** allows you to filter by source IP address, source port, destination IP address, destination port, and protocol.

DO NOT REPRINT

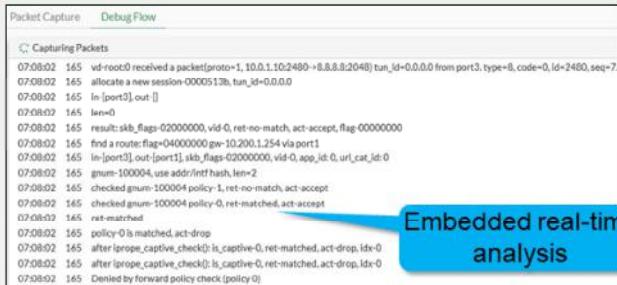
© FORTINET

Debug Flow—GUI (Contd)

- Real Time Analysis

- Embedded real-time analysis page
- Save and download the packet trace output as a CSV file

Real-time flow output

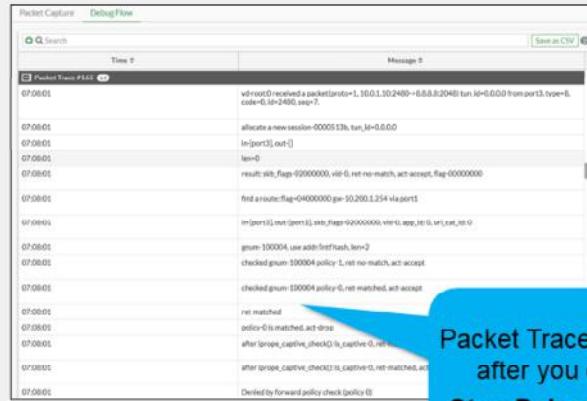


```

Packet Capture Debug Flow
Capturing Packets
07:08:02 165 vd-root0 received a packet(proto>1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.
07:08:02 165 allocate a new session 0000513b, tun_id=0.0.0.0
07:08:02 165 In-[port3],out []
07:08:02 165 len=0
07:08:02 165 result: skb_flags=02000000, vid=0, ret-no-match, act-accept, flag=00000000
07:08:02 165 find a route: flag=04000000 gw=10.200.1.254 via port1
07:08:02 165 In-[port3],out-[port1], skb_flags=02000000, vid=0, app_id=0, url_cat_id=0
07:08:02 165 grnum=100004, use addr/rnt hash, len=2
07:08:02 165 checked grnum=100004 policy=1, ret-no-match, act-accept
07:08:02 165 checked grnum=100004 policy=0, ret-matched, act-accept
07:08:02 165 ret-matched
07:08:02 165 policy=0 is matched, act-drop
07:08:02 165 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:02 165 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:02 165 Denied by forward policy check (policy 0)

```

Packet Trace output



```

Packet Capture Debug Flow
Packet Trace File
Message
07:08:01 vd-root0 received a packet(proto>1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.

07:08:01 allocate a new session 0000513b, tun_id=0.0.0.0
07:08:01 In-[port3],out []
07:08:01 len=0
07:08:01 result: skb_flags=02000000, vid=0, ret-no-match, act-accept, flag=00000000
07:08:01 find a route: flag=04000000 gw=10.200.1.254 via port1
07:08:01 In-[port3],out-[port1], skb_flags=02000000, vid=0, app_id=0, url_cat_id=0
07:08:01 grnum=100004, use addr/rnt hash, len=2
07:08:01 checked grnum=100004 policy=1, ret-no-match, act-accept
07:08:01 checked grnum=100004 policy=0, ret-matched, act-accept
07:08:01 ret-matched
07:08:01 policy=0 is matched, act-drop
07:08:01 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:01 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:01 Denied by forward policy check (policy 0)

```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

After you start the debug flow, the GUI starts displaying the captured packets based on the filter.

When you stop the debug flow, FortiGate displays a Packet Trace output that you can download and save as a CSV file.

The main difference between these two outputs is that real-time messages are displayed for real-time analysis, but you can save the packet trace outputs and download them for future reference.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which information is displayed in the output of a debug flow?
 A. Incoming interface and matching firewall policy
 B. Matching security profile and traffic log

2. When is a new TCP session allocated?
 A. When a SYN packet is allowed
 B. When a SYN/ACK packet is allowed

DO NOT REPRINT

© FORTINET

Lesson Progress



General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Good job! You now understand debug flow.

Now, you will learn about FortiGate CPU and memory diagnosis.

DO NOT REPRINT

© FORTINET

CPU and Memory

Objectives

- Diagnose resource problems, such as high CPU or memory usage
- Diagnose memory conserve mode
- Diagnose fail-open session mode

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

By demonstrating competence in CPU and memory, you will be able to diagnose the most common CPU and memory problems.

DO NOT REPRINT

© FORTINET

Slowness

- High CPU usage
- High memory usage
- What was the last feature you enabled?
 - Enable one at a time
- How high is the CPU usage? Why?
 - # get system performance status
 - # diagnose sys top 1



© Fortinet Inc. All Rights Reserved.

23

Not all problems are network connectivity failures. Sometimes, there are resource problems in the devices.

What else could cause latency? After you have eliminated problems with the physical media and bandwidth usage, you should check the FortiGate resources usage: CPU and memory.

If usage is high, there are tools that can identify which feature is consuming the most CPU. Additionally, you can troubleshoot faster if you know precisely which change (if any) corresponds with the time the problem began.

DO NOT REPRINT**© FORTINET**

High CPU and Memory Troubleshooting

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
1U, 4N, 0S, 95I, 0WA, 0HI, 0SI, 0ST; 994T, 421F
  pyfcgid      248      S      2.9      3.8
  newcli       251      R      0.1      1.0
  merged_daemons 185      S      0.1      0.7
  miglogd      177      S      0.0      6.8
  pyfcgid      249      S      0.0      3.0
  pyfcgid      246      S      0.0      2.8
  reportd      197      S      0.0      2.7
  cmdbsvr      113      S      0.0      2.4
```

Process name

Memory usage (%)

Sort by CPU: Shift + P
Sort by RAM: Shift + M

Process ID

Process state

CPU usage (%)

Next, examine the output for `diagnose sys top`. It lists processes that use the most CPU or memory. Some common processes include:

- `ipsengine`, `scanunitd`, and other inspection processes
- `reportd`
- `fgfmd` for FortiGuard and FortiManager connections
- `forticron` for scheduling
- Management processes (`newcli`, `miglogd`, `cmdb`, `sshd`, and `httpsd`)

To sort the list by highest CPU usage, press Shift+P. To sort by highest RAM usage, press Shift+M.

DO NOT REPRINT

© FORTINET

Memory Conserve Mode

- FortiOS protects itself when memory usage is high
 - It prevents using so much memory that FortiGate becomes unresponsive
- Three configurable thresholds:

Threshold	Definition	Default (% of total RAM)
Green	Threshold at which FortiGate exits conserve mode	82%
Red	Threshold at which FortiGate enters conserve mode	88%
Extreme	Threshold at which new sessions are dropped	95%

```
config system global
  set memory-use-threshold-red <percentage>
  set memory-use-threshold-extreme <percentage>
  set memory-use-threshold-green <percentage>
end
```

If memory usage becomes too high, FortiGate may enter into memory conserve mode. While FortiGate is in memory conserve mode, it must take action to prevent memory usage from increasing, which could cause the system to become unstable and inaccessible.

Memory conserve mode is never a desirable state because it impacts the user traffic.

Three different configurable thresholds define when FortiGate enters and exits conserve mode. If memory usage goes above the percentage of total RAM defined as the red threshold, FortiGate enters conserve mode. The actions that the device takes depend on the device configuration.

If memory usage keeps increasing, it might exceed the extreme threshold. While memory usage is above this highest threshold, all new sessions are dropped.

The third configuration setting is the green threshold. If memory usage goes below this threshold, FortiGate exits conserve mode.

DO NOT REPRINT**© FORTINET**

What Happens During Conserve Mode?

- System configuration cannot be changed
- FortiGate skips quarantine actions (including FortiSandbox analysis)
- For packets that require any flow-based inspection by the IPS engine:
config ips global
 set fail-open {enable|disable}
end
 - enable: Packets can still be transmitted without IPS scanning while in conserve mode
 - disable: Packets are dropped for new incoming sessions, but FortiGate tries to make the existing sessions work in the same way as non-conserve mode



© Fortinet Inc. All Rights Reserved.

26

What actions does FortiGate take to preserve memory while in conserve mode?

- FortiGate does not accept configuration changes, because they might increase memory usage.
- FortiGate does not run any quarantine action, including forwarding suspicious files to FortiSandbox.
- You can configure the `fail-open` setting under `config ips global` to control how the IPS engine behaves when the IPS socket buffer is full.

If the IPS engine does not have enough memory to build more sessions, the `fail-open` setting determines whether the FortiGate should drop the sessions or bypass the sessions without inspection.

It is important to understand that the IPS `fail-open` setting is not just for conserve mode—it kicks in whenever IPS fails. Most failures are due to a high CPU issue or a high memory (conserve mode) issue. Enable the setting so that packets can still be transmitted while in conserve mode (or during any other IPS failure) but are not inspected by IPS. Disable the setting so that packets are dropped for new incoming sessions, but allow FortiOS to try to make the existing sessions work in the same way as non-conserve mode.

Remember that the IPS engine is used for all types of flow-based inspections. The IPS engine is also used when FortiGate must identify the network application, regardless of the destination TCP/UDP port (for example, for application control). Note that NTurbo doesn't support the `fail-open` setting. If `fail-open` is triggered, new sessions that would typically be accelerated with NTurbo are dropped, even if the `fail-open` setting is enabled.

DO NOT REPRINT

© FORTINET

What Happens During Conserve Mode? (Contd)

- For traffic that requires any proxy-based inspection (and if memory usage has not exceeded the extreme threshold yet):

```
config system global
    set av-failopen [off | pass | one-shot]

end
    • off :All new sessions with content scanning enabled are not passed
    • pass (default): All new sessions pass without inspection
    • one-shot: Similar to pass in that traffic is not inspected. However, it will keep bypassing the antivirus proxy even after leaving conserve mode. Administrators must either change this setting, or restart the device, to restart the antivirus scanning
```

- The `av-failopen` setting also applies to flow-based antivirus inspection
- If memory usage exceeds the extreme threshold, all new sessions that require inspection (flow-based or proxy-based) are blocked

The `av-failopen` setting defines the action that is applied to any proxy-based inspected traffic, while the unit is in conserve mode (and as long as the memory usage does not exceed the extreme threshold). This setting also applies to flow-based antivirus inspection. Three different actions can be configured:

- `off`: All new sessions with content scanning enabled are not passed but FortiGate processes the current active sessions.
- `pass` (default): All new sessions pass without inspection until FortiGate switches back to non-conserve mode.
- `one-shot`: Similar to `pass` in that traffic passes without inspection. However, it will keep bypassing the antivirus proxy even after it leaves conserve mode. Administrators must either change this setting, or restart the unit to restart the antivirus scanning

However, if the memory usage exceeds the extreme threshold, new sessions are always dropped, regardless of the FortiGate configuration.

DO NOT REPRINT
© FORTINET

System Memory Conserve Mode Diagnostics

```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2706 MB 89% of total RAM
memory freeable: 334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used threshold green: 2492 MB 82% of total RAM
```

on Off = no conserve mode
on = conserve mode



© Fortinet Inc. All Rights Reserved.

28

The diagnose hardware sysinfo conserve command is used to identify if a FortiGate device is currently in memory conserve mode.

DO NOT REPRINT**© FORTINET**

Fail-Open Session Setting

- The following setting controls how FortiOS handles a session that is impacted by a UTM scan error when doing http/mapi proxy or explicit webproxy

```
config system global
    set av-failopen-session [enable | disable]
```

- enable = Sessions are allowed
- disable (default) = Block all new sessions that require proxy-based inspection



© Fortinet Inc. All Rights Reserved.

29

Another undesirable state for FortiGate is the fail-open session mode. This mode kicks in, not during a high-memory situation, but when a proxy on FortiGate runs out of available sockets to process more proxy-based inspected traffic.

If `av-failopen-session` is enabled, FortiGate allows all the sessions. Otherwise, by default, it blocks new sessions that require proxy-based inspection until new sockets become available.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which action does FortiGate take during memory conserve mode?
 A. Configuration changes are not allowed.
 B. Administrative access is denied.

2. Which threshold is used to determine when FortiGate enters conserve mode?
 A. Green
 B. Red

DO NOT REPRINT

© FORTINET

Lesson Progress



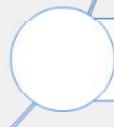
General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Good job! You now understand FortiGate CPU and memory diagnosis.

Now, you will learn about FortiGate firmware and hardware diagnosis.

DO NOT REPRINT

© FORTINET

Firmware and Hardware

Objectives

- Format the flash memory
- Load a firmware image from the BIOS menu
- Run hardware tests
- Display crash log information

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

By demonstrating competence in firmware and hardware, you will be able to diagnose the most common firmware and hardware problems.

DO NOT REPRINT**© FORTINET**

Access to BIOS Menu

FortiGate-81E-POE (12:25-10.04.2016)

Ver:05000003

Serial number: FG81EPxxxxxxxxxx

CPU: 1000MHz

Total RAM: 2 GB

Initializing boot device...

Initializing MAC... nplite#0

Please wait for OS to boot or press any key to display configuration menu

BIOS version. Options in the BIOS menu depend on the version

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,I,B,Q,or H:

Press any key at this prompt to enter the BIOS menu

On the FortiGate BIOS, administrators can run some operations over the flash memory and firmware images. To access the BIOS menu, you must reboot the device while connected to the console port. The booting process, at one point, shows the following message:

Press any key to display configuration menu

While this prompt is displayed, press any key to interrupt the booting process and display the BIOS menu. In the BIOS menu, you can see the options shown on this slide.

Firmware Installation From Console

Make sure that a TFTP server application is installed on your PC

Configure the TFTP server directory and copy the FortiGate firmware [image.out]

Connect your PC NIC to the FortiGate TFTP install interface

Select get firmware image from the BIOS menu

After reformatting the flash memory, you must install the firmware image from the BIOS menu. Follow these steps:

1. Run a TFTP server.
2. Configure the TFTP server with the folder where the firmware image file is stored.
3. Connect the PC Ethernet port to the FortiGate TFTP installation interface.
4. Select get firmware image from the BIOS menu.

The interface assigned as the TFTP installation interface depends on the model. However, and in most cases, it is either the *port1* or *internal* interface.

DO NOT REPRINT**© FORTINET**

Format Flash Memory

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Recommended for a clean
installation and problems possibly
related to corrupted firmware

Enter C,R,T,F,I,B,Q,or H: F

All data will be erased, continue: [Y/N]?

Formatting boot device...

.....

Format boot device completed.

CAUTION: Formatting the flash memory deletes the firmware,
configuration, and digital certificates

From the BIOS menu, select F to format the flash memory.

Doing this might be required if the firmware gets corrupted, or if the administrator wants to do a clean installation of new firmware. Keep in mind, though, that formatting the flash memory deletes any information stored on it, such as firmware images, configuration, and digital certificates.

DO NOT REPRINT**© FORTINET**

Configure TFTP Parameters

Enter C,R,T,F,I,B,Q,or H: C

[P]: Set firmware download port.
[D]: Set DHCP mode.
[I]: Set local IP address.
[S]: Set local subnet mask.
[G]: Set local gateway.
[V]: Set local VLAN ID.
[T]: Set remote TFTP server IP address.
[F]: Set firmware file name.
[E]: Reset TFTP parameters to factory defaults.
[R]: Review TFTP parameters.
[N]: Diagnose networking(ping).
[Q]: Quit this menu.
[H]: Display this list of options.

Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:



© Fortinet Inc. All Rights Reserved.

36

From the BIOS menu, select C to configure TFTP parameters. Use the menu options to configure parameters, such as local IP address, subnet mask, gateway address, and firmware file name.

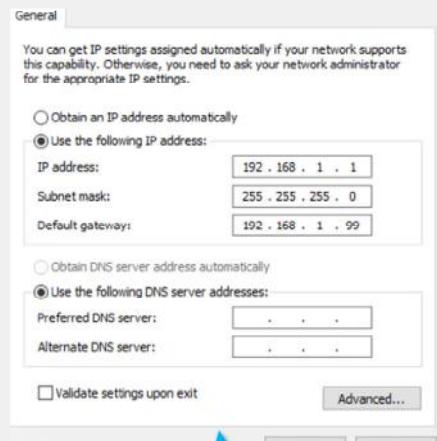
DO NOT REPRINT
© FORTINET

FortiGate and TFTP Server Configuration Settings

Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H: R

Image download port: MGMT
 DHCP status: Disabled
 Local VLAN ID: <NULL>
 Local IP address: 192.168.1.99
 Local subnet mask: 255.255.255.0
 Local gateway: 192.168.1.1
 TFTP server IP address: 192.168.1.1
 Firmware file name: image.out

FortiGate TFTP settings



TFTP server IP address configuration

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

37

Press R to review the TFTP configuration settings.

After you have configured the TFTP parameters, press Q to return to the main configuration menu.

DO NOT REPRINT
© FORTINET

BIOS Firmware Transfer

Enter C,R,T,F,I,B,Q,or H: T

CAUTION: Transferring a firmware image deletes the configuration and installs the factory default configuration

```
Enter TFTP server address []: 192.168.1.1
Enter local address []:192.168.1.99
Enter firmware image file name []:image.out
MAC:00090FC371BE
#####
Total 23299683 bytes data downloaded.
Verifying the integrity of the firmware image.

Total 40000kB unzipped.
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]? D
Programming the boot device now.
.
.
.
Reading boot image 1375833 bytes.
Initializing firewall...
System is started.
Formatting shared data partition ... done!
```



© Fortinet Inc. All Rights Reserved.

38

From the BIOS menu, press **T** to initiate the TFTP firmware transfer.

The BIOS requires you to enter:

- The IP address of the TFTP server
- The FortiGate IP address (it must be in the same class-C subnet as the TFTP server)
- The name of the firmware image

If everything is OK, you should see a series of pound signs, indicating that the device is downloading the image. The BIOS will then verify the integrity of the file and give you the following three options:

- Save it as the default firmware
- Save it as the backup firmware
- Run the image without saving it

If the firmware is going to be used in production, select the first option: Save it as the default firmware.

The last option (Run the image without saving it) allows you to run and test firmware without overwriting any existing firmware in the memory. After you have finished the tests and are ready to roll back the change, you must reboot the device, and the previously existing firmware will be used.

DO NOT REPRINT

© FORTINET

Hardware Tests

- Designed for both manufacturing testing and for end users to verify major hardware components:
 - CPU
 - RAM memory
 - Network interfaces
 - Hard disk
 - Flash memory
 - USB interface
 - Front panel LEDs
 - Wi-Fi
 - And so on



© Fortinet Inc. All Rights Reserved.

39

As with any other electronic device, damage to RAM can cause intermittent crashes.

If you suspect hardware failure, you can run hardware tests.

How do you run the hardware tests? It depends on the FortiGate model.

DO NOT REPRINT
© FORTINET

How to Run the Hardware Tests

- In some E, F, and D-series models, the hardware tests can be run directly from FortiOS
 - Can run a single test, or multiple tests
- For other models, a special HQIP image must be loaded using TFTP and run from the BIOS menu
 - Instructions: <https://support.fortinet.com/Download/HQIPImages.aspx>



© Fortinet Inc. All Rights Reserved.

40

For some FortiGate E, F, and D-series models, you can run the hardware tests directly from the FortiOS CLI.

For other models, you must download special HQIP hardware testing images from the Fortinet Technical Support website.

The steps for uploading the hardware test image are the same as the ones used for uploading a firmware image. You can run the hardware test image without saving it in the flash memory, so any existing firmware image won't be overwritten.

DO NOT REPRINT**© FORTINET**

FortiOS Hardware Tests Command

```
# diagnose hardware test suite all

- Please connect ethernet cables:
[WAN - Any of PORT1...PORT4]
To skip this test, please press 'N'.
Do you want to continue? (y/n) (default is n) N
Following tests will request you to check the colours of the system LEDs.
To skip this test, please press 'N'.
Do you want to continue? (y/n) (default is n) N
Following tests will request you to check the colours of the NIC LEDs.
- Please connect ethernet cables:
[WAN - Any of PORT1...PORT4]
To skip this test, please press 'N'.
Do you want to continue? (y/n) (default is n) N
Test Begin at UTC Time Wed May 05 21:08:53 2021
```



© Fortinet Inc. All Rights Reserved.

41

For some models, the command `diagnose hardware test suite all` runs the hardware tests from FortiOS. The hardware tests require user interaction while running. Users can skip some of the steps. Some tests require connecting external devices (such as USB flash drives) or network cables to FortiGate.

DO NOT REPRINT

© FORTINET

Crash Logs

- Inspect crash logs for debugging purposes
- Any time a process closes, it is recorded as *killed*
 - Some are normal (for example, closing `scanunit` to update definitions)

```
# diagnose debug crashlog history
Crash log interval is 3600 seconds
httpsd crashed 1 times. The last crash was at 2022-06-03 02:31:34

# diagnose debug crashlog read
97: 2022-05-24 01:59:31 from=license sn=FGVM0100000/5036 msg=License status changed to VALID
98: 2022-06-03 02:31:34 Signal <11> was sent to process <31308> by user <admin>
99: 2022-06-03 02:31:34 <31308> firmware FortiGate-VM64-KVM v7.2.0,build1157b1157,220331 (GA.F)
100: 2022-06-03 02:31:34 <31308> application httpsd
101: 2022-06-03 02:31:34 <31308> *** signal 11 (Segmentation fault) received ***
102: 2022-06-03 02:31:34 <31308> Register dump:
103: 2022-06-03 02:31:34 <31308> RAX: 0000000000000002b RBX: 0000000000000000
```

The https process was restarted
by the administrator

Another area you might want to monitor, purely for diagnostics, is the crash logs. Crash logs are available through the CLI.

Any time a process is closed for any reason, the crash log records this as a crash. Most of the logs in the crash log are normal. For example, any time the antivirus definitions package is updated, the `scanunit` process needs to close down in order to apply the new package. This is a normal shutdown. Some logs in the crash log shows they are initiated by a user, which indicates the administrator manually restarted a process.

Some logs in the crash log might indicate problems. For that reason, the crash logs are frequently requested by Fortinet Technical Support for troubleshooting purposes.

This slide shows the commands you have to use to get a crash log. The crashlog output shows the http process is restarted by the administrator.

Two commands can show information from the crash logs:

- `diagnose debug crashlog history` lists a summary of the processes that have crashed, how many crashes have happened, and the time of the last crash.
- `diagnose debug crashlog read` provides details about each crash, in addition to other system events, such as conserve mode entry and exit times.

DO NOT REPRINT**© FORTINET**

Conserve Mode Events in Crash Logs

- The crash log also records conserve mode events

- Entering:

```
12: 2021-04-06 14:10:16 logdesc="Kernel enters conserve mode" service=kernel
conserve-on free="127962
13: 2021-04-06 14:10:16 pages" red="128000 pages" msg="Kernel enters conserve
mode"
```

- Exiting:

```
14: 2021-04-06 14:19:55 logdesc="Kernel leaves conserve mode" service=kernel
conserve=exit
15: 2021-04-06 14:19:55 free="192987 pages" green="192000 pages" msg="Kernel
leaves conserve mode"
```

This slide shows the entries generated in the crash logs when FortiGate enters and exits memory conserve mode.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which types of information are stored in the crash log?
 A. Process crashes and conserve mode events
 B. Traffic logs and security logs

2. Which protocol is used to upload new firmware from the console?
 A. HTTP/HTTPS
 B. TFTP

DO NOT REPRINT

© FORTINET

Lesson Progress



General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Congratulations! You have completed the lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify the normal behavior of your network
- ✓ Monitor for abnormal behavior, such as traffic spikes
- ✓ Diagnose problems at the physical and network layers
- ✓ Diagnose connectivity problems using the debug flow
- ✓ Diagnose resource problems, such as high CPU or memory usage
- ✓ Diagnose memory conserve mode
- ✓ Diagnose fail-open session mode
- ✓ Format the flash memory
- ✓ Load a firmware image from the BIOS menu
- ✓ Run hardware tests
- ✓ Display crash log information



© Fortinet Inc. All Rights Reserved.

46

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

By mastering the objectives covered in this lesson, you learned how to use diagnostic commands and tools.



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© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.