

**DO NOT REPRINT
© FORTINET**



Enterprise Firewall Study Guide

for FortiOS 6.4

DO NOT REPRINT © FORTINET

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

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

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguards.com>

Fortinet Network Security Expert Program (NSE)

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

Fortinet | Pearson VUE

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

Feedback

Email: courseware@fortinet.com



6/26/2020

TABLE OF CONTENTS

01 Security Fabric.....	4
02 FortiOS Architecture.....	35
03 Traffic and Session Monitoring.....	87
04 Routing.....	128
05 FortiGuard.....	168
06 High Availability.....	202
07 Central Management.....	237
08 OSPF.....	265
09 Border Gateway Protocol.....	310
10 Web Filtering.....	349
11 Intrusion Prevention System.....	372
12 IPsec.....	412
13 Autodiscovery VPN.....	457
Solution Slides.....	491

DO NOT REPRINT
© FORTINET



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

DO NOT REPRINT
© FORTINET

Objectives

- Describe the Enterprise Firewall solution
- Configure the Fortinet Security Fabric
- Perform security rating audit
- Configure automation stitches

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

By demonstrating competence in the Fortinet Security Fabric, you will be able to describe the Fortinet Enterprise Firewall solution. You will also be able to configure the Fortinet Security Fabric, perform a security rating audit of your Security Fabric, and configure automation.

**DO NOT REPRINT
© FORTINET**

Enterprise Firewall Solution Overview

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

DO NOT REPRINT
© FORTINET

Evolution of the Enterprise Network

- Networks are no longer flat and one-dimensional
 - Protecting the perimeter is not enough
- Enterprises must protect against a range of constantly evolving threats
 - Zero-day attacks, advanced persistent threats (APT), polymorphic malware, insider threats, and much more
- Bring your own device (BYOD), and evolving cloud technologies are creating *borderless* networks

FORTINET

© Fortinet Inc. All Rights Reserved.

4

The traditional way of protecting a network by securing the perimeter has become a thing of the past. Network and security administrators today must protect against a wide range of threats such as zero-day attacks, APTs, polymorphic malware, and many more. They must also protect the network from any potential insider threats. BYOD and evolving cloud technologies are creating borderless networks, which is further compounding the challenge of securing such complex networks.

DO NOT REPRINT
© FORTINET

The Borderless Enterprise

- The enterprise perimeter has been stretched so far that it's no longer recognizable:
 - Mobile workforce
 - Partners accessing your network services
 - Public and private clouds
 - Internet of things (IoT)
 - BYOD
- You must apply the zero-trust model:
 - The attack can come from anywhere, using any method, and affect anything

FORTINET

© Fortinet Inc. All Rights Reserved.

5

The perimeter of an enterprise network is no longer recognizable. What happens when employees connect to the corporate network from home? Does the network perimeter extend to each employee's home network? Where is the perimeter when there are services running in the cloud? What about employees' personal devices (BYOD)?

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

DO NOT REPRINT
© FORTINET

The Enterprise Firewall Solution

- Apply end-to-end security
 - From IoT to the cloud
- Segment your network!
 - Internal segmentation firewall (ISFW)
- However, there are challenges:
 - Many layers
 - Multiple vendors
 - No central visibility
 - No central control
 - Zero-day growth

FORTINET

© Fortinet Inc. All Rights Reserved.

6

In the same way that threats and network technologies have evolved, your network security strategies must evolve too. You must apply end-to-end security, from the endpoints to the cloud. Additionally, you must deploy internal segmentation firewalls to segment the network so that any breach coming from inside can be contained in one segment of the network, without reaching other segments.

However, there are challenges to implementing these measures. You need to implement multiple layers of security, from the endpoints, through the protected services, through the network entry points, and up to the cloud. This usually implies the use of multiple vendors, which means no central management and no central visibility over what is happening in the network.

[illegible]

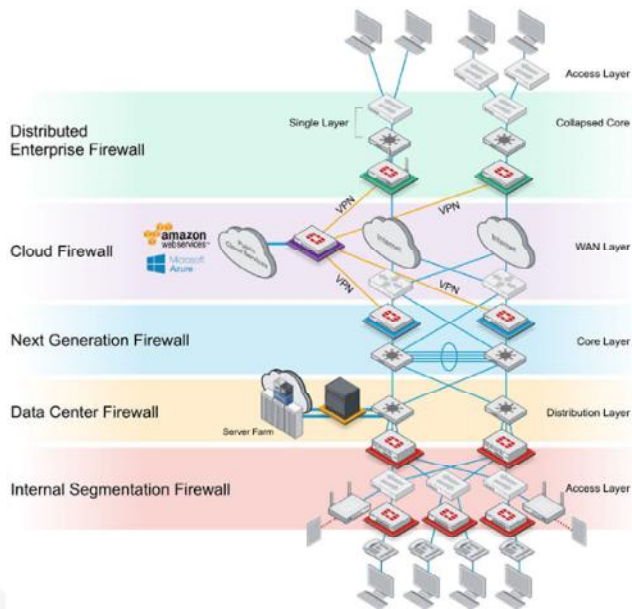
© Fortinet Inc. All Rights Reserved.

7

Enterprise Firewall 6.4 Study Guide

DO NOT REPRINT
© FORTINET

Firewall Roles



- Different roles depending on where FortiGate is deployed:

- Distributed enterprise firewall (DEFW)
- Cloud firewall (CFW)
- Next-generation firewall (NGFW)
- Data center firewall (DCFW)
- Internal segmentation firewall (ISFW)

FORTINET

© Fortinet Inc. All Rights Reserved.

8

In the Enterprise Firewall solution, each FortiGate device has a specific role, depending on where it is installed and what assets it's protecting. In general, there are five roles:

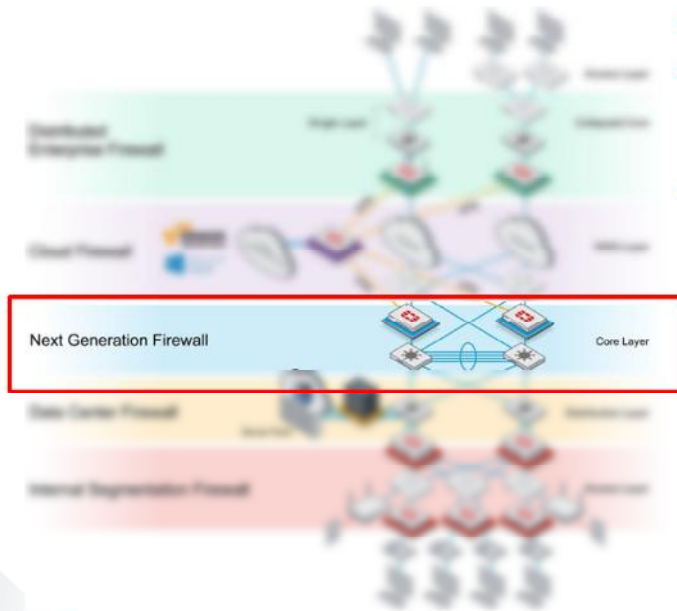
- Distributed enterprise firewall (DEFW)
- Cloud firewall (CFW)
- Next-generation firewall (NGFW)
- Datacenter firewall (DCFW)
- Internal segmentation firewall (ISFW)

In this lesson you will learn about the DEFW, NGFW, DCFW, and ISFW.

Please note that these are not different types of FortiGate models. You can define these roles depending on where FortiGate is installed.

DO NOT REPRINT
© FORTINET

Next-Generation Firewall



- 1G – 40Gbps throughput
- Usually deployed for firewall, application control, IPS, antivirus, and VPN
- Depending on the infrastructure, you can deploy NGFW at the edge, or in the core

FORTINET

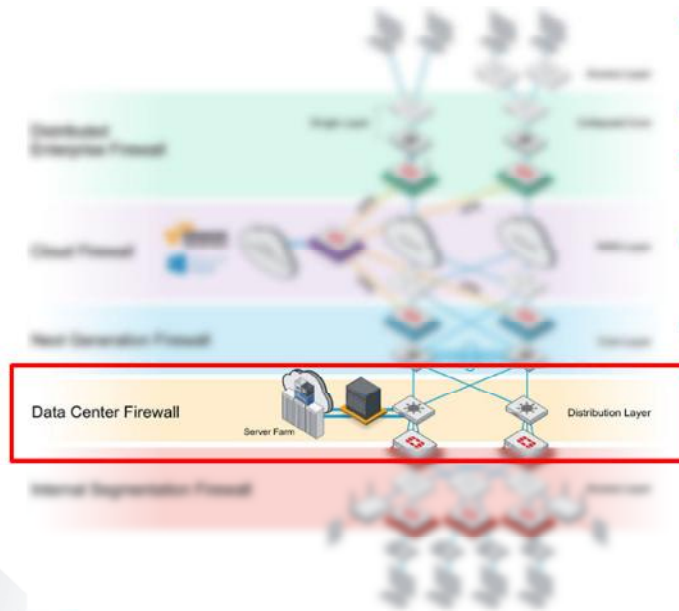
© Fortinet Inc. All Rights Reserved.

9

NGFWs are usually deployed for firewall, application visibility, intrusion prevention, malware detection, and VPNs. NGFWs can play the traditional role of the entry-point firewall or, depending on the network infrastructure, can be deployed in the core.

DO NOT REPRINT
© FORTINET

Data Center Firewall



- Protect servers, low latency, inbound-security focused
- 10G – 1Tbps throughput
- Firewall, application control, and IPS commonly used
- Placed in data centers and in the enterprise DMZ
- Deployed at the distribution layer

FORTINET

© Fortinet Inc. All Rights Reserved.

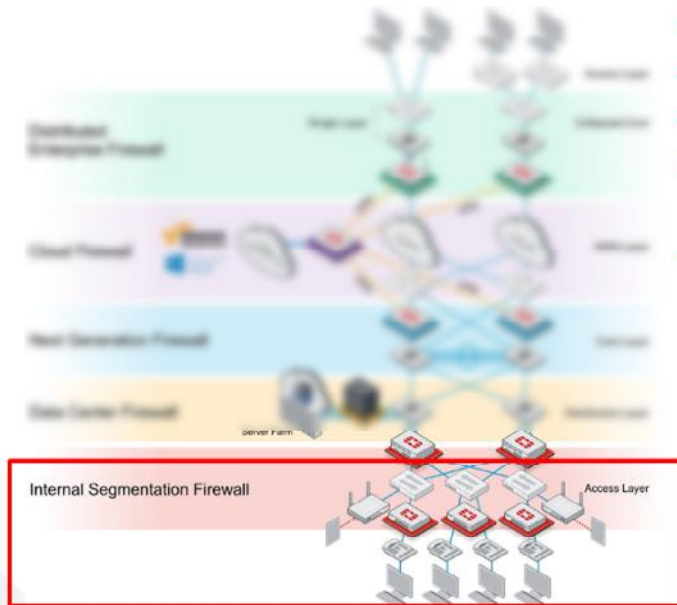
10

DCFWs protect corporate services. They focus on inspecting incoming traffic and are usually installed at the distribution layer.

The throughput requirements of DCFW is the highest of all deployment roles. This can range from 10Gbps all the way up to 1Tbps. Because of the high performance requirements, in most cases the security functions are kept to a minimum: firewall, application control, and IPS.

DO NOT REPRINT
© FORTINET

Internal Segmentation Firewall



- Zero trust network
- Breach containment
- 1G – 100Gbps throughput
- Firewall, application control, web filtering, and IPS most common
- Placed in the access layer

FORTINET

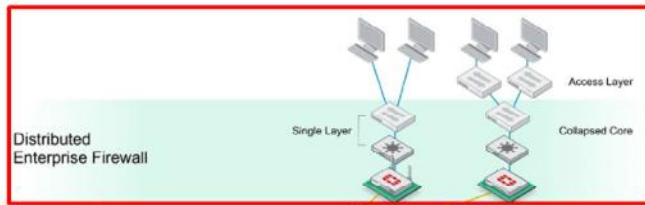
© Fortinet Inc. All Rights Reserved.

11

ISFWs split your network into multiple security segments. They serve as breach containers for attacks that come from inside. Firewall, application control, web filtering, and IPS are the features that are commonly enabled in these firewalls. It's also a good place to perform antivirus, and implement sandbox inspection so you can isolate specific devices in specific segments and prevent propagation.

DO NOT REPRINT
© FORTINET

Distributed Enterprise Firewall



- Extension of the enterprise network
- VPN dependent
- 1Gbps throughput
- Security for smaller locations and branch offices
- All-in-one security (firewall, application control, VPN, IPS, antivirus)

FORTINET

© Fortinet Inc. All Rights Reserved.

12

DEFWs are usually smaller devices installed in branch offices and remote sites. Distributed enterprises usually don't follow a standardized enterprise network design, and therefore multiple layers are collapsed into one or two layers. They are connected to the corporate headquarters using a VPN.

DEFWs are all-in-one security devices, doing firewall, application control, IPS, web filtering, and antivirus inspection.

DO NOT REPRINT
© FORTINET

Security Fabric



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

DO NOT REPRINT
© FORTINET

Fortinet End-to-End Solution

- Fortinet Security Fabric delivers solutions in five key areas:
 - Zero-trust access
 - Security-driven networking
 - Dynamic cloud security
 - AI-driven security operations
 - Fabric management center



FORTINET

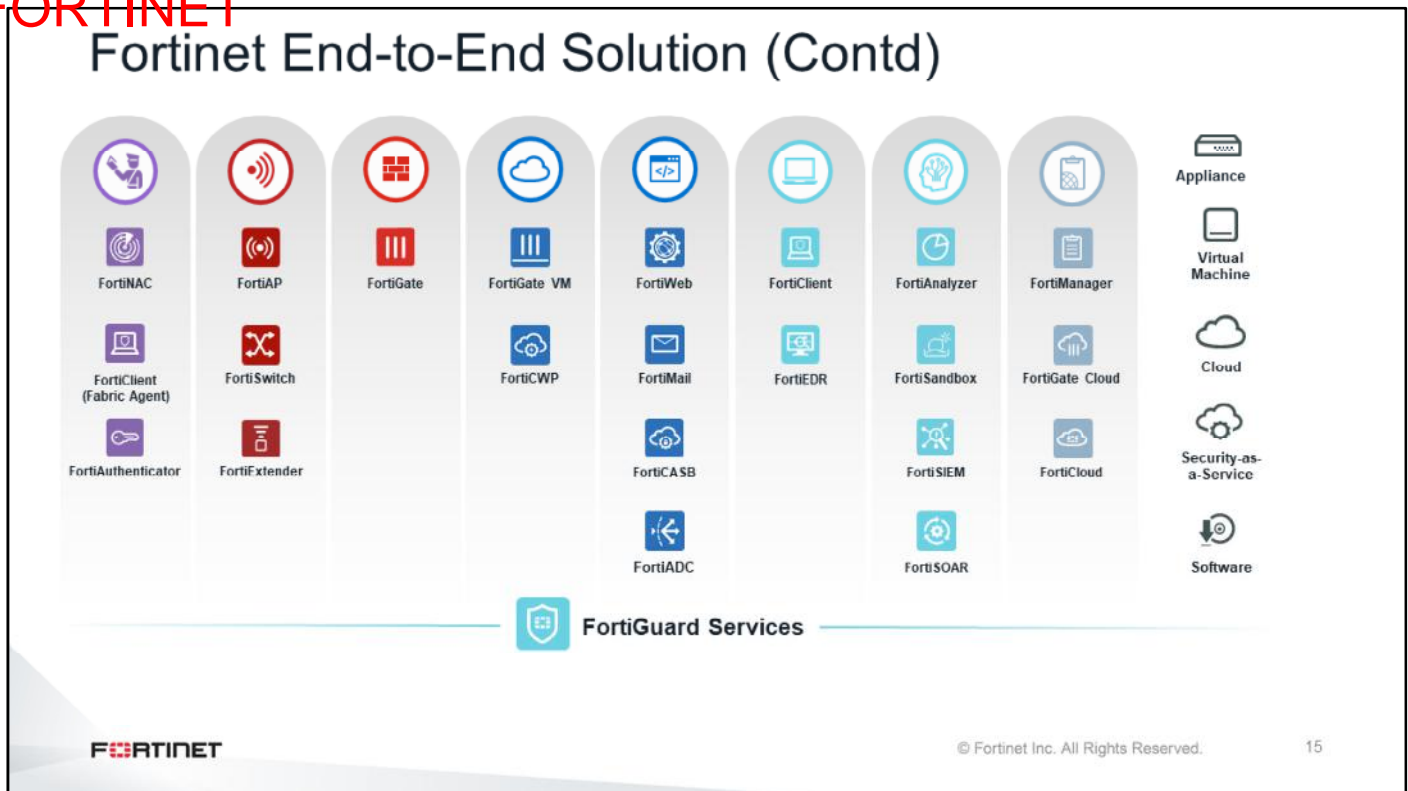
© Fortinet Inc. All Rights Reserved.

14

The Fortinet Security Fabric ties your network together to provide visibility and control. The Fortinet Security fabric covers:

- Zero-trust network access
- Security-driven networking
- Dynamic cloud security
- AI-driven security operations
- Fabric management center

DO NOT REPRINT
© FORTINET

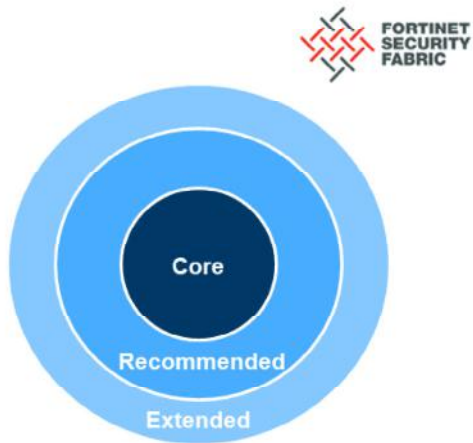


The Fortinet Security Fabric delivers a unified approach that is broad, integrated, and automated. It reduces and manages the attack surface through integrated broad visibility, stopping advanced threats through integrated AI-driven breach prevention, while reducing complexity through automated operations and orchestration.

The Fortinet Security Fabric segments the entire network—from the Internet of things (IoT) to the cloud—to provide an end-to-end solution.

DO NOT REPRINT
© FORTINET

Devices That Comprise the Security Fabric



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

FORTINET

© Fortinet Inc. All Rights Reserved.

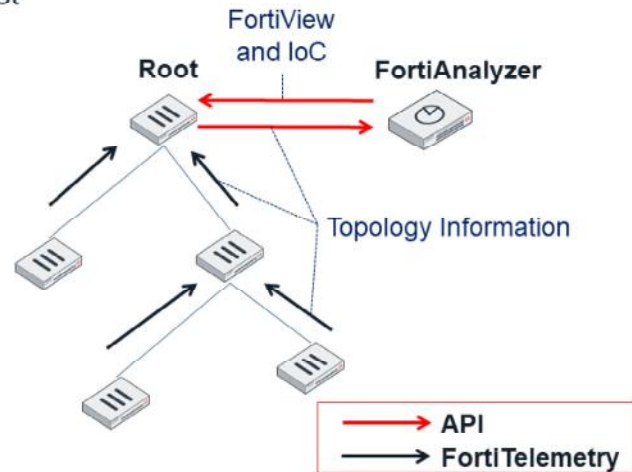
16

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

DO NOT REPRINT
© FORTINET

Security Fabric Topology

- Root FortiGate must be configured first
 - FortiAnalyzer registration
 - FortiManager registration
- Tree structure
 - Branch FortiGate devices connect to upstream FortiGate devices
- FortiGate verifies the FortiAnalyzer serial number against its certificate
 - The serial number is stored in the FortiGate configuration



FORTINET

© Fortinet Inc. All Rights Reserved.

17

The Security Fabric follows a tree model. You must configure the root FortiGate first. This includes FortiAnalyzer registration and, if any, FortiManager registration. The branch FortiGate devices connect to upstream FortiGate devices to form the Security Fabric tree.

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

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

DO NOT REPRINT
© FORTINET

Upstream and Downstream FortiGate

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

18

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

DO NOT REPRINT
© FORTINET

Security Fabric Configuration Synchronization

- FortiAnalyzer and FortiManager configuration is pushed from the root FortiGate:
 - All members send logs to a single FortiAnalyzer
 - All members are managed by the same FortiManager

- You can disable the configuration synchronization:

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

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

19

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

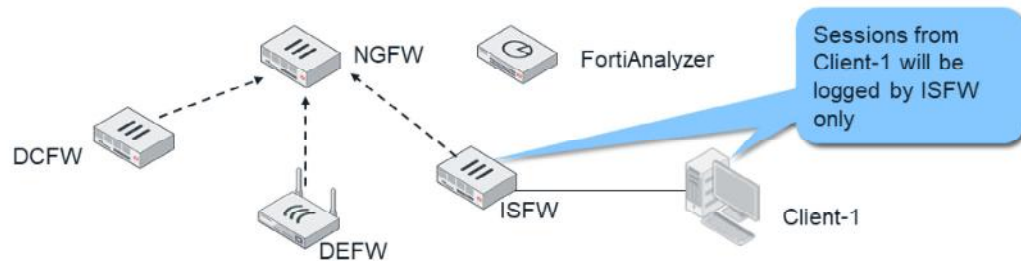
All FortiGate devices in the Security Fabric maintain their own Security Fabric map. Security Fabric maps include the MAC address and IP address of all connected FortiGate devices and their interfaces.

DO NOT REPRINT
© FORTINET

Security Fabric Logging

- Traffic logs are always enabled in all firewall policies
- The Security Fabric, as a whole, logs each session once
 - A session is logged by the first FortiGate that handles it in the Security Fabric
 - Any upstream FortiGate that is a member of the Security Fabric will not log traffic if it is coming from another member's MAC address.

Note: If upstream FortiGate performs NAT, then another log on that device will be generated.



FORTINET

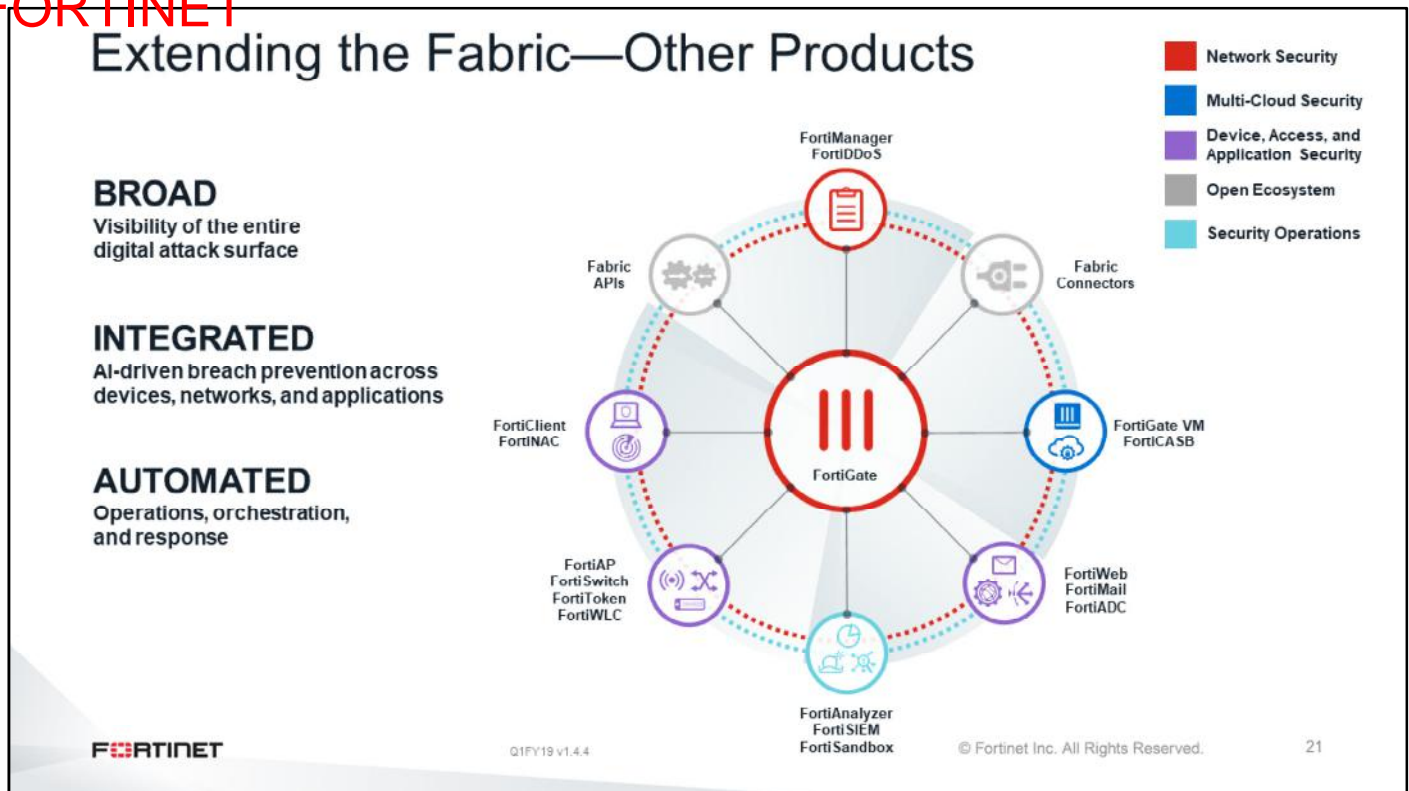
© Fortinet Inc. All Rights Reserved.

20

FortiGate devices in the Security Fabric know the MAC addresses of their upstream and downstream peers. If a FortiGate receives a packet from a MAC address that belongs to another FortiGate in the Security Fabric, it will not log that session. This helps to eliminate the repeated logging of a session by multiple FortiGate devices. A session is always logged by the first FortiGate that handled it in the Security Fabric.

One exception to the behavior is that if upstream FortiGate performs NAT, then another log will be generated. The additional log is needed to record NAT details such as translated ports and/or addresses.

DO NOT REPRINT
© FORTINET



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

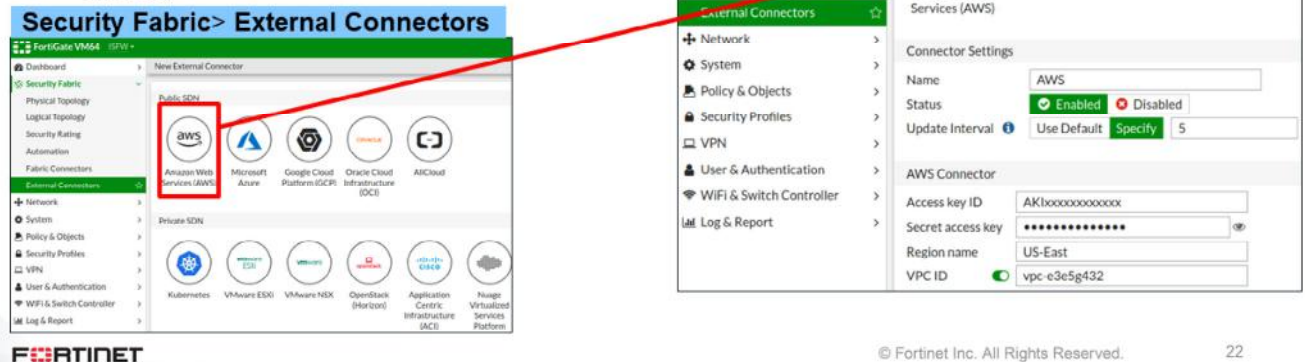
You can also extend the Security Fabric by integrating FortiMail, FortiWeb, and FortiClient EMS.

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

DO NOT REPRINT
© FORTINET

Extending the Fabric—Fabric Connectors

- Security Fabric multi-cloud support adds Security Fabric connectors to the Security Fabric configuration
- Allow you to integrate
 - Amazon Web Services (AWS)
 - Microsoft Azure
 - Oracle Cloud Infrastructure (OCI)
 - Google Cloud Platform (GCP)
 - AliCloud



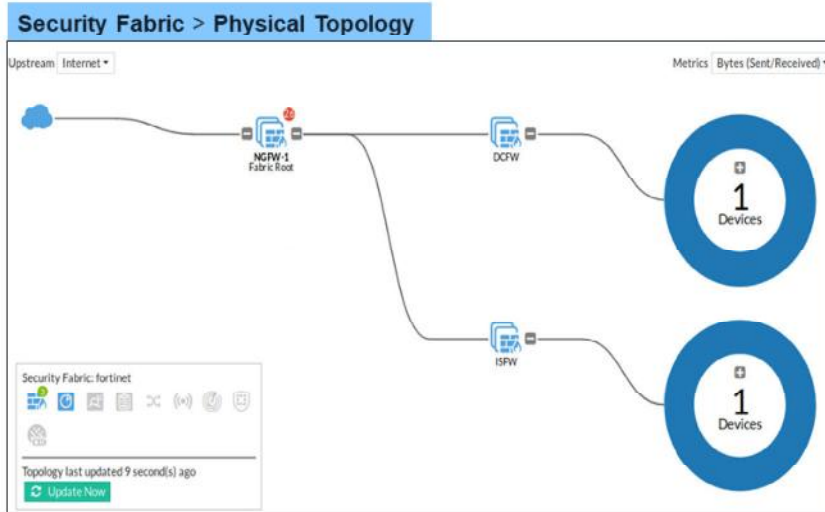
Fabric connectors allow you to integrate multi-cloud support, such as ACI and AWS, to name a few.

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

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

DO NOT REPRINT
© FORTINET

Topology Views



- Authorize or deauthorize access devices (FortiSwitch, FortiAPs)
- Ban or unban compromised clients
- Some device management tasks
 - Upgrade
 - Connect to device CLI

FORTINET

© Fortinet Inc. All Rights Reserved.

23

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

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

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

Only Fortinet devices are shown in the topology views.

Security Fabric Rating

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



FORTINET

© Fortinet Inc. All Rights Reserved.

24

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

- Security Posture
- Fabric Coverage
- Optimization

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

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

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

DO NOT REPRINT
© FORTINET

Security Posture



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

Security issues that are labelled as Apply can be resolved immediately

Identifies critical security gaps

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

The security posture service now supports the following:

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

DO NOT REPRINT
© FORTINET

Automation Stitches

AUTOMATION STITCH



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

Security Fabric > Automation

New Automation Stitch

Name:

Status: Enabled Unabled

FortiGate: All FortiGates

Trigger:

☐ Compromised Host
 ☐ Security Rating Summary
 ☐ Configuration Change
 ☐ Reboot
 ☐ License Expiry
 ☐ HA Failover
 ☐ AV & IPS DB Update
 ☐ FortiOS Event Log
 ☐ FortiAnalyzer Event Handler
 ☐ Incoming Webhook
 ☐ Schedule

Action:

☐ CLI Script
 ☐ Email
 ☐ FortiExplorer Notification
 ☐ AWS Lambda
 ☐ Azure Function
 ☐ Google Cloud Function
 ☐ AIOCloud Function
 ☐ Slack Notification
 ☐ Webhook

Minimum interval (seconds):

OK Cancel

FORTINET

© Fortinet Inc. All Rights Reserved.

26

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

Each automation pairs an event trigger and one or more actions, which allows you to monitor your network and take appropriate action when the Security Fabric detects a threat. 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 to make sure you don't receive repeat notifications about the same event.

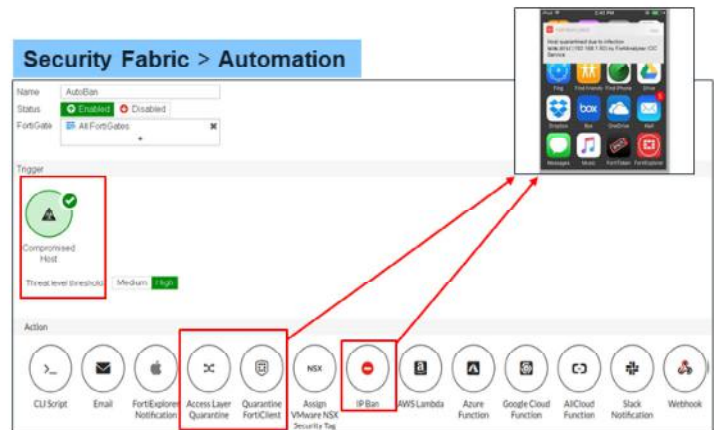
DO NOT REPRINT
© FORTINET

Automation Stitches—Compromised Host

QUARANTINE



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



FORTINET

© Fortinet Inc. All Rights Reserved.

27

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

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

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

DO NOT REPRINT
© FORTINET

Testing Stitches

- You can test stitches in the CLI

```
# diagnose automation test <stitch_name>
```
- When an automation stitch is triggered, FortiGate creates an event log

Log & Report > System Events

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

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Review the Enterprise Firewall solution
- ✓ Examine FortiGate deployment modes in an Enterprise Firewall solution
- ✓ Explore the Fortinet Security Fabric
- ✓ Diagnose the Security Fabric operation
- ✓ Perform a security rating audit
- ✓ Configure automation stitches

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

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

DO NOT REPRINT
© FORTINET

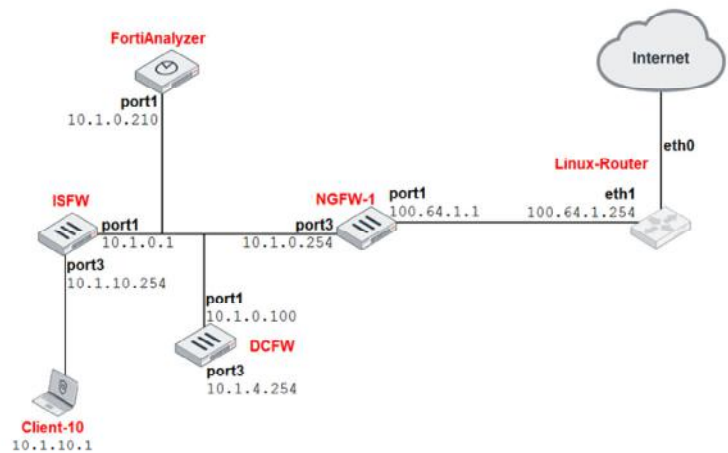
Lab 1—Security Fabric

Now, you will work on *Lab 1—Security Fabric*.

DO NOT REPRINT
© FORTINET

Lab 1—Security Fabric

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



FORTINET

© Fortinet Inc. All Rights Reserved.

31

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

DO NOT REPRINT
© FORTINET



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

DO NOT REPRINT
© FORTINET

Objectives

- Describe how FortiOS processes a packet
- Monitor process activity by using real-time debugs
- Describe how FortiOS uses memory
- Diagnose high memory and high CPU problems
- Diagnose conserve mode
- Optimize the memory usage
- Troubleshoot unexpected reboots and frozen units
- Use the crashlog for diagnostics
- Understand FortiOS workspace mode

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

By demonstrating competence in FortiOS architecture, you will be able to identify how FortiOS processes packets and uses memory. You will be able to also diagnose high resource utilization and conserve mode issues, and optimize memory usage.

DO NOT REPRINT
© FORTINET

Life of a Packet



In this section, you will learn about the life of a packet.

DO NOT REPRINT
© FORTINET

Parallel Path Processing

- Parallel path processing (PPP) chooses from a group of parallel options to identify the optimal path for processing a packet
- FortiGate can offload and accelerate many processes in hardware
 - Security processors (CP8 or CP9) offload traffic that requires UTM or NGFW processing
 - Network processors (NP6) offload traffic that does not require any UTM or NGFW processing
- FortiGate hardware and software configuration affect the path that a packet takes

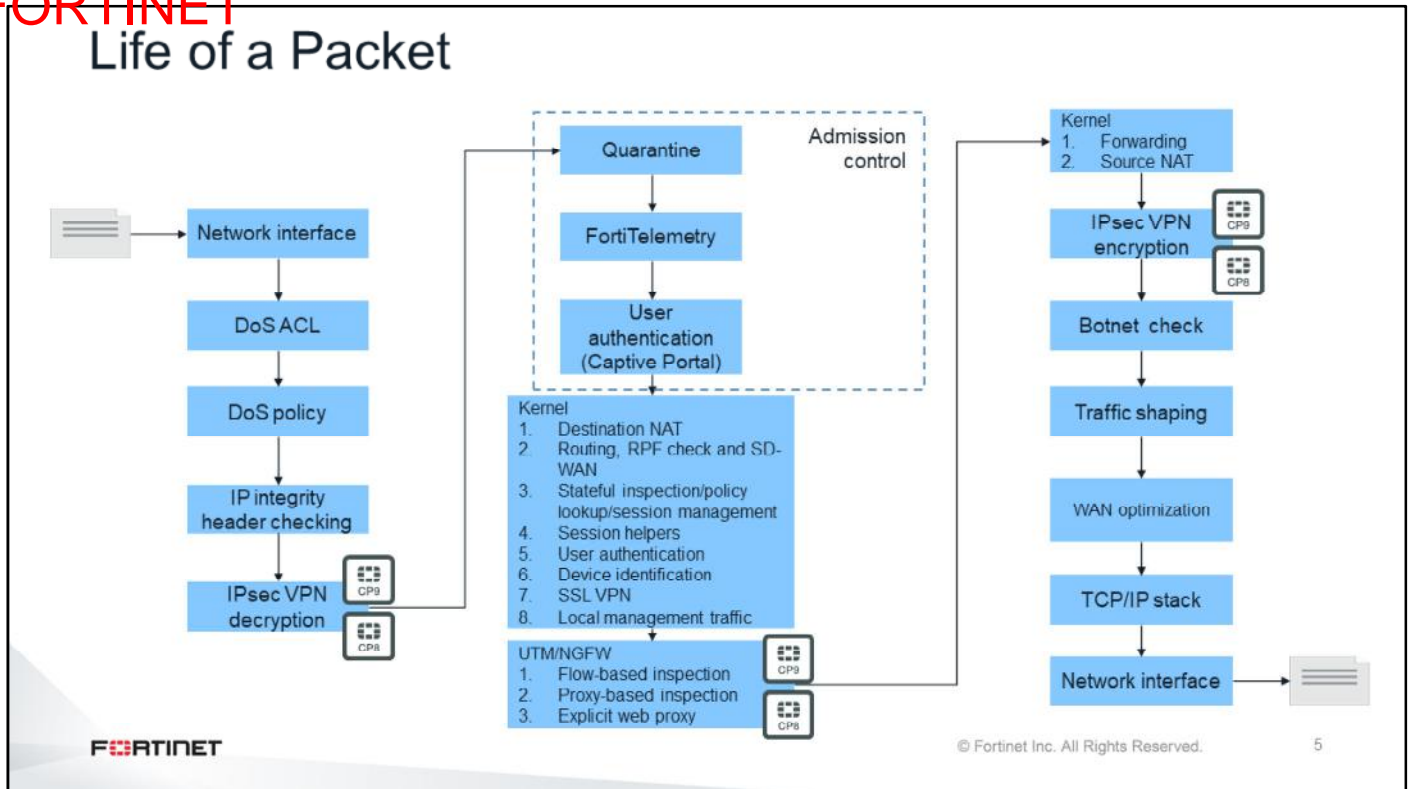


© Fortinet Inc. All Rights Reserved.

4

PPP uses the firewall policy configuration to choose from a group of parallel options to identify the optimal path for processing a packet. The path identified by PPP is made up of the various processes the packet must pass through. Hardware, such as CP8, CP9, or network processors, can offload and accelerate many of these processes. FortiGate hardware and software configuration affects the path that a packet takes.

DO NOT REPRINT
© FORTINET



This slide shows all the steps that a packet goes through as it enters, passes through, and exits FortiGate. This scenario is for FortiGate without network processors.

FortiGate performs some security inspections early in the life of the packet, such as DoS checking, reverse path forwarding (RPF) checking, and IP integrity header checking. FortiGate does this to make sure the packets are within acceptable parameters before allowing the packet to move through the rest of the processes.

FortiGate offloads IPsec VPN encryption and decryption, and flow-based inspection to SPUs if they exist on the FortiGate hardware. Additionally, some FortiGate models support network processors, such as the NP6 or NP6lite. FortiGate offloads packets that don't require any UTM or NGFW processing to these network processors for acceleration.

DO NOT REPRINT
© FORTINET

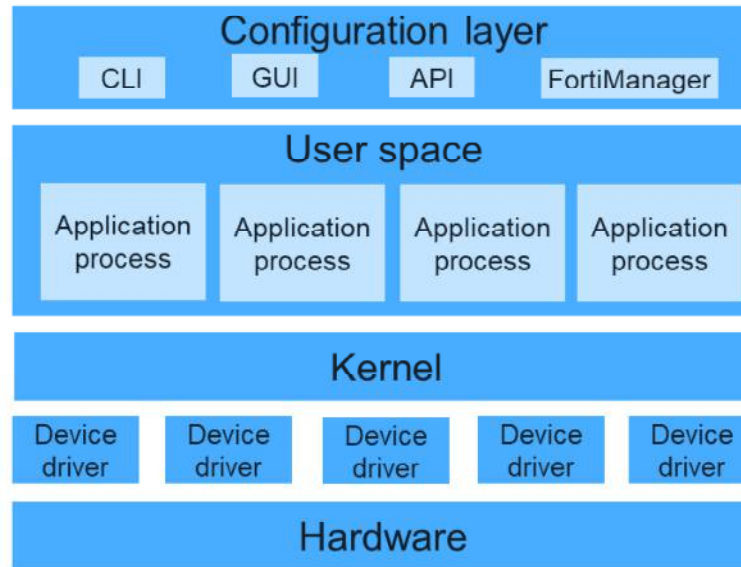
Memory Architecture

A large rectangular frame containing a stylized graphic. The graphic consists of several overlapping, semi-transparent triangular shapes in various shades of gray and light blue. These shapes are arranged to create a sense of depth and movement, with some pointing towards the top left and others towards the bottom right. The overall effect is abstract and modern, suggesting a complex architectural or technical structure.

In this section, you will learn about how FortiGate uses memory.

DO NOT REPRINT
© FORTINET

FortiOS Architecture



FORTINET

© Fortinet Inc. All Rights Reserved.

7

To understand how FortiGate uses its memory, you need to understand the architecture of FortiOS. The heart of FortiOS is its kernel. The kernel is where FortiGate makes some of the most basic and important decisions, such as how to route a packet, or when to offload a session to an NPU processor. FortiOS runs on hardware. The device drivers bridge the kernel with the hardware. The user space is located above the kernel. Several application processes or daemons run in the user space. Above the kernel and the user space is the configuration layer.

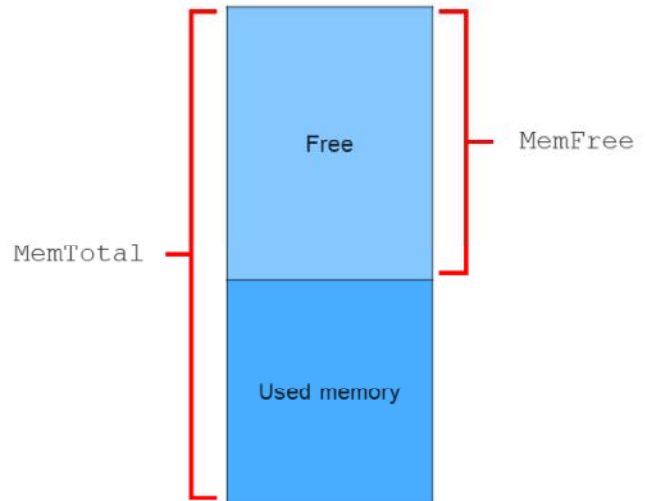
DO NOT REPRINT
© FORTINET

FortiGate Memory Segmentation

- Kernel accesses the entire system memory directly

```
# diagnose hardware sysinfo memory
```

```
MemTotal:      3112828 kB  
MemFree:       1680796 kB  
Buffers:       506548 kB  
Cached:        426892 kB  
SwapCached:    0 kB  
...
```



FORTINET

© Fortinet Inc. All Rights Reserved.

8

FortiOS is a 64-bit architecture, therefore the kernel doesn't need to use memory paging to access the whole memory space. All the memory space is directly accessible by the kernel.

The command shown on this slide displays:

- The total amount of system memory (MemTotal)
- The total amount of free memory (MemFree)

DO NOT REPRINT
© FORTINET

How the FortiGate Memory is Used

- Kernel memory slabs
- System I/O cache
- Buffers
- Shared memory
- Process memory

FORTINET

© Fortinet Inc. All Rights Reserved.

9

FortiGate allocates memory for five main purposes:

- Kernel memory slabs
- System I/O cache
- Buffers
- Shared memory
- Process memory

You will learn about each of these purposes in this lesson.

DO NOT REPRINT
© FORTINET

Slabs

- Collection of objects with a common purpose and a fixed size
- Used by kernel
- Examples:

Slab	Usage
tcp_session	TCP session
ip_session	Non-TCP session
ip_dst_cache	Route cache
buffer_head	Read/write data from disk, flash
inode_cache	Information about files and directories
dentry_cache	Cache for file system directory entries
arp_cache	Cache for ARP

FORTINET

© Fortinet Inc. All Rights Reserved.

10

The kernel memory slabs are collections of objects with a common purpose. They are used by the kernel to store information in memory.

This slide shows an example of some slabs. There are slabs for storing information about the TCP sessions. The entries in the route cache are also stored in memory slabs.

DO NOT REPRINT
© FORTINET

Slabs (Contd)

```
# diagnose hardware sysinfo slab
```

```
slabinfo - version: 2.1
```

# name	<active_objs>	<num_objs>	<objsize>	<objperslab>	<pagesperslab>	: tunables	<limit>	<batchcount> ...
tcp6_session	0	0	1344	3	1	: tunables	60	30
ip6_session	0	0	1200	3	1	: tunables	60	30
sctp_session	0	0	1536	5	2	: tunables	60	30
tcp_session	45	60	1408	5	2	: tunables	60	30
ip_session	37	39	1344	3	1	: tunables	60	30
fib6_nodes	10	59	64	59	1	: tunables	252	126
ip6_dst_cache	34	60	384	10	1	: tunables	124	62
ndisc_cache	3	24	320	12	1	: tunables	124	62
ip6_mrt_cache	0	0	128	30	1	: tunables	252	126
RAWv6	5	8	1024	4	1	: tunables	124	62
UDPLITEv6	0	0	1024	4	1	: tunables	124	62
UDFv6	7	0	1024	4	1	: tunables	124	62
tw_sock_TCPv6	0	0	320	12	1	: tunables	124	62
request_sock_TCPv6	0	0	192	20	1	: tunables	252	126
TCPv6	14	14	1792	2	1	: tunables	60	30
uhci_urb_priv	0	0	56	67	1	: tunables	252	126
...								

Active objects

Available objects

Object size

Total slab size = available objects x object size

FORTINET

© Fortinet Inc. All Rights Reserved.

11

To check how much memory is being allocated to kernel slabs, use the command shown on this slide.

The first column shows the slab name. The second column shows the total number of active objects, and the third and fourth columns show the number of available objects, and the size of each object.

You can calculate the total amount of memory allocated to each slab type by multiplying the number of available objects by their size.

You can use the output of this command to identify how much memory the session table is using. If that value is too high, it might indicate that the configuration needs some tuning (for example, setting shorter session TTLs), or that the FortiGate model is too small for the amount of traffic crossing the device.

DO NOT REPRINT
© FORTINET

System I/O Cache

- Speeds up hard disk and flash disk writing and reading operations:
 - Logging
 - WAN optimization
 - Explicit proxy
- Made of pages (4K size) of disk block (1K size)
- Two types of pages:
 - Active
 - Recently accessed
 - Inactive
 - Not used after some time
 - Might be reclaimed by the kernel in case of shortage

FORTINET

© Fortinet Inc. All Rights Reserved.

12

There are no direct reads and writes made to hard disks or flash disks. Each access is done through a cache held in memory—the system I/O cache.

The system I/O cache is used to speed up the access to information stored in the hard and flash disk memories. Some processes, such as logging, WAN optimization, and explicit proxy, store information in the hard disk, so they get the performance boost provided by this memory allocation.

An I/O cache page is labeled as active when it has been recently been used or modified. It enters the inactive state after it has not been used for some time. An inactive page may be reclaimed by the kernel if needed.

DO NOT REPRINT
© FORTINET

System I/O Cache (Contd)

```
# diagnose hardware sysinfo memory
```

```
...
```

```
Cached: 1137808 kB
```

```
SwapCached: 0 kB
```

```
Active: 568600 kB
```

```
Inactive: 569208 kB
```

```
...
```

FORTINET

© Fortinet Inc. All Rights Reserved.

13

The command shown on this slide displays the total amount of memory allocated for the I/O cache. The cache value is the overall sum of all active and inactive pages.

DO NOT REPRINT
© FORTINET

Shared Memory

- Allocated dynamically
- Allows the sharing of information among multiple processes

```
# diagnose hardware sysinfo shm
SHM FS total:      1001861120      955 MB
SHM FS free:       947621888       903 MB
SHM FS avail:      947621888       903 MB
SHM FS alloc:      54239232        51 MB
```

FORTINET

© Fortinet Inc. All Rights Reserved.

14

Above the kernel layer there are multiple application processes or daemons running. The operating system allocates separate blocks of memory to each process. A process can access the memory that was allocated to it, but it cannot access the memory that was allocated to any other process. So, a process cannot share information with another process by reading or writing data into the memory allocated to that other process. For that purpose, the operating system dynamically allocates shared memory (SHM). Multiple processes can access the SHM, allowing them to share information.

DO NOT REPRINT
© FORTINET

Process CPU Usage

```
# diagnose sys top [refresh_time_sec] [number_of_lines]
```

```
Run Time: 1 days, 3 hours and 35 minutes
```

```
OU, ON, OS, 100I, OWA, OHI, OSI, OST; 995T, 202F
```

newcli	520	R	0.3	2.2
sshd	518	S	0.1	1.2
fsd	90	S	0.1	1.1
ipsengine	99	S	0.0	5.5
miglogd	41	S	0.0	4.8
pyfcgid	432	S	0.0	3.9
httpsd	102	S	0.0	3.3
pyfcgid	435	S	0.0	3.0
updated	75	S	0.0	2.4
cmdbsvr	25	S	0.0	2.3

Press Shift+P to sort by CPU usage. Press Shift+M to sort by memory usage.

Process ID

State

CPU

Memory

FORTINET

© Fortinet Inc. All Rights Reserved.

15

This slide shows how you can see how much memory space is being used by each process. The command shown on this slide displays the information shown in the last column. For each process, the command also displays the ID number, state, and CPU use. You can specify the refresh frequency and the number of lines to display.

While the command is running, you can press Shift+P to sort the processes by CPU use, or Shift+M to sort them by memory use. To stop the command, press Ctrl+C or Ctrl+Q.

DO NOT REPRINT
© FORTINET

Most Common Processes

Name	Description
cmdbsrv	Applies configuration changes
miglogd	Logs collection, and automation stitches
httpsd	GUI access
sslvpn	SSL VPN
updated	FortiGuard updates
wad	WAN optimization, explicit proxy, proxy-based inspection for HTTP and HTTPS, and FTP
scanunitd	File scanning
iked	IPsec

The table on this slide shows some of the most common processes.

DO NOT REPRINT
© FORTINET

Most Common Processes (Contd)

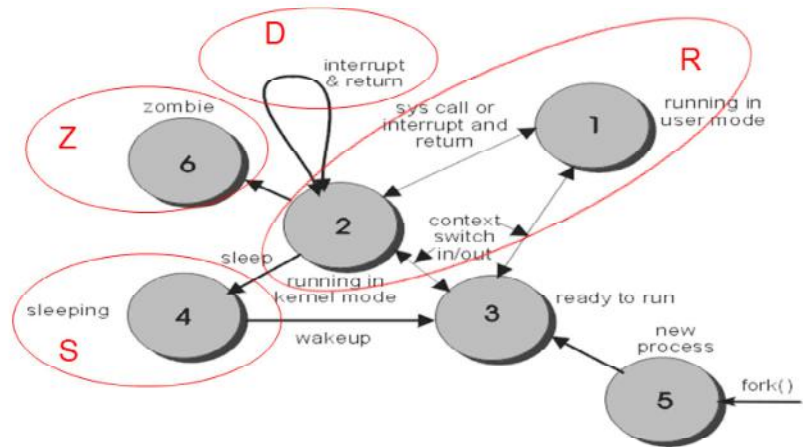
Name	Description
pppoed	PPPoE protocol
hataalk, hasync	HA protocol and synchronization
pptpd, l2tps	PPTP and L2TP protocols
urlfilter	FortiGuard web filtering
authd	User authentication
fssod	FSSO
proxyworker	Proxy-based inspection for IMAP, POP, SMTP

The table on this slide shows more of the most common processes.

DO NOT REPRINT
© FORTINET

Process States Review

- States:
 - S: Sleeping
 - R: Running
 - D: Do not disturb
 - Z: Zombie
- Normal states:
 - S, R, and D (for a short time)
- Abnormal state:
 - Z and D (if not for a short time)



FORTINET

© Fortinet Inc. All Rights Reserved.

18

The command `diagnose sys top` shows the state of each process. A process can be in one of four states: sleeping (S), running (R), do not disturb (D), or zombie (Z).

The S and R states are normal. It is also normal if a process goes briefly to the D state. The Z state is not normal. Also, it is not normal if a process stays in the D state for a long time. This usually indicates that the process is not working properly.

DO NOT REPRINT
© FORTINET

General System Troubleshooting Commands

In this section, you will learn about general system troubleshooting commands.

DO NOT REPRINT
© FORTINET

System Information

```
# get system status
Version: FortiGate-VM64 v6.4.0,build1579,200330 (GA)
Virus-DB: 76.00683(2020-04-13 15:20)
Extended DB: 76.00683(2020-04-13 15:20)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 15.00815(2020-04-10 01:10)
APP-DB: 15.00815(2020-04-10 01:10)
INDUSTRIAL-DB: 15.00814(2020-04-09 00:21)
Serial-Number: FGVM010000077649
IPS Malicious URL Database: 2.00609(2020-04-10 04:34)
License Status: Warning
VM Resources: 1 CPU/1 allowed, 2154 MB RAM
Log hard disk: Available
Hostname: NGFW-1
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: 1579
Release Version Information: GA
FortiOS x86-64: Yes
System time: Mon Apr 27 21:19:31 2020
```

FORTINET

© Fortinet Inc. All Rights Reserved.

20

The command shown on this slide is usually one of the first debug commands that you use when troubleshooting. The output shows the firmware version, FortiGuard database versions, license status, operation mode, number of VDOMs, and system time.

DO NOT REPRINT
© FORTINET

Resource Usage

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2206640k total, 910020k used (41.2%), 1104740k free (50.1%), 191072k
freeable (8.7%)
Average network usage: 4 / 4 kbps in 1 minute, 6 / 6 kbps in 10 minutes, 16 /
20 kbps in 30 minutes
Average sessions: 22 sessions in 1 minute, 31 sessions in 10 minutes, 33
sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions
per second in last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days, 9 hours, 59 minutes
```

FORTINET

© Fortinet Inc. All Rights Reserved.

21

The command shown on this slide displays overall memory and CPU use. It also shows session creation rate, number of viruses caught, and number of attacks blocked by the IPS. The last line displays the system uptime. This output gives you a quick view of how much traffic the device is handling.

DO NOT REPRINT
© FORTINET

Real-Time Application Debug

- To enable most of the real-time debugs:

```
# diagnose debug application <application> <debug_level>
# diagnose debug enable
```
- Some applications (daemons) that can be debugged in real time:
 - sslvpn SSL VPN
 - ike IPsec VPN
 - authd User authentication
 - update FortiGuard updates
- Debug level:
 - 0: Disable the specific debug
 - Other values: outputs vary depending on the daemon
 - -1: Enable all outputs

FORTINET

© Fortinet Inc. All Rights Reserved.

22

The real-time debug commands generate information in real time about what a specific FortiGate process or feature is doing.

The debug level is a bitmask value that specifies which types of messages are displayed. The meaning of the debug value depends on each process. However, for all cases, a debug level of 0 means no output (disabled) and a debug level of -1 means enabling all possible message types.

DO NOT REPRINT
© FORTINET

Real-Time Application Debug (Contd)

- Example, for IPsec real-time debug:
diagnose debug application ike -1
diagnose debug enable
- Enable timestamp:
diagnose debug console timestamp enable
- Remember to disable the debug after troubleshooting:
diagnose debug application ike 0
diagnose debug disable
- Disable all application debugging
diagnose debug reset



© Fortinet Inc. All Rights Reserved.

23

This slide shows the two commands you use to enable the IPsec real-time debug output. You can also enable the option to prepend the system time to each debug line. It's important to disable any real-time debug after using it because they consume FortiGate resources and some can be CPU intensive.

DO NOT REPRINT
© FORTINET

Application Layer Test Commands

```
# diagnose test application ?  
mm17          MM1/MM7 proxy.  
smtp          SMTP proxy.  
ftpd          FTP proxy.  
pop3          POP3 proxy.  
imap          IMAP proxy.  
nntp          NNTP proxy.  
forticldd     FortiCloud daemon.  
miglogd       Miglog logging daemon.  
urlfilter     URL filter daemon.  
ipsmonitor    ips monitor  
ipsengine     ips sensor  
ipldbd        IP load balancing daemon.  
.....
```

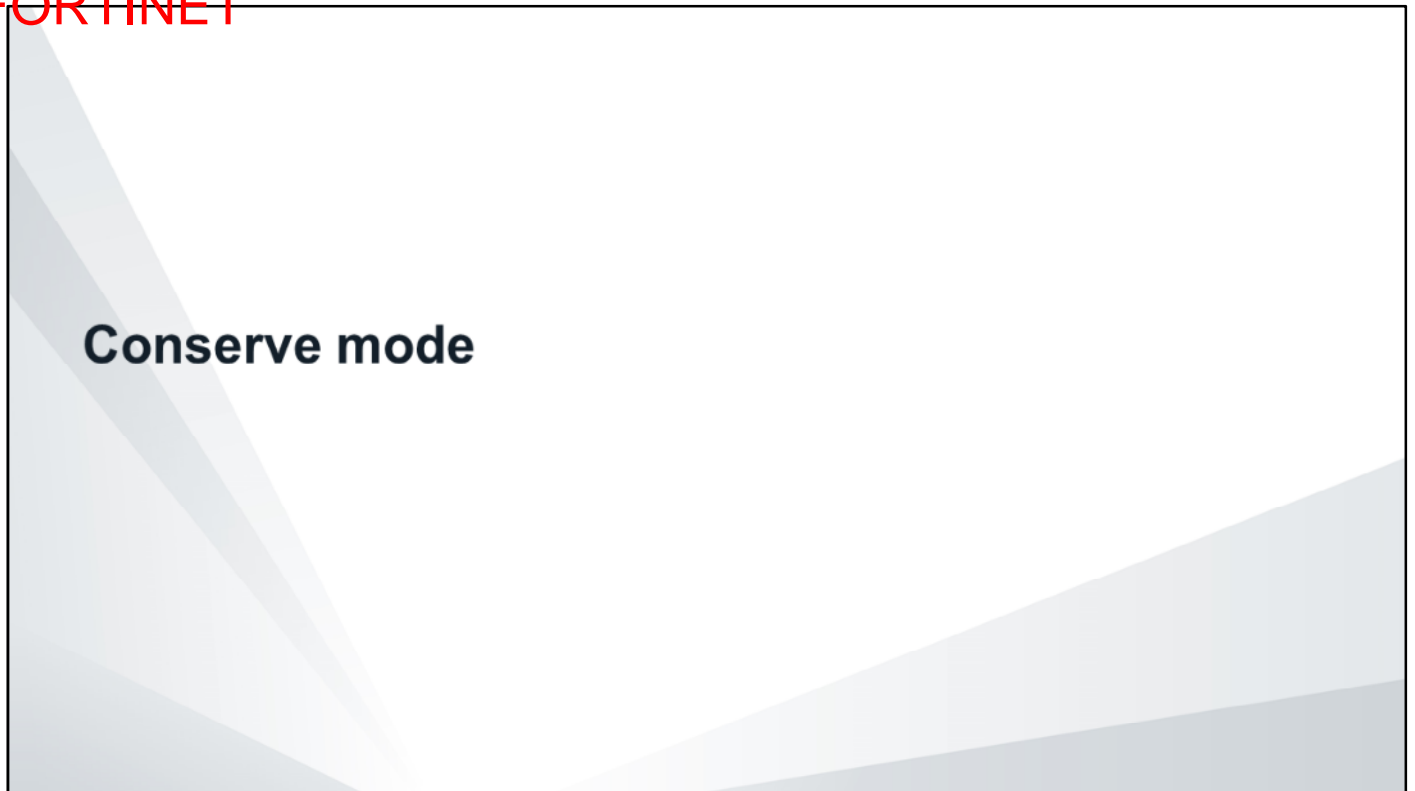
FORTINET

© Fortinet Inc. All Rights Reserved.

24

Application layer test commands don't display information in real time, but they do show statistics and configuration information about a feature or process. You can also use some of these commands to restart a process or execute a change in its operation.

DO NOT REPRINT
© FORTINET



In this section, you will examine conserve mode, now that you have a better understanding of how FortiGate uses memory.

DO NOT REPRINT
© FORTINET

Conserve Mode

- Triggered based on memory use
 - Prevents using so much memory that FortiGate becomes unresponsive
 - FortiGate leaves conserve mode as memory use goes below set threshold
- Three memory thresholds that you can configure on the CLI
 - Extreme: threshold at which FortiGate starts dropping new sessions
 - Red: threshold at which FortiGate enters conserve mode
 - Green: threshold at which FortiGate exits conserve mode

FORTINET

© Fortinet Inc. All Rights Reserved.

26

Conserve mode is a protection mechanism that is triggered when FortiGate doesn't have enough memory available to handle traffic. Content inspection (especially proxy-based) increases memory use beyond simple firewall policies. In other words, when antivirus is enabled, FortiGate is more likely to use more memory, which can cause FortiGate to enter conserve mode. You can identify whether antivirus or any other process is using too much memory by running the CLI command `diagnose sys top`.

FortiGate has only one conserve mode. It is triggered based on memory usage. There are three memory thresholds that you can configure on the CLI:

- Extreme: threshold at which FortiGate starts dropping new sessions
- Red: threshold at which FortiGate enters conserve mode
- Green: threshold at which FortiGate exits conserve mode

DO NOT REPRINT
© FORTINET

Conserve Mode Thresholds

```
# config system global
...
set memory-use-threshold-extreme 95
set memory-use-threshold-red 88
set memory-use-threshold-green 82
...
end
```

Default
threshold values

You can use the commands shown on this slide to change the default conserve mode threshold values.

DO NOT REPRINT
© FORTINET

Conserve Mode Logs

Log & Report > Events > System Events

#	Level	User	Message	Log Description
1	*****		Kernel enters memory conserve mode	Memory conserve mode entered

Log Details	
General	
Date	2020/04/28
Time	11:12:59
Virtual Domain	root
Log Description	Memory conserve mode entered
Source	
User	
Application Control	
Service	kernel
Security	
Level	*****
Cellular	
Service	kernel
Event	
Message	Kernel enters memory conserve mode
Other	
Log ID	0100022011
Type	event
Sub Type	system
Log event original timestamp	1588097579088056000
Timezone	-0700
Conserve	on
Total	1000
Used	858
Red	800 MB
Green	750 MB

- Crash log:

```
# diagnose debug crashlog read
...
2020-04-28 11:12:59 logdesc="Memory conserve mode
entered" service=kernel conserve-on total="1234 MB"
used="878 MB" red="876 MB" green="864 MB" msg="Kernel
enters memory conserve mode"
...
```

FORTINET

© Fortinet Inc. All Rights Reserved.

28

This slide shows the entries that are generated in the event logs when FortiGate enters memory conserve mode. If the GUI is under a heavy load, it may be unresponsive, making the GUI logs inaccessible. In this case, you can view the crash log on the CLI for conserve mode messages. This slide shows an example of a typical conserve mode crash log entry.

DO NOT REPRINT
© FORTINET

Proxy Inspection While in Conserve Mode

- Antivirus failopen governs FortiGate behavior for proxy-based inspection while in conserve mode

```
config system global
    set av-failopen {off | one-shot | pass}
    set av-failopen-session {enable | disable}
end
```

- `av-failopen-session` - Enable or disable failopen
 - Default setting is `disable`
- `av-failopen` - Configure *how* sessions failopen
 - `off` – All new sessions that require content inspection are dropped, but existing sessions are still processed
 - `pass` – Stops inspecting new sessions. Inspection is automatically restarted when FortiGate exits conserve mode.
 - `one-shot` – Similar to `pass`, but you must manually change the `av-failopen` setting to restart inspection after FortiGate exits conserve mode

FORTINET

© Fortinet Inc. All Rights Reserved.

29

Use the commands shown on this slide to control how FortiGate handles traffic that requires proxy-based content inspection during conserve mode.

There are two settings—`av-failopen-session` and `av-failopen`. When `av-failopen-session` is enabled, FortiGate applies the action configured in `av-failopen`. By default, FortiGate blocks new sessions (`av-failopen-session disable`).

DO NOT REPRINT
© FORTINET

Flow Inspection While in Conserve Mode

- IPS failopen governs FortiGate behavior for flow-based inspection while in conserve mode

```
config ips global
    set fail-open {enable | disable}
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

30

All flow-based inspection is handled by the IPS engine. You can configure the IPS failopen setting to manage flow-based inspection while FortiGate is in conserve mode.

When you have mixed UTM profiles using proxy-based inspection, and flow-based inspection is enabled on FortiGate, nTurbo does not work. In this case, all the packets for flow-based inspection need to go through the socket buffer and deliver to IPS. When the socket buffer is full, the event is logged as a fail-open event and sessionact is used to reflect the fail-open settings. By default, IPS fail-open is disabled, which means the IPS engine will drop all new sessions that require flow-based inspection, but will try to process all existing sessions. If IPS fail-open is enabled, IPS engine will not perform any scan, but will allow new packets.

If you have all flow based UTM profiles, nTurbo handles all packets, except the three-way handshake, and it does not require any software socket buffer.

DO NOT REPRINT
© FORTINET

Conserve Mode Diagnostics

```
# diagnose hardware sysinfo conserve
```

```
memory conserve mode: off
total RAM: 3039 MB
memory used: 817 MB 26% of total RAM
memory freeable: 582 MB 19% 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
```

FORTINET

© Fortinet Inc. All Rights Reserved.

31

The command shown on this slide is used to identify if a FortiGate device is currently in conserve mode.

DO NOT REPRINT
© FORTINET

Memory Tension Drops

- Kernel deletes oldest sessions if it cannot allocate more memory pages
- No direct link with conserve mode

```
# diagnose sys session stat
misc info:      session_count=184 setup_rate=0 exp_count=0 clash=0
                memory tension drop=0 ephemeral=0/196608 removeable=0
                npu_session_count=61
                nturbo_session_count=0
delete=0, flush=87, dev_down=16/120 ses_walkers=0
TCP sessions:
    38 in ESTABLISHED state
    1 in CLOSE_WAIT state
```

FORTINET

© Fortinet Inc. All Rights Reserved.

32

FortiGate has one more mechanism to free memory when there is not much available. If the kernel cannot allocate more memory pages, it deletes the oldest sessions. The command shown on this slide displays the numbers of sessions deleted by the kernel because of this mechanism.

DO NOT REPRINT
© FORTINET

Ephemeral Drops

- A session is categorized as ephemeral when one of the following is true:
 - A TCP session is not fully established
 - A UDP with only a single packet is received
- These types of open sessions are common types of DoS attacks
- To protect memory usage, FortiOS sets a limit on the total number of ephemeral sessions (based on the model)

```
# diagnose sys session stat
misc info:      session_count=184 setup_rate=0 exp_count=0 clash=0
                memory_tension_drop=0 ephemeral=0/196608 removeable=0
                npu_session_count=61
                nturbo_session_count=0
delete=0, flush=87, dev_down=16/120 ses_walkers=0
TCP sessions:
    38 in ESTABLISHED state
    1 in CLOSE_WAIT state
```

FORTINET

© Fortinet Inc. All Rights Reserved.

33

FortiGate has a mechanism to protect memory use against some forms of DoS attacks. FortiGate categorizes an entry in the session table as an ephemeral session when it is a TCP session that is not fully established (three-way handshake not completed), or it is a UDP session with only one packet received. During some DoS attacks, the number of these types of sessions tends to increase abnormally, potentially consuming the unit memory. FortiGate sets a hard limit on the maximum number of ephemeral sessions that can simultaneously exist in the session table.

DO NOT REPRINT
© FORTINET

Memory Usage Optimization

What can you do if FortiGate enters conserve mode frequently, or if its memory utilization is too high? In this section, you will learn how to optimize memory use by fine-tuning the FortiGate configuration.

DO NOT REPRINT
© FORTINET

Memory Usage Optimization

- Disable features that are not required:
 - Inspection of specific protocols (HTTP, FTP, SMTP, POP, IMAP)
 - Logging to memory
 - DHCP server
 - Some IPS signatures
- Reduce the maximum file size to inspect (default 10MB):

```
config firewall profile-protocol-options
  edit <profile_name>
    config [http|ftp|pop3|smtp|imap]...
      set oversize-limit <MB>
    end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

35

Many FortiGate processes, such as DLP or AV scanning, are memory intensive. So, memory optimization is important, especially in small devices, to guarantee that these processes will not force FortiGate into memory conserve mode. This slide shows some recommendations for optimizing memory use. These tips might significantly increase the available memory in a device that is frequently entering conserve mode.

The first and most logical step is to disable features that are not required. For example, if the network already has a FortiMail device doing antispam, an administrator does not need to do antispam on FortiGate. Also, usually not all the IPS signatures are required.

Another recommendation is to reduce the maximum file size to inspect, which is set to 10MB by default. You can reduce this value to 2 or 3MB without significantly reducing the virus catching rate, as a typical virus size is less than 1MB.

DO NOT REPRINT
© FORTINET

Memory Usage Optimization (Contd)

- Reduce the FortiGuard cache TTL (default 3600 and 1800 seconds):

```
config system fortiguard
  set webfilter-cache-ttl 500
  set antispam-cache-ttl 500
end
```

- Reduce DNS cache (default 1800 seconds):

```
config system dns
  set dns-cache-ttl 300
end
```



© Fortinet Inc. All Rights Reserved.

36

Additionally, you can reduce the amount of memory allocated to some caches, such as the ones for FortiGuard and DNS.

DO NOT REPRINT
© FORTINET

Memory Usage Optimization (Contd)

- Reduce the session time to live (TTL)
 - Globally:
 - For TCP (default to 3600 seconds):


```
config system session-ttl
  set default 300
```
 - For UDP (default to 180 seconds):


```
config system global
  set udp-idle-timer 90
```
 - For each service:


```
config system session-ttl
  config port
    edit <id>
      set protocol <IP_protocol>
      set start-port <start_port>
      set end-port <end_port>
      set timeout 300
```

FORTINET

© Fortinet Inc. All Rights Reserved.

37

The FortiGate session table can consume an important portion of memory, especially in networks with a high rate of traffic. By default, a session without traffic remains in the table for up to one hour.

Although a TTL this high might be required by some applications, in most networks, you can reduce the session TTL. When you reduce the TTL, FortiGate ages out idle sessions much quicker, increasing the amount of available memory.

There are four places in the FortiGate configuration where you can reduce the session TTL. Two of them are:

- Globally, for all the traffic
- On an IP protocol and port number basis

DO NOT REPRINT
© FORTINET

Memory Usage Optimization (Contd)

- Reduce the session TTL (default 3600 seconds)

- For each firewall policy:

```
config firewall policy
edit <id>
set session-ttl 300
```

- Per application control

Security Profiles > Application Control

Application and Filter Overrides

+ Create New

Edit

Delete

Priority	Details	Type	Action
1	Outlook.Anywhere	Application	✓ Allow

Policy & Objects > Firewall Policy

port3 → port1	1	10.1.10.	all	always	ALL	✓ ACCEPT	✗ Disabled	APP default	SSL certificate-inspection	✓ All
---------------	---	----------	-----	--------	-----	----------	------------	-------------	----------------------------	-------

FORTINET

© Fortinet Inc. All Rights Reserved.

38

The other two places where you can reduce the session TTL are:

- For each firewall policy
- For each application control

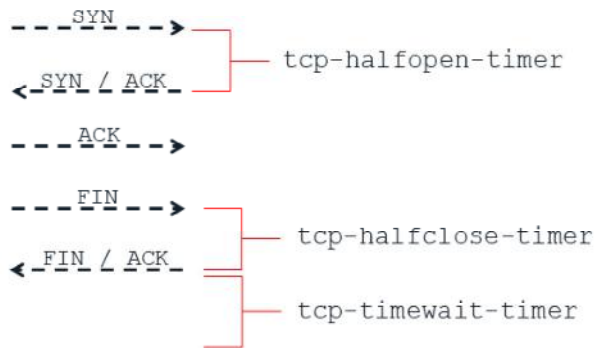
If an application requires a high session TTL, you can reduce the TTL globally, to five minutes. However, you can also set it to a higher number for the specific application port number or firewall policy.

DO NOT REPRINT
© FORTINET

Memory Usage Optimization (Contd)

- Reduce TCP session timers:

```
config system global
  set tcp-halfclose-timer 30    (default 120)
  set tcp-halfopen-timer 8      (default 10)
  set tcp-timewait-timer 1      (default 1)
end
```



FORTINET

© Fortinet Inc. All Rights Reserved.

39

You can also reduce most TCP session timers from their default values without causing problems to the applications. This slide shows some recommended values that are equal to or below the default values. Use these recommended values to optimize the memory use.

The `tcp-halfopen-timer` controls for how long, after a SYN packet, a session without SYN/ACK remains in the table.

The `tcp-halfclose-timer` controls for how long, after a FIN packet, a session without FIN/ACK remains in the table.

The `tcp-timewait-timer` controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

DO NOT REPRINT
© FORTINET



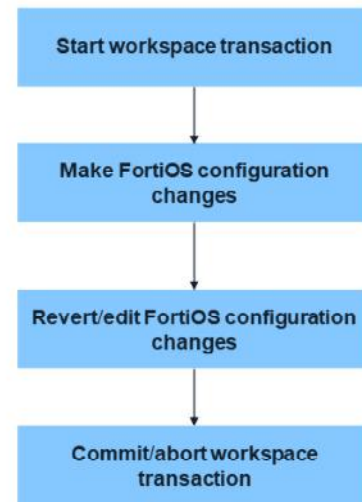
Workspace Mode

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

DO NOT REPRINT
© FORTINET

Workspace Mode

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



FORTINET

© Fortinet Inc. All Rights Reserved.

41

Workspace mode allows administrators to make a batch of changes that are not implemented until the transaction is committed. Prior to committing, the changes can be reverted or edited as needed without impacting current operations.

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

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

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

Workspace mode is only available from the FortiGate CLI.

DO NOT REPRINT
© FORTINET

Diagnosing Workspace mode

```
# diagnose sys config-transaction status
```

```
The CLI is running config transaction (id=1)
```

Transaction ID

Admin user

```
# diagnose sys config-transaction show txn-info
```

```
txn_id=1, expire=12 seconds, user='admin', userfrom='ssh(10.1.10.1)',  
cliCmd_ipath='/dev/cmdb/txn/4_Edc9G.conf'
```

```
config transaction id=1 will expire in 10 seconds
```

```
config transaction id=1 has expired
```

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

```
# diagnose sys config-transaction show txn-cli-commands
```

```
config system global
```

```
set hostname "NewHostname"
```

Changes pending to be
committed

```
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

42

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

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

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

DO NOT REPRINT
© FORTINET

Troubleshooting System Crashes

In this section, you will learn how to troubleshoot system crashes.

DO NOT REPRINT
© FORTINET

Console Logging

- Available only on some models
- Records console CLI output in a 4MB log file on flash memory
- Useful for troubleshooting unexpected restarts and unresponsive devices
- Can be displayed on the CLI or downloaded from the GUI
- To enable or disable console logging (disabled by default):

```
# diagnose debug comlog < enable | disable >
```
- To read console logging:

```
# diagnose debug comlog read
```
- To clear console logging:

```
# diagnose debug comlog clear
```
- To display the console logging settings:

```
# diagnose debug comlog info
```

FORTINET

© Fortinet Inc. All Rights Reserved.

44

On some FortiGate models, you can configure the device to store all console logs in the flash memory. This is especially useful when troubleshooting unexpected restarts and devices that randomly become unresponsive. Once FortiGate stores the logs, you can display them on the CLI, or download them from the GUI, for further analysis.

This slide shows the commands for enabling, displaying, and clearing the console logs.

DO NOT REPRINT
© FORTINET

Troubleshooting Unexplained Restarts

- A crashdump message is usually generated through the console
- After an unexpected restart, check:
 - Logs
 - Console logs (available in some models)
 - Crashlog
- If the model does not support console logs, keep a laptop connected to the console port and capture the crashdump

FORTINET

© Fortinet Inc. All Rights Reserved.

45

A crashdump message is usually generated through the console port when the device crashes. Crashdump messages can provide useful information to Fortinet developers. If the problem is a FortiGate that is restarting unexpectedly, you should check the logs, the console logs, and the crashlog. If the FortiGate model doesn't support a console log, keep a laptop connected to the console port and wait until another crash happens.

DO NOT REPRINT
© FORTINET

Troubleshooting a Device That Freezes

- Keep a laptop connected to the console port
- In multi-CPU platforms, enable NMI watchdog:
 - # `diagnose sys nmi-watchdog enable`
 - (Crashes the system if it has not scheduled any daemon in 10 minutes)
- After the device freezes, push the NMI button while the laptop is connected to generate the crashdump
 - Not all FortiGate models have an NMI button

FORTINET

© Fortinet Inc. All Rights Reserved.

46

A FortiGate *freezes* when it stops handling traffic, you cannot connect to it, and you can't access its console port. Only power cycling fixes the issue. In these cases, you could capture any crashdump in the console port. Additionally, and in the case of models with more than one CPU, you can enable the NMI watchdog feature, which automatically causes a crash in the system (and forces the crashdump) when no new daemons have been scheduled in the last 10 minutes. This is an indication that the unit is not operating normally and might be frozen.

Some FortiGate models also have an external NMI button. If the device is frozen and no crashdump has been generated, you can press the NMI button to force a crash and generate a crashdump.

DO NOT REPRINT
© FORTINET

Crashlog

```
# diagnose debug crashlog read
21:31:52 <03689> firmware FortiGate-VM64 v6.4.0,build1579b1579,200330(GA) (Release)
21:31:52 <03689> application sslvpnd
21:31:52 <03689> *** signal 11 (Segmentation fault) received ***
21:31:52 <03689> Register dump:
21:31:52 <03689> RAX: ffffffff00000000 RBX: 000000000000da4850
21:31:52 <03689> RCX: ffffffff00000000 RDX: 0000000000000400
21:31:52 <03689> R08: 0000000000000000 R09: 0000000000000000
21:31:52 <03689> R10: 000000000000007d0 R11: 00000000000003246
21:31:52 <03689> R12: 0000000000bd38fd0 R13: 0000000000000000
21:31:52 <03689> R14: 00007ffff7bc6420 R15: 0000000000000000
21:31:52 <03689> RSI: 000000000bdeb370 RDI: 000000000000000a
21:31:52 <03689> RBP: 00007ffff7bc6070 RSP: 00007ffff7bc6038
21:31:52 <03689> RIP: 00007fde3bbffde0 EFLAGS: 00000000000003246
21:31:52 <03689> CS: 0033 FS: 0000 GS: 0000
21:31:52 <03689> Trap: 0000000000000000 Error: 0000000000000000
21:31:52 <03689> OldMask: 0000000000000000
21:31:52 <03689> CR2: 0000000000000000
21:31:52 <03689> stack: 0x7ffff7bc6038 - 0x7ffff7bc7430
21:31:53 the killed daemon is /bin/sslvpnd: status=0x0
```

Application name

Termination signal

FORTINET

© Fortinet Inc. All Rights Reserved.

47

Each time an application crashes, or closes, an entry is generated in the crashlog. When an application crashes, the entry contains the name of the application, the time it crashed, and the termination signal.

This slide shows a sample of a crash in the crashlog. In this example, the application that failed was the `sslvpnd` process, which manages SSL VPN connections. The termination signal is 11, which is a segmentation fault.

DO NOT REPRINT
© FORTINET

Termination Signals

- Any time a process closes, a crash log is generated

```
# diagnose sys kill <termination_signal> <process_id>
```

Signal number	Description
4	Illegal instruction
6	Abort command from FortiOS
7	Bus error
9	Unconditional kill
11	Invalid memory reference
14	Alarm clock
15	Graceful kill

The table shown on this slide contains the most common termination signal numbers. Any administrator can manually kill a process by using the command shown on this slide, followed by the termination signal number, and the process ID. The command `diagnose sys top` lists the process ID numbers. Manually killing a process is not usually required under normal circumstances. If you have to kill a process, use the termination signal 9. Improperly killing a process can make a FortiGate system unstable.

Please note that not all the signal numbers will generate a crash log.

DO NOT REPRINT
© FORTINET

Crashlog Tips

- In most cases, entries in the crashlog are normal
- A crashlog can be considered suspicious when:
 - It happens at the same time as an abnormal FortiGate behavior
 - For example, unexpected system restarts
 - The crashed process is related to the FortiGate feature that failed
 - For example a crash in the `sslvpn` process when all SSL VPN connections went down
- The crashlog can provide information to Fortinet developers about the crash cause

FORTINET

© Fortinet Inc. All Rights Reserved.

49

So, how do you know if the crashlog is normal or not?

In most cases, entries in the crashlog *are* normal. A crashlog entry can be considered suspicious if it happens at the same time as a failure in a FortiGate feature, or abnormal behaviour of the FortiGate.

For example, a crashlog entry that is generated when the device unexpectedly restarts might provide information about the cause. A crash in the `sslvpn` process when all SSL VPN users get disconnected is also relevant. The crashlog includes the details about the crash and information that can be used by Fortinet development to identify which code triggered the problem.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand the life of a packet
- ✓ Review general system troubleshooting commands
- ✓ Enable real-time debugs
- ✓ Examine how FortiOS uses memory
- ✓ Review the most common FortiOS processes and process states
- ✓ Identify memory conserve mode
- ✓ Troubleshoot unexpected reboots and frozen units
- ✓ Optimize memory usage and examine the crashlog
- ✓ Understand FortiOS workspace mode

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

By mastering the objectives covered in this lesson, you learned about the architecture of FortiOS.

DO NOT REPRINT
© FORTINET

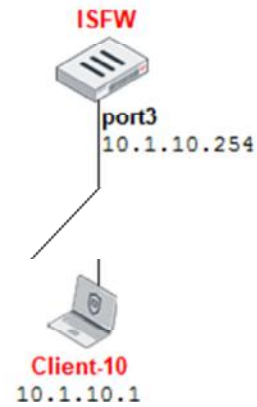
Lab 2—FortiOS Architecture

Now, you will work on *Lab 2—FortiOS Architecture*.

DO NOT REPRINT
© FORTINET

Lab 2—FortiOS Architecture

- Run debug commands to gather information about resource utilization on ISFW
- Check the crashlog



FORTINET

© Fortinet Inc. All Rights Reserved.

52

In this lab, you will run debug commands to gather information about resource utilization on ISFW.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about traffic and session monitoring.

DO NOT REPRINT
© FORTINET

Objectives

- Analyze the information in the session table
- Capture traffic using the built-in sniffer
- Analyze the output of the debug flow
- Configure and troubleshoot session helpers
- Configure and troubleshoot the SIP application layer gateway

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

By demonstrating competence in traffic and session monitoring, you will be able to interpret the information in the session table, capture traffic using the built-in sniffer, analyze the output of the debug flow, configure and troubleshoot session helpers and the SIP application layer gateway.

DO NOT REPRINT
© FORTINET

Session Table

In this section, you will learn about session table entries.

DO NOT REPRINT
© FORTINET

Session Table Summary

```
# get sys session status
```

The total number of IPv4 sessions for the current VDOM: 11

```
# get sys session list
```

PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT
tcp	3522	10.1.10.1:41418	100.64.1.1:41418	172.217.0.106:443	-
udp	151	10.1.0.1:4387	100.64.1.1:64803	208.91.112.220:53	-
udp	28	10.1.0.1:1687	100.64.1.1:62103	208.91.112.52:53	-
udp	61	100.64.1.1:3075	-	208.91.112.53:53	-
udp	55	100.64.1.1:3075	-	208.91.112.52:53	-
udp	172	10.1.10.1:123	100.64.1.1:60539	209.121.129.48:123	-
udp	152	10.1.0.1:4387	100.64.1.1:64803	173.243.138.221:53	-
udp	152	10.1.0.1:4387	100.64.1.1:64803	45.75.200.89:53	-
udp	171	10.1.10.1:123	100.64.1.1:60539	208.81.1.197:123	-
udp	104	10.1.0.1:1420	-	10.1.0.254:53	-
tcp	3600	10.1.10.1:34433	-	10.1.0.254:22	-
udp	176	10.1.0.1:1900	-	10.1.0.254:53	-
tcp	3524	10.1.10.1:59972	100.64.1.1:59972	172.217.0.110:80	-
tcp	119	10.1.10.1:42824	100.64.1.1:42824	72.21.91.29:80	-
tcp	3517	10.1.10.1:42816	100.64.1.1:42816	72.21.91.29:80	-
udp	171	10.1.10.1:123	100.64.1.1:60539	144.217.65.184:123	-
udp	175	10.1.10.1:123	100.64.1.1:60539	144.217.65.182:123	-

FORTINET

© Fortinet Inc. All Rights Reserved.

4

The FortiGate session table contains detailed information about every IP connection that crosses or terminates at FortiGate. We can use the commands shown on the slide to display the total number of sessions in an active VDOM, and to view a brief summary of each session. The `session list` command lists one session on each line, and includes information, such as protocol, source IP address, destination IP address, and port. You can use the `grep` utility with this command to list only the sessions for a specific IP address.

DO NOT REPRINT
© FORTINET

Session Table Details

- Clear any previous filter
diagnose sys session filter clear
- Set the filter
diagnose sys session filter ?
dport destination port
dst destination IP address
policy policy id
sport source port
src source ip address
- List all entries matching the configured filter
diagnose sys session list

FORTINET

© Fortinet Inc. All Rights Reserved.

5

To display detailed information about sessions, use the command shown on this slide. It is recommended that you set the session filter first, because an unfiltered output displays *all* the details about *all* the existing sessions. For high-end devices, a list of all existing sessions could be in the thousands, or even millions. You can filter the output by policy ID, source IP address, source port, destination IP address, and destination port.

DO NOT REPRINT
© FORTINET

Clearing Session Table Entries

- Some configuration changes, such as security profile changes or session helper changes, apply only to new sessions
- In those cases, you can clear existing sessions so changes will apply once new sessions are created
 - Set the filter

```
# diagnose sys session filter ?
```
 - Check the filter

```
# diagnose sys session filter
```
 - Clear all entries matching the configured filter

```
# diagnose sys session clear
```

FORTINET

© Fortinet Inc. All Rights Reserved.

6

Some configuration changes, such as security profile changes or session helper changes, apply only to new sessions. In the case of those changes, existing sessions keep using the previous configuration until they expire or are terminated. This is important to remember when troubleshooting problems. After a security profile change, you should clear any sessions related to that change, and generate new sessions.

Use the command shown on this slide to remove all sessions that match the session filter. You must be careful with this command because it can, potentially, clear all the existing sessions if no filter has been set. Before clearing out any sessions, use appropriate filters.

DO NOT REPRINT
© FORTINET

Session Table—UDP Example

```

session info: proto=17 proto_state=01 duration=26 expire=153 timeout=0 flags=00000000
socktype=00000000 sockport=0 av_idx=0 use=4
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class id=0 shaping policy id=1 ha id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may dirty npu os rs f00
statistic(bytes/packets/allow_err): org=1445/2/1 reply=1437/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=3->8/8->3 gwy=99.247.80.1/10.10.110.19
hook=post dir=org act=snat 10.10.110.19:43124->172.217.7.14:443(99.247.86.206:43124)
hook=pre dir=reply act=dnat 172.217.7.14:443->99.247.86.206:43124(10.10.110.19:43124)
src_mac=e4:f0:42:47:b5:a4
misc=0 policy id=1 auth_info=0 chk_client_info=0 vd=0
serial=003afffa tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id = 00000000
dd type=0 dd mode=0
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=67/88, ipid=88/67,
vlan=0x0000/0x0000
vlifid=88/67, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=3/2

```

FORTINET

© Fortinet Inc. All Rights Reserved.

7

This slide shows a sample of the output contained in the FortiGate session table. From left to right, and from top to bottom, the following information is highlighted:

- The IP protocol number and the protocol state (this value is covered in this lesson)
- The length of time until the session expires (if there is no more traffic)
- Traffic shaping counters
- Session flags
- Received and transmitted packet and byte counters
- If the unit is doing NAT, this portion shows the type of NAT (source or destination) for each traffic direction, and the NAT IP address
- The source MAC address of the packet
- The ID number of the matching policy
- Counters for hardware acceleration

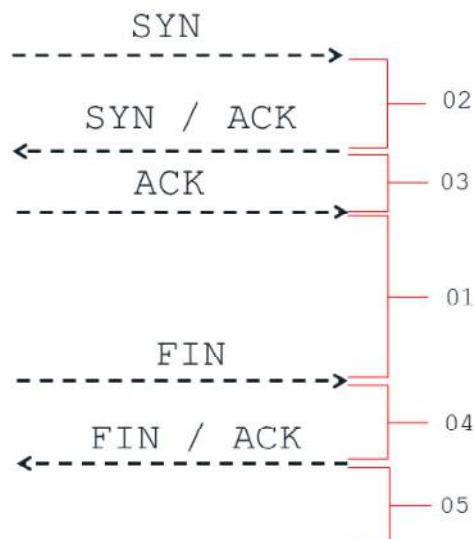
DO NOT REPRINT
© FORTINET

TCP Protocol States

- `proto_state=05`

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

TCP State	Value
NONE	0
ESTABLISHED	1
SYN_SENT	2
SYN & SYN/ACK	3
FIN_WAIT	4
TIME_WAIT	5
CLOSE	6
CLOSE_WAIT	7
LAST_ACK	8
LISTEN	9



FORTINET

© Fortinet Inc. All Rights Reserved.

8

The protocol state in the session table is a two-digit number. For TCP, the first number (from left to right) is related to the server-side state and is 0 when the session is not subject to any inspection (flow or proxy). If flow or proxy inspection is done, then the first digit will be different from 0. The second digit is the client-side state. This table and flow graph correlate the second-digit value with the different TCP session states. For example, when FortiGate receives the SYN packet, the second digit is 2. It changes to 3 when the SYN/ACK packet is received. After the three-way handshake, the state value changes to 1.

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

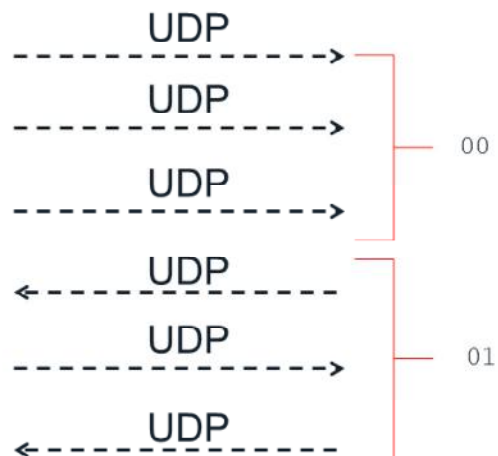
DO NOT REPRINT
© FORTINET

ICMP and UDP Protocol States

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

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

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



FORTINET

© Fortinet Inc. All Rights Reserved.

9

For UDP, the session state can only have two values: 00 when traffic is only one way, and 01 when there is traffic two ways. For ICMP, the protocol state is always 00.

DO NOT REPRINT
© FORTINET

Some Common Session Flags

Flag	Description
log	Session is being logged
local	Session is to/from local stack
ndr	Session will be checked by IPS signature
nds	Session will be checked by IPS anomaly
br	Session is being bridged (TP mode)
npu	Session can be offloaded to NPU
wccp	Web caching
npd	Session cannot be offloaded to NPU
redir	Session is being processed by an application layer proxy
authed	Session was successfully authenticated
auth	Session requires (or required) authentication

FORTINET

© Fortinet Inc. All Rights Reserved.

10

This table shows the meaning of the most important session flags. For example, the `log` flag indicates that the session is being logged. The `local` flag indicates that the session originated from FortiGate or terminates on FortiGate.

DO NOT REPRINT
© FORTINET

Dirty and May Dirty Flags

- Usually only the first session packet is evaluated against the firewall policies:
 - If traffic is allowed, session is created and flagged as `may_dirty`
- After a change in the firewall policy configuration, all `may_dirty` sessions are also flagged as `dirty`:
 - Next packet goes to the CPU, even for offloaded sessions
 - CPU re-evaluates the packet against the new configuration
- If any dirty session has to be blocked:
 - It is flagged as `block`
 - It remains in memory until it expires
 - Further packets are blocked

FORTINET

© Fortinet Inc. All Rights Reserved.

11

Take a look at the `dirty` and `may_dirty` flags. When FortiGate receives the first packet for a new session, it evaluates whether the traffic should or shouldn't be allowed, based on firewall policies. As long as there are no changes in the firewall policy configuration, this evaluation is done on only the first session packet. If the traffic is allowed by a firewall policy, FortiGate creates a session and flags the session as `may_dirty`.

After that, if there is a change in the firewall policy configuration, all the existing sessions with the `may_dirty` flag are also flagged as `dirty`. This indicates to FortiGate that it needs to reevaluate the next session packet to determine if the session must be blocked. If the session is still allowed, the `dirty` flag is removed, but the `may_dirty` flag is kept. If the session must be blocked, it is flagged as `block` and remains in the session table until it expires. Any packet matching a session with the `block` flag is dropped.

DO NOT REPRINT
© FORTINET

Session Handling Settings

- Global session handling setting:

```
config system settings
    set firewall-session-dirty { check-all | check-new | check-policy-option }
end
```

Default option

- **check-all**: All policy information is removed from sessions affected by a policy change. When new packets are received, they are re-evaluated.
- **check-new**: Existing sessions are unaffected. New sessions are evaluated against the modified policies.
- **check-policy-option**: Sessions will be handled based on firewall policy configuration.

- If you configure the **check-policy-option**, you can use the policy specific session handling setting:

```
config firewall policy
    edit <policy_id>
        set firewall-session-dirty { check-all | check-new }
    next
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

12

You can use the CLI commands shown on this slide to modify FortiGate's session handling behaviour after policy changes.

The system-level setting is global, or per-VDOM, if you have VDOMs enabled. The default option is **check-all**, where all policy information is removed from sessions affected by a policy change. When new packets arrive, FortiGate re-evaluates them before adding them to the session table. This is the most resource-intensive behavior.

The **check-new** option is another alternative. When this option is enabled, FortiGate does not modify any existing session after a policy change. When new sessions arrive, FortiGate evaluates them against the modified policies. You can use this option if you have policies handling millions of sessions.

The **check-policy-option** is the most granular setting you can use. When you enable this option, the firewall policy-level settings become available, which you can use to modify how FortiGate handles sessions on a per-policy level.

DO NOT REPRINT
© FORTINET

NGFW Policy Mode Review

Select Entries

Q Search

FORTIGUARD WEB FILTER CATEGOR

Adult/Mature Content (15)

Abortion

Advocacy Organizations

Alcohol

Alternative Beliefs

Dating

Gambling

Lingerie and Swimsuit

Marijuana

Nudity and Risque

Other Adult Materials

Pornography

Sex Education

Sports Hunting and War Games

Tobacco

Close

Policy & Objects > Security Policy

Name

Incoming Interface

Outgoing Interface

Source

Destination

Schedule

Service

Application

URL Category

Action

always

App Default

Specify

ACCEPT

DENY

Select Entries

Application

Category

Group

Q Search

+

Create

FIREWALL APPLICATION (2,009)

Business (143)

Acronis.Snap.Deploy

Act!

ActiveCampaign

ActiveCampaign_File.Upload

ADP

AirWatch.MDM

Alibaba

Apache.Cassandra

Applane.CRM

Atlassian.JIRA

AutoDesk.360

AutoDesk.360_Upload

Autodesk.BIM360

Close

FORTINET

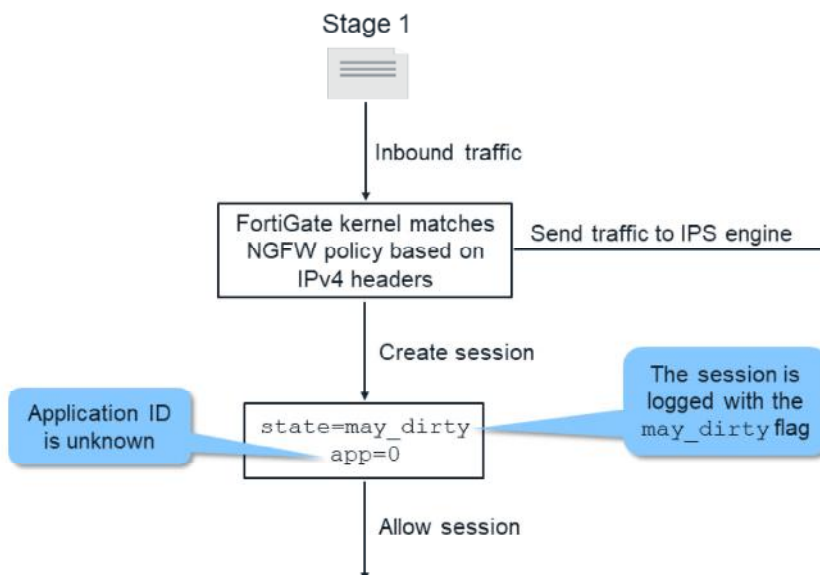
© Fortinet Inc. All Rights Reserved.

13

You can now configure FortiGate to operate in NGFW policy mode. NGFW policy mode is a flow-based inspection mode that allows you to configure application signatures, categories, groups, and FortiGuard web filter categories directly on the firewall policy. Other security inspection features, such as antivirus and DLP, are still configured as profiles.

DO NOT REPRINT
© FORTINET

NGFW Policy Mode Session Handling—Stage 1



FORTINET

© Fortinet Inc. All Rights Reserved.

14

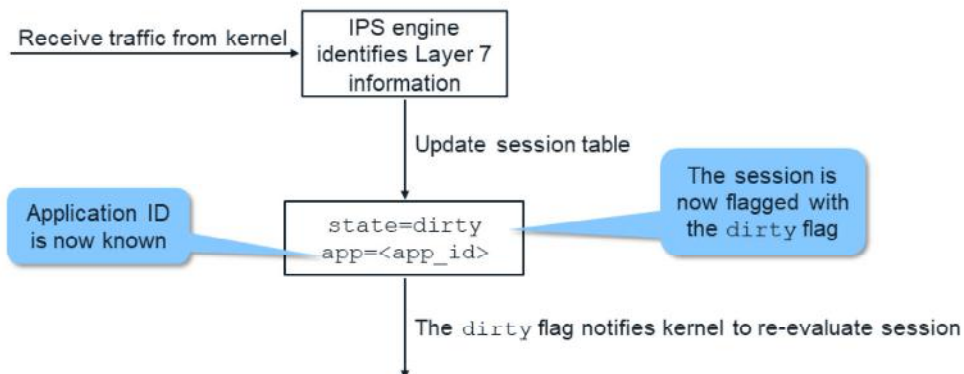
You should view NGFW policy mode session handling as having three distinct stages.

The FortiGate kernel can identify ICMP, DNS, and NTP traffic in the kernel. All other traffic types, the kernel cannot identify. So, when the session first comes in, the kernel is not aware of any Layer 7 information, and uses the Layer 4 headers to search the NGFW policy table for a match. At this point, the kernel creates a session table entry with the `may_dirty` flag, creates an application ID of 0 for the `app` field, and allows the session to flow.

DO NOT REPRINT
© FORTINET

NGFW Policy Mode Session Handling—Stage 2

Stage 2



FORTINET

© Fortinet Inc. All Rights Reserved.

15

While the session is allowed, the kernel forwards packets to the IPS engine. The IPS engine performs Layer 7 identification, and updates the session table. The session table entry is flagged with the `dirty` flag, and the identified application ID is added. The `dirty` flag notifies the kernel that the session needs to be re-evaluated.

DO NOT REPRINT
© FORTINET

NGFW Policy Mode Session Handling—Stage 3

Stage 3

state=dirty
app=<app_id>

The dirty flag notifies kernel to re-evaluate session

Kernel searches
NGFW policy
table using Layer
7 information

Kernel applies action configured on the matching policy

FORTINET

© Fortinet Inc. All Rights Reserved.

16

The kernel uses the Layer 7 information to search the NGFW policy table again for a match. Once a match is found, the kernel applies the configured action on the matching policy.

DO NOT REPRINT
© FORTINET

Sniffer and Debug Flow

In this section, you will learn about two useful troubleshooting tools: the built-in sniffer and the debug flow.

DO NOT REPRINT
© FORTINET

Advanced Packet Capture Options

```
#diagnose sniffer packet <interface> '<filter>' <level> <count>
<tsformat>
```

- <count> stops packet capture after this many packets
- <tsformat> changes the time stamp format
- a – Absolute UTC time
- l – Local time

Level	IP headers	IP payload	Ethernet headers	Port names
1	✓			
2	✓	✓		
3	✓	✓	✓	
4	✓			✓
5	✓	✓		✓
6	✓	✓	✓	✓

FORTINET

© Fortinet Inc. All Rights Reserved.

18

Now you will learn about the built-in sniffer. When you enable this tool, you can choose from six verbosity levels. The table on this slide shows what information is displayed in each level. Level 4 is usually used to check how the traffic is flowing and that FortiGate is not dropping packets. Level 3 or Level 6 are usually used to convert the output to PCAP format, which can later be analyzed with a tool such as WireShark.

DO NOT REPRINT
© FORTINET

Advanced Packet Capture Options—Output

```
# diagnose sniffer packet any 'host 8.8.8.8 and icmp' 4
interfaces=[any]
filters=[host 8.8.8.8 and icmp]
11.208116 lan in 10.1.10.1 -> 8.8.8.8: icmp: echo request
11.208370 wan1 out 172.20.121.11 -> 8.8.8.8: icmp: echo request
11.216576 wan1 in 8.8.8.8 -> 172.20.121.11: icmp: echo reply
11.216680 lan out 8.8.8.8 -> 10.1.10.1: icmp: echo reply
4 packets received by filter
0 packets dropped by kernel
```

any to capture all interfaces

Number of packets matching the filter that could not be captured by the sniffer; therefore, you must use a more specific filter

```
Hub # diagnose sniffer packet any 'icmp' 4 3 a
interfaces=[any]
filters=[host 8.8.8.8 and icmp]
2019-05-15 18:04:48.722396 lan in 10.1.10.1 -> 8.8.8.8: icmp: echo request
2019-05-15 18:04:48.722549 wan1 out 172.20.121.11 -> 8.8.8.8: icmp: echo request
2019-05-15 18:04:48.730349 wan1 in 8.8.8.8 -> 172.20.121.11: icmp: echo reply
```

Timestamp

To sniffer traffic in all interfaces, use the keyword `any` as the interface name.

Stop the sniffer by pressing Ctrl+C, and check for dropped packets. If there were dropped packets during the sniffer, it means that not all the traffic that matched the sniffer filter could be captured. So, you might need to capture the traffic again using a stricter filter.

If you don't specify an option for the timestamp, the debug shows the time, in seconds, since it started running. As you learned earlier in the lesson, you can prepend the local system time to easily correlate a packet with another recorded event.

DO NOT REPRINT
© FORTINET

Debug Flow

- Shows kernel decisions
- Multi-step command
 - Enable display of function names:
`# diagnose debug flow show function-name enable`
 - Specify the filter:
`# diagnose debug flow filter [filter]`
 - Send output to telnet/SSH:
`# diagnose debug enable`
 - Start the trace:
`# diagnose debug flow trace start <count>`
 - Stop the trace:
`# diagnose debug flow trace stop`

FORTINET

© Fortinet Inc. All Rights Reserved.

20

Another useful FortiGate troubleshooting tool is the debug flow.

The debug flow is also called internal sniffer because it works similarly to the built-in sniffer, but the output shows step-by-step, and with details, what the kernel is doing with each packet.

DO NOT REPRINT
© FORTINET

Debug Flow Example

```
id=20085 trace_id=13 func=print_pkt_detail 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=20085 trace_id=13 func=init_ip_session_common line=4831 msg="allocate a new session-00007fc0"
id=20085 trace_id=13 func=vf_ip_route_input_common line=2582 msg="find a route: flag=04000000 gw-
10.200.1.254 via port1"
id=20085 trace_id=13 func=fw_forward_handler line=699 msg="Allowed by Policy-1: SNAT"
id=20085 trace_id=13 func=_ip_session_run_tuple line=2719 msg="SNAT 10.0.1.10->10.200.1.1:49886"
```

SYN

```
id=20085 trace_id=14 func=print_pkt_detail 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"
id=20085 trace_id=14 func=resolve_ip_tuple_fast line=4739 msg="Find an existing session, id-00007fc0, reply
direction"
id=20085 trace_id=14 func=_ip_session_run_tuple line=2733 msg="DNAT 10.200.1.1:49886->10.0.1.10:49886"
id=20085 trace_id=14 func=vf_ip_route_input_common line=2582 msg="find a route: flag=00000000 gw-10.0.1.10
via port3"
```

SYN/ACK

```
id=20085 trace_id=15 func=print_pkt_detail line=4677 msg="vd-root received a packet(proto=6,
10.0.1.10:49886->66.171.121.44:80) from port3. flag [.], seq 2176715502, ack 3567496941, win 256"
id=20085 trace_id=15 func=resolve_ip_tuple_fast line=4739 msg="Find an existing session, id-00007fc0,
original direction"
id=20085 trace_id=15 func=ipv4_fast_cb line=53 msg="enter fast path"
id=20085 trace_id=15 func=ip_session_run_all_tuple line=5798 msg="SNAT 10.0.1.10->10.200.1.1:49886"
```

ACK

FORTINET

© Fortinet Inc. All Rights Reserved.

21

This slide shows an example of a debug flow output. In this example, the debug flow has captured the three packets of a TCP three-way handshake. The output for the SYN packet shows when the kernel creates a new session (with its session ID), finds the route to the destination, and applies NAT. It also shows the ID of the policy that matches this traffic.

The output of the SYN/ACK and ACK packets shows the session ID and NAT information.

This tool is useful for many troubleshooting cases, such as 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

Common Debug Flow Blocking Messages

- `denied by forward policy check`
 - No firewall policy allows the traffic
 - A firewall policy allows the traffic, but disclaimer is enabled. Disclaimer must be accepted first.
- `denied by end point ip filter check`
 - Source IP address has been quarantined by DLP
- `exceeded shaper limit, drop`
 - Packet dropped because of traffic shaping

FORTINET

© Fortinet Inc. All Rights Reserved.

22

The debug flow can also help you identify why FortiGate is dropping packets. In those cases, the debug flow usually shows an error message explaining why a packet was dropped.

This slide shows three messages that you commonly see in debug flow output when FortiGate is dropping packets:

- `Denied by forward policy check` indicates that either no firewall policy allows the traffic, or that a disclaimer has not been accepted yet
- `Denied by end point ip filter check` indicates that the IP address has been quarantined by the DLP inspection
- `exceeded shaper limit, drop` indicates that the packet was dropped because of a traffic shaper that has exceeded one of its thresholds

DO NOT REPRINT
© FORTINET

Common Debug Flow Blocking Messages

- `reverse path check fail, drop`
 - Packet dropped because of the reverse path forwarding check
- `iprope_in_check() check failed, drop`
 - Packet is destined to a FortiGate IP address (management traffic) but:
 - The service is not enabled
 - Or the service is using a different TCP port
 - Or the source IP address is not included in the trusted host list
 - Or the packet matches a local-in policy with action deny
 - Packet is not destined to a FortiGate IP address, but there is a virtual IP or IP pool configuration using the destination IP address

FORTINET

© Fortinet Inc. All Rights Reserved.

23

This slide shows two more common debug flow error messages. The first error message indicates that the packet failed the reverse path forwarding check.

The second error message usually indicates one of the following:

- The packet is destined to a FortiGate IP address (for example, management traffic), but the service is not enabled, the service is using a different port, the source IP address is not included in the trusted list, or the packet matches a local-in policy with the action `deny`.
- The packet is destined to a device on the other side of FortiGate, but a virtual IP or IP pool is wrongly using that IP address. In this case, check your virtual IP or IP pool configuration.

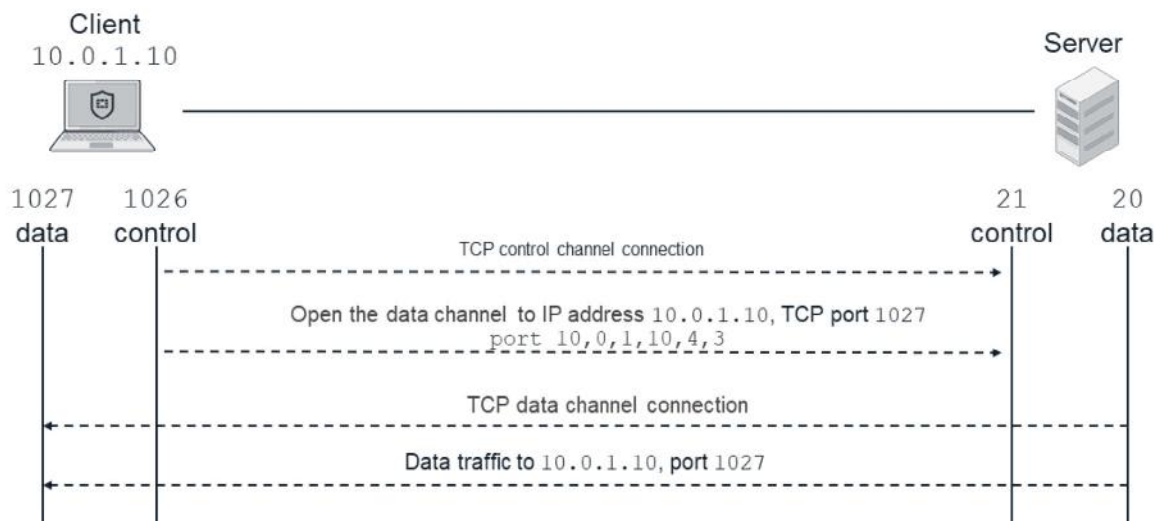
DO NOT REPRINT
© FORTINET

Session Helpers and Application Layer Gateways

Not all sessions are created by existing traffic matching firewall policies. In this section, you will examine how FortiGate can create sessions for traffic that is expected to come, but hasn't arrived yet. This is part of what session helpers and the application layer gateway do.

DO NOT REPRINT
© FORTINET

Session Helper Example—Active FTP Case



FORTINET

© Fortinet Inc. All Rights Reserved.

25

To understand what a session helper does, take a look at this example of a network protocol that might have problems when a network device is doing NAT. The example on this slide shows the FTP protocol working in active mode.

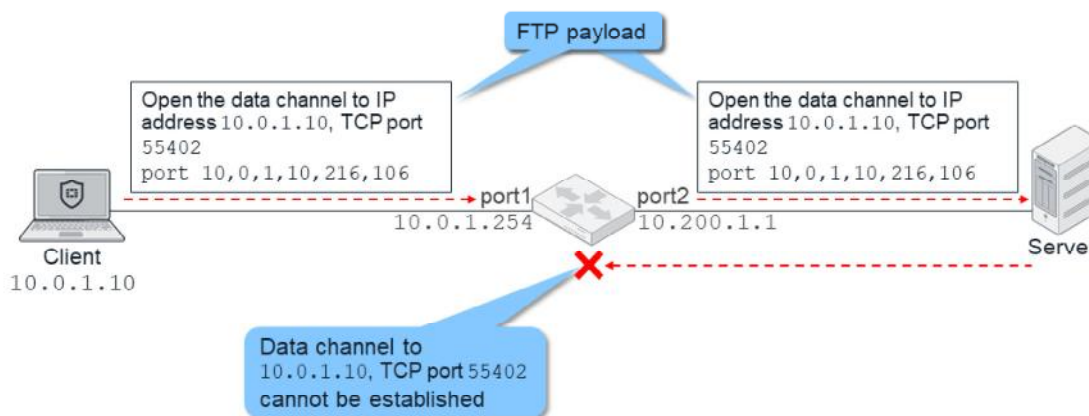
Any FTP file transfer is composed of two TCP sessions: one for the control channel and one for data transfer. The control channel is always initiated from the client to the server and is used to send the FTP commands. The FTP commands allow the client to move through the server folder, specify the type of file transfer, and initiate the data channel for uploading or downloading a file.

FTP has two modes: active and passive. The mode determines who initiates the data channel. In passive mode, the data channel is initiated by the client. In active mode, the client sends the `port` command through the control channel. The command includes the client IP address and the TCP port for the incoming data channel. Then, the server initiates the TCP session to the IP address and port number specified by the `port` command.

DO NOT REPRINT
© FORTINET

Active FTP with NAT and No Session Helper

- Router doing NAT of 10.0.1.10 to 10.200.1.1



FORTINET

© Fortinet Inc. All Rights Reserved.

26

Active FTP won't work if the control channel crosses a network device doing NAT, that does not have a session helper. In the example shown on this slide, an FTP client is connecting to an active mode FTP server. There is a router in the middle doing NAT of the client IP address 10.0.1.10 to the NAT IP address 10.200.1.1.

After the control channel is up, the client sends the `port` command with its IP address, 10.0.1.10, as the destination for the data channel.

When that FTP packet crosses the router, the source IP address in the IP header is changed from 10.0.1.10 to 10.200.1.1. However, the IP address in the FTP `port` command is *not* translated to 10.200.1.1.

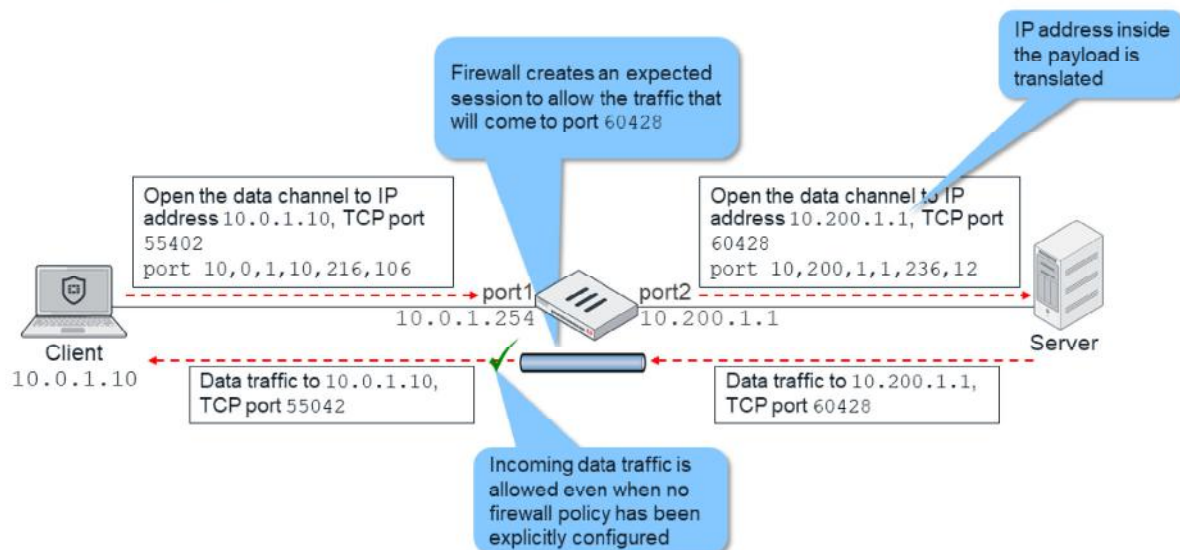
Once the server receives that FTP command, it tries to bring up the TCP session for the data channel. It sends the SYN packet to the IP address 10.0.1.10. This address is probably not routable because it is a private IP behind a device doing NAT.

The file transfer fails.

DO NOT REPRINT
© FORTINET

Active FTP with NAT and Session Helper

- FortiGate doing NAT of 10.0.1.10 to 10.200.1.1



FORTINET

© Fortinet Inc. All Rights Reserved.

27

The FTP session helper fixes this problem by replacing the router with a FortiGate device. The following describes what the FortiGate session helper does.

When the packet with the FTP `port` command arrives at FortiGate, FortiGate not only translates the source IP address in the IP header, the session helper also translates the IP address inside the FTP `port` command. If the source port is also translated in the TCP header, the session helper also does the same in the `port` command.

Another important function of the session helper is to temporarily create an expected session (or pinhole) for the data channel connection that will come from the server. That means that the administrator does not need to manually create firewall policies to allow these incoming TCP sessions (which use random TCP ports numbers). The session helper automatically creates the session and opens the door for the incoming connection.

After that, the server connects the data channel to the right IP address: 10.200.1.1. That incoming TCP connection is allowed by the expected session previously created by the session helper, even when there is no firewall policy allowing it.

DO NOT REPRINT
© FORTINET

Active FTP—Sniffer Before FortiGate

No.	Time	Source	Destination	Protocol	Length	Info
20	0.047003	10.200.3.254	10.0.1.10	FTP	60	Response: 200 Always in data mode.
21	0.070533	10.0.1.10	10.200.3.254	FTP	60	Request: PWD
22	0.071152	10.200.3.254	10.0.1.10	FTP	63	Response: 257 "/"
23	0.086150	10.0.1.10	10.200.3.254	FTP	62	Request: TYPE I
24	0.086721	10.200.3.254	10.0.1.10	FTP	85	Response: 200 Switching to Binary mode.
25	0.097044	10.0.1.10	10.200.3.254	FTP	78	Request: PORT 10,0,1,10,216,106
26	0.097694	10.200.3.254	10.0.1.10	FTP	105	Response: 200 PORT command successful. Consider using
27	0.107037	10.0.1.10	10.200.3.254	FTP	60	Request: LIST
28	0.107921	10.200.3.254	10.0.1.10	FTP	93	Response: 150 Here comes the directory listing.

Offset	Hex	ASCII
0000	00 50 56 97 45 88 00 50 56 97 3e c5 08 00 45 00	.PV.E..P V.>...E.
0010	00 40 0a 7b 40 00 80 06 d6 bd 0a 00 01 0a 0a c8	.@.{@... .m.....
0020	03 fe d8 69 00 15 23 a2 46 7d fa 98 ef c3 50 18	...i..#. F]...P.
0030	00 ff 1b 88 00 00 50 4f 52 54 20 31 30 2c 30 2cPO RT 10,0,
0040	31 2c 31 30 2c 32 31 36 2c 31 30 36 0d 0a	1,10,216 ,106..

This slide shows a packet capture of the previous FTP traffic before the `port` command reaches FortiGate. You can see the original client IP address, 10.0.1.10.

DO NOT REPRINT
© FORTINET

Active FTP—Sniffer After FortiGate

No.	Time	Source	Destination	Protocol	Length	Info
19	0.046955	10.200.1.1	10.200.3.254	FTP	68	Request: OPTS UTF8 ON
20	0.047563	10.200.3.254	10.200.1.1	FTP	80	Response: 200 Always in UTF8 mode.
21	0.070455	10.200.1.1	10.200.3.254	FTP	59	Request: PWD
22	0.071046	10.200.3.254	10.200.1.1	FTP	63	Response: 257 "/"
23	0.086062	10.200.1.1	10.200.3.254	FTP	62	Request: TYPE I
24	0.086611	10.200.3.254	10.200.1.1	FTP	85	Response: 200 Switching to Binary mode.
25	0.096985	10.200.1.1	10.200.3.254	FTP	78	Request: PORT 10.200.1.1 236,12
26	0.097592	10.200.3.254	10.200.1.1	FTP	105	Response: 200 PORT command successful. Consider using
27	0.106050	10.200.1.1	10.200.3.254	FTP	60	Request: LIST

Frame 25: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)

Ethernet II, Src: Vmware_97:7e:ea (00:50:56:97:7e:ea), Dst: vmware_97:2f:94 (00:50:56:97:2f:94)

Internet Protocol Version 4, Src: 10.200.1.1 (10.200.1.1), Dst: 10.200.3.254 (10.200.3.254)

Transmission Control Protocol, Src Port: 55401 (55401), Dst Port: 21 (21), Seq: 77, Ack: 236, Len: 24

File Transfer Protocol (FTP)

0000 00 50 56 97 2f 94 00 50 56 97 7e ea 08 00 45 00 .PV./..P V....E.
 0010 00 40 0a 7b 40 00 7f 06 d6 ae 0a c8 01 01 0a c8 .@.{@... ..
 0020 03 fe d8 69 00 15 23 a2 46 7d fa 98 ef c3 50 18 ...l..#. F]...P.
 0030 00 ff 08 db 00 00 50 4f 52 54 20 31 30 2c 32 30PO RT 10,20
 0040 30 2c 31 2c 31 2c 32 33 36 2c 31 32 0d 0a 0,1,1,23 6,12..

FORTINET

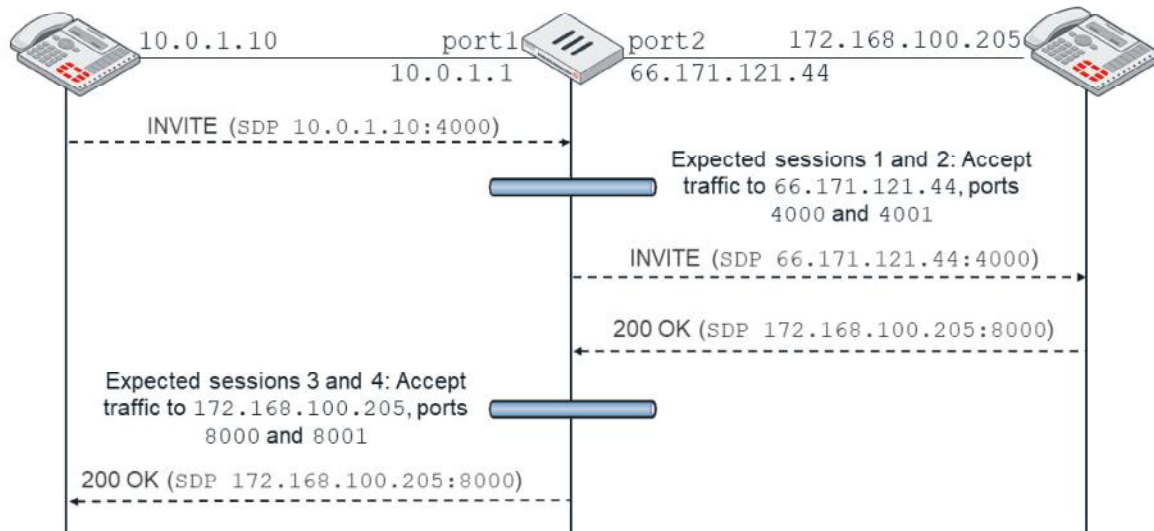
© Fortinet Inc. All Rights Reserved.

29

This slide shows another packet capture, this time after the `port` command crosses FortiGate. The session helper has translated the IP address inside the `port` command to 10.200.1.1.

DO NOT REPRINT
© FORTINET

Session Helper Example—SIP Case



FORTINET

© Fortinet Inc. All Rights Reserved.

30

SIP is another protocol that requires a session helper in a NAT environment. Similar to FTP, SIP uses control channels and data channels. In SIP, four data channels, two for each traffic direction, are required for each call. In the example shown on this slide, there are two SIP phones with the IP addresses 10.0.1.10 and 172.168.100.205. Additionally, FortiGate is doing NAT of 10.0.1.10 to 66.171.121.44.

Once the control channel is up, a SIP phone sends an `invite` packet with its IP address and port numbers for two of the four data channels. The FortiGate session helper creates two expected sessions, and translates the IP address inside the `invite` packet to 66.171.121.44.

The remote phone sends an `OK` packet to the right destination IP address (66.171.121.44). The packets include the IP address and ports for the other two data channels. The session helper creates two more expected sessions, this time using the information coming in the `OK` packet. After that, the four data channels can be connected through the four expected sessions. Firewall policies are not needed to allow this traffic.

DO NOT REPRINT
© FORTINET

Expected Sessions

```
# diagnose sys session list expectation

session info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
origin->sink: org pre->post, reply pre->post dev=2->4/4->2
gw=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0->100.64.1.1:60426(10.0.1.10:50365)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

Pinhole opened from traffic
from 10.171.121.38 to
100.64.1.1 port 60426

FORTINET

© Fortinet Inc. All Rights Reserved.

31

There is a way to list the expected sessions created by the session helpers. In the example shown on this slide, the command lists an expected session to allow traffic from 10.171.121.38 to 100.64.1.1, port TCP 60426.

DO NOT REPRINT
© FORTINET

Monitoring Session Helper

- For traffic inspected by a helper, debug flow shows:
`run helper-ftp(dir=original)`
or
`run helper-ftp(dir=reply)`
- For traffic matching an expected session, debug flow shows:
`Find an EXP session, id 00016f90`

FORTINET

© Fortinet Inc. All Rights Reserved.

32

The debug flow shows the name of the session helper (if any) that is inspecting the traffic. In this case, it is the FTP session helper.

Also, for traffic that matches an expected session previously created by a session helper, the debug flow shows the message: `Find an EXP session`.

DO NOT REPRINT
© FORTINET

Adding a Helper for a Non-Standard Port

```
config system session-helper
show
    edit 13
        set name sip
        set protocol 17
        set port <port_number>
    next
    edit 14
        set name h323
        set protocol 6
        set port <port_number>
    next
... *
```

FORTINET

© Fortinet Inc. All Rights Reserved.

33

There are other protocols that, in some circumstances, also require a session helper. Examples includes PPTP, H323, and RSH. You can list the active session helpers by using the command shown on this slide. The output lists the TCP or UDP port numbers that each session helper is listening to. If one of those protocols is using a different port number, you need to change the FortiGate configuration to match it. You can either change the port number in the existing session-helper entry, or add a new entry.

DO NOT REPRINT
© FORTINET

SIP Application Layer Gateway

- The SIP application layer gateway (ALG) provides:
 - All the same features as the SIP helper
 - SIP TCP and UDP support
 - SIP IPv6
 - Rate limiting
 - SIP messages syntax checking
 - SIP HA failover
 - Detailed logging and reporting
- Session helpers run in the kernel
- SIP ALG runs as a user space process

FORTINET

© Fortinet Inc. All Rights Reserved.

34

For SIP traffic inspection, FortiGate includes a feature that is smarter and more versatile than the SIP session helper. It is the SIP ALG.

The SIP ALG has all the same functions as the SIP helper, but provides more features. Also, while session helpers run in the kernel, the SIP ALG runs as a user space process.

DO NOT REPRINT
© FORTINET

VoIP Mode

- Setting the VoIP mode:

```
config system settings
    set default-voip-alg-mode [proxy-based | kernel-helper-based]
end
```
- The SIP ALG is used when:
 - Traffic matches a policy with a VoIP profile, regardless of the VoIP mode
 - Traffic does not match a policy with a VoIP profile and the VoIP mode is set to `proxy-based`
- The SIP helper is used when:
 - Traffic does not match a policy with a VoIP profile and the VoIP mode is set to `kernel-helper-based`

FORTINET

© Fortinet Inc. All Rights Reserved.

35

FortiGate uses either the SIP helper or the SIP ALG, depending on the configuration. The system setting `default-voip-alg-mode` specifies which one is used when no VoIP profile is applied. If it is set to `proxy-based` (default), the SIP ALG is used. If it is set to `kernel-helper-based`, the SIP helper is used.

If the SIP traffic matches a firewall policy with a VoIP profile, the SIP ALG is always used, regardless of the `default-voip-alg-mode` setting.

Fortinet recommends using the SIP ALG. The SIP helper should be used only when the SIP ALG is not working as expected.

DO NOT REPRINT
© FORTINET

Changing SIP ALG Port Numbers

```
config system settings
  set sip-tcp-port <port_number_1> <port_number_2>...
  set sip-udp-port <port_number_1> <port_number_2>...
  set sip-ssl-port <port_number_1> <port_number_2>...
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

36

These are the commands you use to change the ports for the SIP ALG. The SIP ALG supports SIP over UDP, SIP over TCP, and encrypted (SSL) SIP.

DO NOT REPRINT
© FORTINET

SIP Call List

```
# diagnose sys sip-proxy calls list
sip calls
  vdom 0 (root) call 2a9ac86140
    call-id: 7a95e96130fa458b85b2d941456108e4
    txn 2a9ac29800 (INVITE)
      cseq 24786 dir 0 state 5 status 200 expiry 179 HA 0
      i_session: 2a9ac65400 r_session: 2a9ac65400
      register: not-present
      from: sip:10.0.1.10
      to: sip:10.0.2.10
      src: 10.0.1.10:54078
      dst: 10.0.2.10:5060

# diagnose sys sip-proxy calls clear
```



© Fortinet Inc. All Rights Reserved.

37

You can display all active SIP calls and disconnect any active SIP calls using the commands shown on this slide.

DO NOT REPRINT
© FORTINET

SIP Real-Time Debug

```
# diagnose debug application im 31
# diagnose debug application sip <debug_level>
# diagnose debug enable
```

Level	Description
1	Configuration changes
2	Connections accepted and redirected
4	Session creation and deletion
16	I/O reads/writes
32	ASCII dump of all data
64	HEX dump of all data
128	FortiCarrier dynamic profile
256	Summary of SIP fields
1024	SIP geo-redundancy
2048	SIP HA synchronization

FORTINET

© Fortinet Inc. All Rights Reserved.

38

You can use `im` and `sip` real-time debugs to display real-time information about SIP traffic.

DO NOT REPRINT
© FORTINET

Review

- ✓ Analyze the session table
- ✓ Capture traffic using the built-in sniffer
- ✓ Analyze the debug flow output
- ✓ Configure and troubleshoot session helpers
- ✓ Configure and troubleshoot the SIP application layer gateway

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

DO NOT REPRINT
© FORTINET

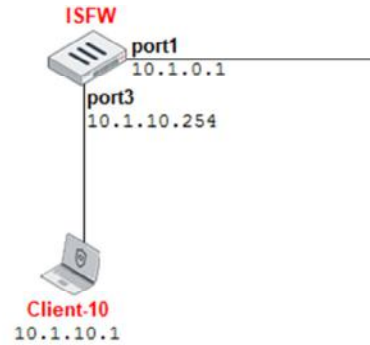
Lab 3—Traffic and Session Monitoring

Now, you will work on *Lab 4—Traffic and Session Monitoring*.

DO NOT REPRINT
© FORTINET

Lab 3—Traffic and Session Monitoring

- Analyze session table information on ISFW
- Troubleshoot connectivity problems on ISFW:
 - No Telnet administrative access to ISFW
 - No access to the web server (<http://10.1.4.10>)
 - No internet access
 - No Telnet to the Linux-Router



FORTINET

© Fortinet Inc. All Rights Reserved.

41

In this lab, you will use debug commands to troubleshoot four connectivity problems. You will also analyze the information in the FortiGate session table, run the built-in sniffer, and use the debug flow to understand how FortiGate is processing each IP packet.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about advanced routing concepts that are relevant to enterprise networks.

Objectives

- Describe how FortiGate routes traffic
- Diagnose routing problems caused by reverse path forwarding check
- Identify sessions that will be routed through a different path after a routing table change
- Use debug commands to troubleshoot routing problems
- Configure virtual routing and forwarding instances

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

By demonstrating competence in routing, you will be able to describe how FortiGate routes traffic, diagnose routing problems caused by reverse path forwarding check, identify sessions that will be routed through a different path, and use debug commands to troubleshoot routing problems.

DO NOT REPRINT
© FORTINET

General Concepts and Troubleshooting

In this section, you will learn about general routing concepts and troubleshooting.

DO NOT REPRINT
© FORTINET

Route Lookup

- For any session, FortiGate performs routing table lookup twice:
 - On the first packet sent by the originator
 - On the first reply packet coming from the responder
- Routing information written to session table and route cache
- Exception: after a routing change, route information is flushed from affected sessions and route cache entries
 - So, additional routing table lookups are required after



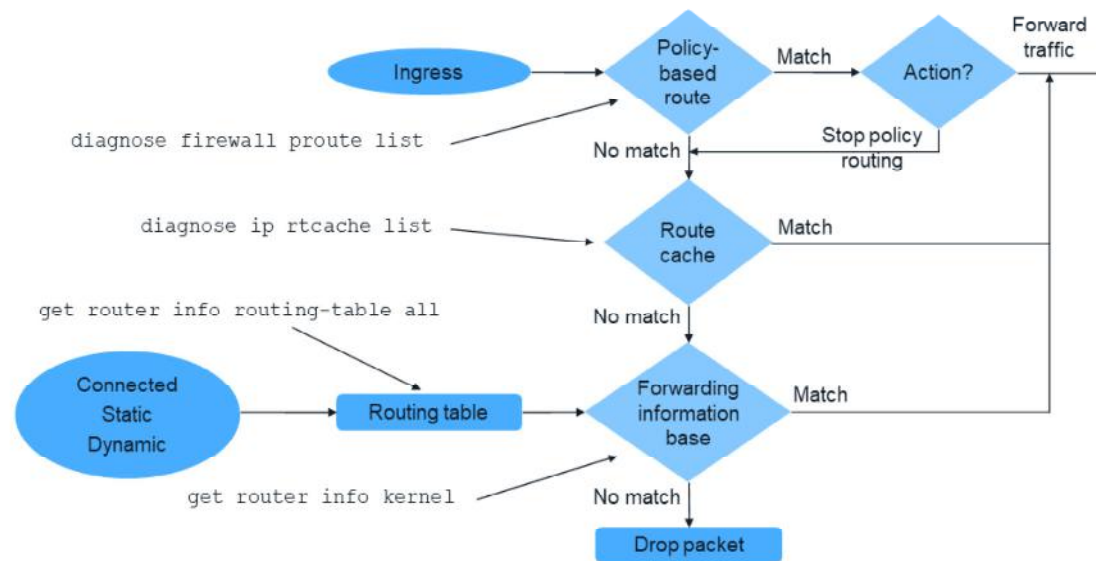
© Fortinet Inc. All Rights Reserved.

4

FortiGate is a stateful device, so it decodes a lot of information at the beginning of a session, based on the first packets. For any traffic session, FortiGate usually performs only two routing lookups: one on the first packet sent by the originator and another one on the first reply packet coming from the responder. After that, all the routing information is written in the FortiGate session table. However, after a change to the routing table, the route information is flushed from the affected entries in the session table. So, FortiGate would perform additional routing table lookups in order to repopulate the session table with the new routing information.

DO NOT REPRINT
© FORTINET

Routing Table Lookup



FORTINET

© Fortinet Inc. All Rights Reserved.

5

How does FortiGate decide routes? FortiGate has multiple routing modules. The diagram shown on this slide illustrates the logic of the routing modules.

First, FortiGate searches its policy routes. You can view them using the command `diagnose firewall proute list`. If there is a match in a policy route, and the action is `Forward Traffic`, FortiGate routes the packet accordingly. If the action is `Stop Policy Routing`, FortiGate goes to the next table, which is the route cache. You can view that content using the CLI command `diagnose ip rtcache list`.

Finally, FortiGate searches the forwarding information base (FIB). The FIB is generated by the routing process, and is the table used for packet forwarding. Think of the routing table's purpose as *management*, while the FIB's purpose is *forwarding*. This separation becomes clearer in a FortiGate high availability (HA) cluster. In an HA cluster, both route management and forwarding tables exist on the master FortiGate. But on the slave FortiGate, only the FIB exists.

If there's no match in any of those tables, FortiGate drops the packet because it is unroutable.

DO NOT REPRINT
© FORTINET

Route Selection Process

1. Most specific route
2. Lowest distance
3. Lowest metric (dynamic routes)
4. Lowest priority (static routes)
5. Equal cost multipath (ECMP) supported for static, BGP, and OSPF

FORTINET

© Fortinet Inc. All Rights Reserved.

6

When there is more than one route to a destination, this is the process for selecting which route to use.

First, FortiGate uses the most specific route, which is the one with the longest netmask (smallest subnet). If there are two or more routes with the same longest netmask, the unit selects the one with the shortest distance. After that, the lowest metric is used as the tiebreaker for dynamic routes. In the case of static routes, the priority is used instead. If there are multiple routes with the same netmask, distance, metric, and priority, FortiGate shares the traffic among all of them. This is called equal cost multipath (ECMP). ECMP is supported for static, BGP, and OSPF routes.

DO NOT REPRINT
© FORTINET

Static Routes

- FortiGate places a configured static route in the routing table if the following requirements are met:
 - The outgoing interface is up
 - There is no other matching route with a lower distance
 - The link health monitor (if configured) is successful

FORTINET

© Fortinet Inc. All Rights Reserved.

7

FortiGate adds a static route to the routing table only if all of the following requirements are met:

- The outgoing interface is up
- There is no other route to the same destination with a shorter distance
- The link health monitor (if configured) is up

DO NOT REPRINT
© FORTINET

Reverse Path Forwarding

- Protects against IP spoofing attacks and routing loops
- Checks the source IP address
- Is carried out on the first packet when the session is created
- If the check fails, the debug flow shows:
 - `reverse path check fail, drop`

FORTINET

© Fortinet Inc. All Rights Reserved.

8

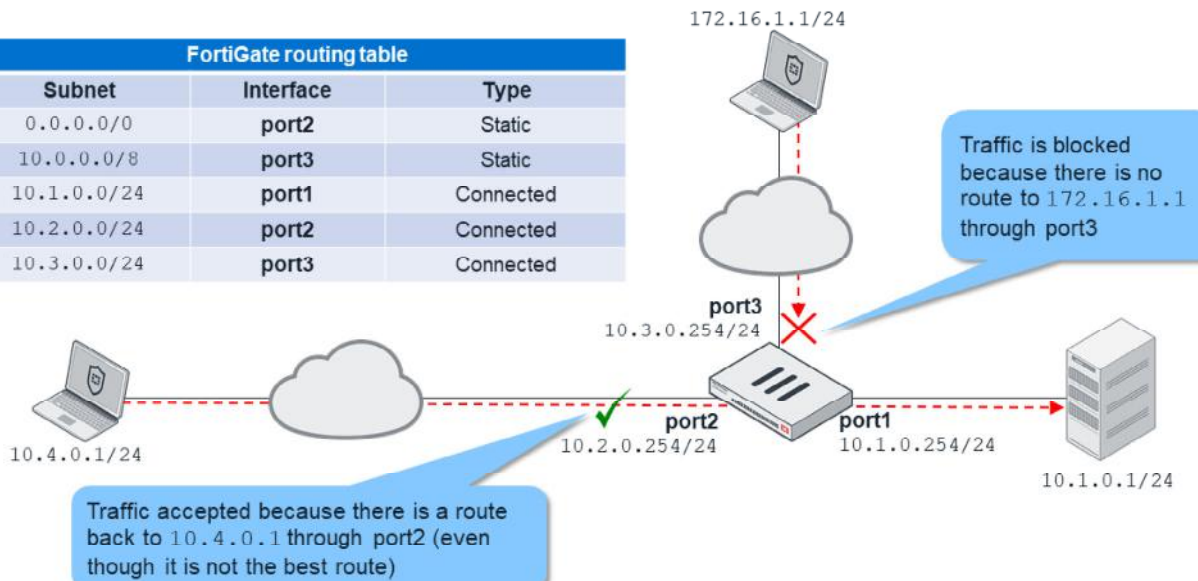
Now, you will review an important routing concept: reverse path forwarding (RPF) check.

RPF check protects against IP spoofing attacks and routing loops by checking the route to the source IP address. This check is performed only on the first packet when the session is being created. If the check fails, the packet is dropped and the debug flow shows this error: `reverse path check fail, drop`.

DO NOT REPRINT
© FORTINET

Feasible Path RPF

FortiGate routing table		
Subnet	Interface	Type
0.0.0.0/0	port2	Static
10.0.0.0/8	port3	Static
10.1.0.0/24	port1	Connected
10.2.0.0/24	port2	Connected
10.3.0.0/24	port3	Connected



FORTINET

© Fortinet Inc. All Rights Reserved.

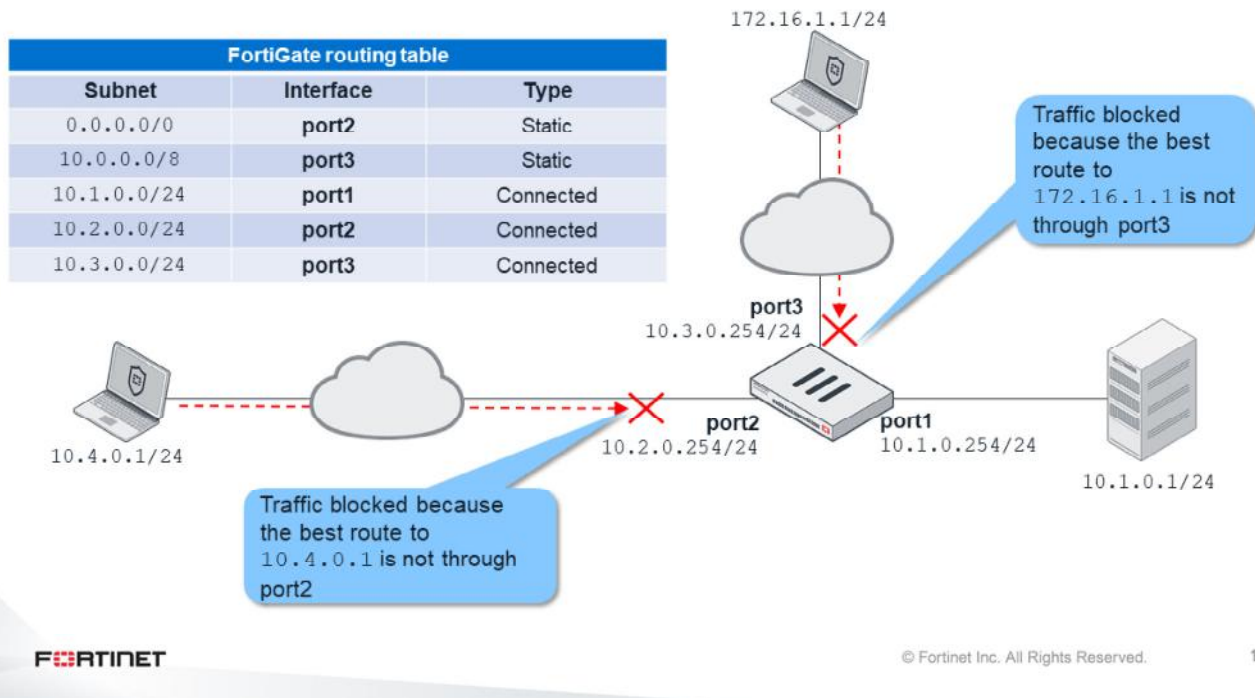
9

There are two RPF check modes: feasible path (formerly known as loose) and strict. Feasible path is the default mode.

In feasible path mode, the packet is accepted as long as there is one active route to the source IP through the incoming interface. It does not have to be the best route, just an active one. In the example shown on this slide, the packet from 10.4.0.1 to 10.1.0.1 is accepted because FortiGate has an active route (the default route) to 10.4.0.1 through port2. However, the packet from 172.16.1.1 to 10.1.0.1 is *not* accepted, because there is no active route to the IP address 172.16.1.1 through port3.

DO NOT REPRINT
© FORTINET

Strict RPF



In strict mode, FortiGate checks that the best route to the source IP address is through the incoming interface. The route not only has to be active (as in the case of feasible path mode), but it also has to be the best.

If you use the same example, but change FortiGate from feasible path mode to strict mode, you will get the following results:

- The packet from 172.16.1.1 to 10.1.0.1 is still blocked because there is no route to the source IP address through port3.
- The packet from 10.4.0.1 to 10.1.0.1 is also blocked. There is an active route to 10.4.0.1 through port2, but it is *not* the best route to the source IP address. The best route to 10.4.0.1 is through port3. So, strict mode accepts traffic from the subnet 10.4.0.0/24 only when port3 is the incoming interface.

DO NOT REPRINT
© FORTINET

Return Packet Routing

- FortiGate remembers the interface to source for the return packets
- The return packet is routed through that interface, even when there is a better route through a different interface
- This ensures the same route path is used for both directions (symmetric routing)

Content inspection requires routing to be kept as symmetric as possible; that is, traffic must follow the same path both ways. There are multiple scenarios where asymmetric routing prevents FortiGate from inspecting traffic content. So, FortiGate routes traffic symmetrically. This means that, under some network topologies, FortiGate might not route the return traffic through the best path, but through the same path that the originating traffic used. For that purpose, FortiGate *remembers* the interface to source and uses that interface to route the return packets, even when a better route using a different interface exists. You will look at an example on the next slides.

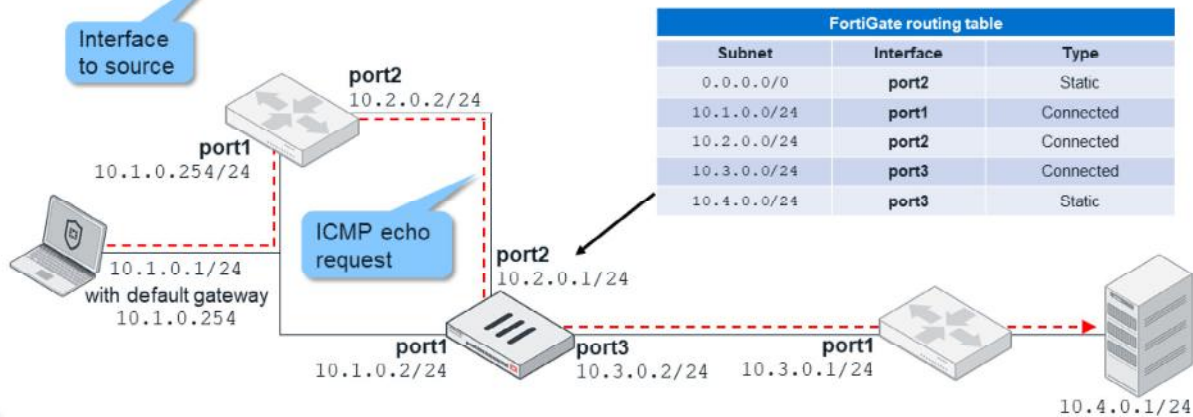
DO NOT REPRINT
© FORTINET

Return Packet Routing Example

- A first routing lookup happens with the first ICMP packet

- FortiGate creates a first entry in the route cache:

```
family=02 tab=254 vrf=0 vf=0 type=01 tos=0 flag=00000200
10.1.0.1@6(port2)->10.4.0.1@9(port3) gwy=10.3.0.1 prefsrc=10.2.0.1
ci: ref=1 lastused=2 expire=0 err=00000000 used=0 br=0 pmtu=1500
```



FORTINET

© Fortinet Inc. All Rights Reserved.

12

Now, you will analyze this network topology. The local network, 10.1.0.0/24 has three network devices: a local workstation, a local router, and a FortiGate port1. Also, the FortiGate port2 is directly connected to the local router (using the subnet 10.2.0.0/24).

There is a remote router connected to FortiGate port3 and, behind that, a remote server (10.4.0.1). So, any traffic destined to the remote server must be routed through FortiGate. One important detail in this network is that the local workstation default gateway is 10.1.0.254. This means that if you send an ICMP echo request from the local workstation to the remote server, the packet goes to the local router first, then to FortiGate, then to the remote router, and finally to the destination. When the ICMP packet arrives at FortiGate, an entry for the originating traffic is created in the unit route cache. This entry contains the interface to source, or the incoming interface where the packet arrived which, in this case, is port2.

DO NOT REPRINT
© FORTINET

Return Packet Routing Example (Contd)

- Routing information is added to the FortiGate session

```
session info: proto=1 proto_state=00 duration=2 expire=57 timeout=0 flags=00000000
socktype=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=60/1/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 29/0 rx speed(Bps/kbps): 29/0
origin->sink: org pre->post, reply pre->post dev=6->9/9->6 gw=10.3.0.1/0.0.0.0
hook=pre dir=org act=noop 10.1.0.1:1->10.4.0.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.4.0.1:1->10.1.0.1:0(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00004e30 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

FORTINET

© Fortinet Inc. All Rights Reserved.

13

Additionally, FortiGate creates an entry in the session table. This entry also contains information about the interface to source.

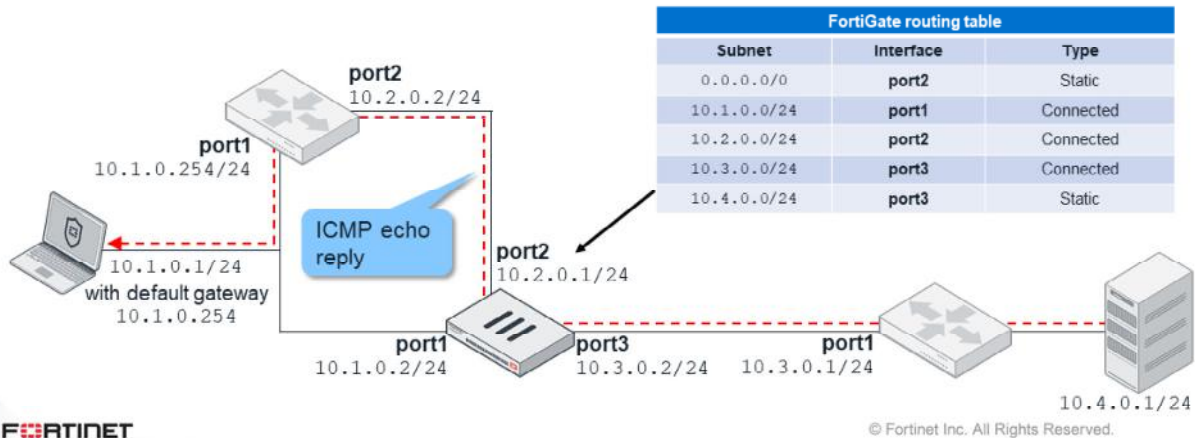
As explained earlier, FortiGate does a first routing lookup to find the next-hop to the destination. That IP address is also stored in the session information.

Because there is no ICMP echo reply yet, you will notice that the next-hop to source is still unknown (it is 0.0.0.0). It will be identified with the second routing lookup that happens with the first reply packet.

Return Packet Routing Example (Contd)

- The return packet is routed through port2, even though port1 is the better route
 - FortiGate creates a second entry in the route cache

```
family=02 tab=254 vrf=0 vf=0 type=01 tos=0 flag=00000200
10.4.0.1@6(port3)->10.1.0.1@9(port2) gwy=10.2.0.2 prefsrc=10.3.0.2
ci: ref=1 lastused=2 expire=0 err=00000000 used=0 br=0 pmtu=1500
```



Now, take a look at how FortiGate routes the return packet.

When FortiGate receives the ICMP echo reply, because there is already a session and a route cache created, it uses the interface to source. So, in this case, the unit routes the packet through port2 toward the local router, even when there is a better route to the destination 10.1.0.1. The FortiGate routing table shows port1 as the best route to 10.1.0.1 (locally connected), but it still uses port2. The objective is to keep the traffic flow symmetric. With the first ICMP echo reply, a second entry is added to the route cache, this time for the return traffic.

DO NOT REPRINT
© FORTINET

Return Packet Routing Example (Contd)

- A second routing lookup is done to find the gateway to source

```
session info: proto=1 proto_state=00 duration=41 expire=21 timeout=0 flags=00000000
socktype=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=240/4/1 reply=240/4/1 tuples=2
tx speed(Bps/kbps): 11/0 rx speed(Bps/kbps): 11/0
origin->sink: org pre->post, reply pre->post dev=6->9/9->6 gwy=10.3.0.1, 10.2.0.2
hook=pre dir=org act=noop 10.1.0.1:1->10.4.0.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.4.0.1:1->10.1.0.1:0(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00005f6a tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

The gateway to source now added to the FortiGate session

FORTINET

© Fortinet Inc. All Rights Reserved.

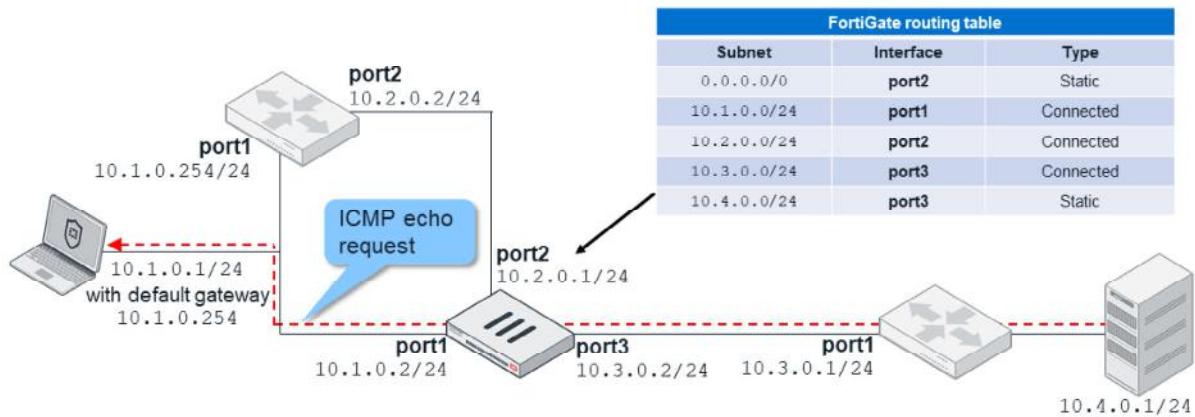
15

Additionally, the unit does a second routing lookup, this time to find the next-hop (or gateway) to the source. That IP address is added to the session, which was previously set to 0.0.0.0.

DO NOT REPRINT
© FORTINET

Return Packet Routing Example (Contd)

- If the session originated from the other side, the packet will be routed through port1



FORTINET

© Fortinet Inc. All Rights Reserved.

16

What happens if the traffic originates from the server side instead?

Say that the ping is sent from the remote server to the local workstation. In this case, when the ICMP echo request arrives at FortiGate, there is no session yet. So, FortiGate uses the best route to 10.1.0.1, which is through port1.

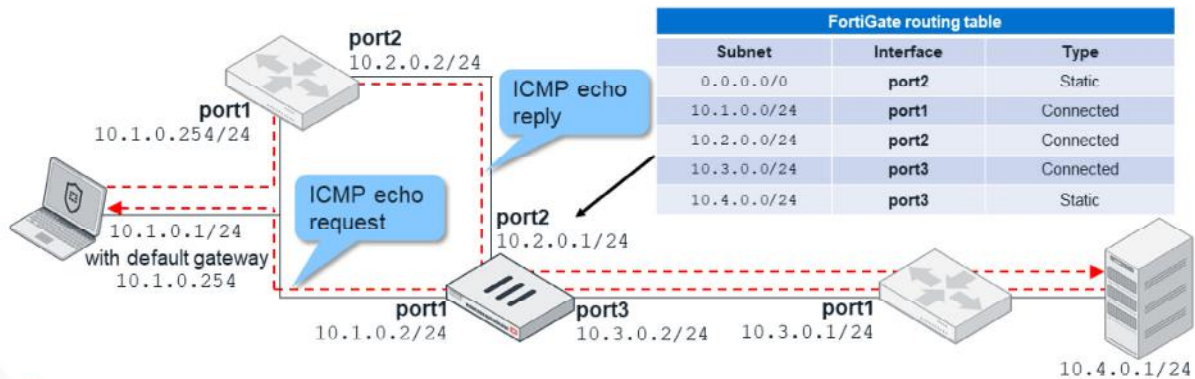
This example shows how FortiGate might, in some network topologies, route packets to the same destination differently, depending on who initiated the session.

DO NOT REPRINT
© FORTINET

Return Packet Routing Example (Contd)

- The return packet arrives through a different interface (port2), but FortiGate accepts it

```
430.637135 port3 in 10.4.0.1 -> 10.1.0.1: icmp: echo request
430.637180 port1 out 10.4.0.1 -> 10.1.0.1: icmp: echo request
430.637309 port2 in 10.1.0.1 -> 10.4.0.1: icmp: echo reply
430.637319 port3 out 10.1.0.1 -> 10.4.0.1: icmp: echo reply
```



FORTINET

© Fortinet Inc. All Rights Reserved.

17

Take a look at the reply traffic in this example.

Because the local workstation default gateway is 10.1.0.254, the ICMP echo reply goes to the local router first. Then, the packet arrives at FortiGate port2. The result is asymmetric routing: the return traffic is following a different path than the originating traffic. The return packet is arriving at port2 instead of port1 (where the originating traffic was sent).

In these particular cases, FortiGate accepts this asymmetry, no packets are dropped, and security inspection is not affected.

Routing Changes Without Source NAT

- After a routing change, routing information is flushed from the affected sessions where source NAT (SNAT) is not applied:
 - Routing lookups are done again for the next packets
 - Route cache entries are removed
 - Session is flagged as dirty
- Example of a session just after a routing change

```
session info: proto=1 proto_state=00 duration=411 expire=56 timeout=0 flags=00000000
socktype=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=17160/286/1 reply=16080/268/1 tuples=2
tx speed(Bps/kbps): 98/0 rx speed(Bps/kbps): 98/0
origin->sink: org pre->post, reply pre->post dev=9->0/0->9 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.4.0.1:1->10.1.0.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.1:1->10.4.0.1:0(0.0.0.0:0)
```

Dirty flag

Interface and gateway information removed

FORTINET

© Fortinet Inc. All Rights Reserved.

18

When FortiGate is not applying SNAT, after a change in the routing table, the routing information is removed from the sessions that are affected by the change. Additionally, related route cache entries are deleted. So, two more routing lookups are done for the next packets in order to learn the new routing information and store it in the routing table.

This slide shows a sample of a session just after a routing change. The gateways in both directions change to 0.0.0.0/0 and the interfaces to 0, indicating that this information must be learned again. Additionally, the dirty flag is added.

DO NOT REPRINT
© FORTINET

Routing Changes Without SNAT

- You can modify the default behavior on the CLI

```
config system interface
  edit <interface>
    set preserve-session-route { enable | disable }
  next
end
```

Default setting

- disable**: FortiGate flushes all routing information from session table after a route change, and performs new routing lookup for new packets
- enable**: FortiGate marks existing session routing information as persistent, and only applies the modified routes to new sessions

You can configure session route persistence at the interface level using the commands shown on this slide. The default value is **disable**. If you enable this setting, sessions passing through that interface will continue to pass without being affected by the routing changes. The routing changes will apply only to new sessions.

DO NOT REPRINT
© FORTINET

Routing Changes and SNAT

- In sessions where SNAT is applied, the action depends on the following setting (which is disabled by default):

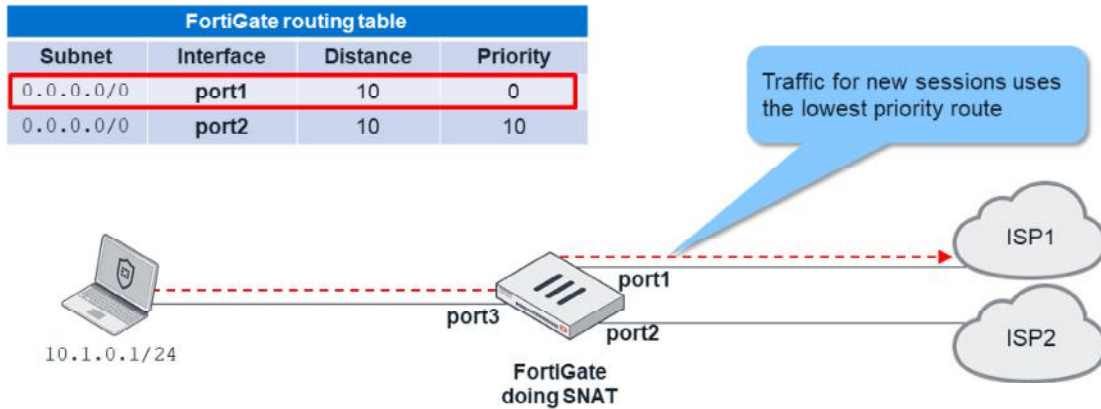
```
config system global
    set snat-route-change [disable | enable]
end
```

In sessions where SNAT is applied, the action that FortiGate takes after a routing change depends on the `snat-route-change` setting.

DO NOT REPRINT
© FORTINET

SNAT Route Change Disable

- When `snat-route-change` is disabled, after a routing change, sessions with SNAT keep using the same outbound interface, as long as the old route is still active



FORTINET

© Fortinet Inc. All Rights Reserved.

21

When this setting is disabled, the behavior that occurs after a routing change is different for sessions using SNAT. Sessions using SNAT keep using the same outbound interface, as long as the old route is still active.

In the example shown on this slide, FortiGate is connected to two different ISPs. A client with the IP address 10.1.0.1/24 is connected behind a FortiGate. FortiGate is doing SNAT of the client traffic to a public IP address, depending on which ISP is using it. The FortiGate routing table contains two default routes: one for each ISP. The two default routes are the same distance, but have different priorities. The route with the lowest priority (port1) is the primary. When both ISP connections are up, the primary route is selected by FortiGate for internet traffic. So, all sessions to the internet are created using port1 as the outbound interface.

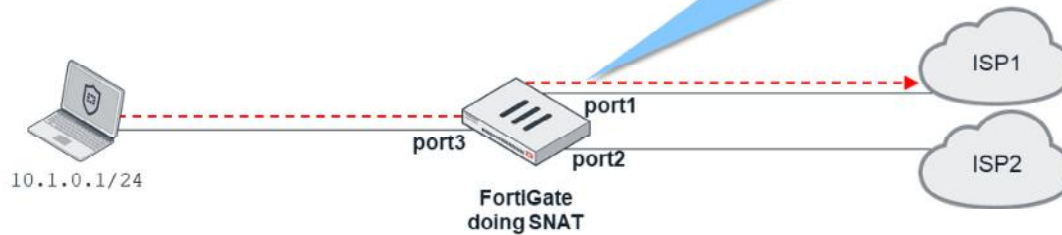
DO NOT REPRINT
© FORTINET

SNAT Route Change Disabled (Contd)

- When `snat-route-change` is disabled, after a routing change, sessions with SNAT keep using the same outbound interface, as long as the original route is still active

FortiGate routing table			
Subnet	Interface	Distance	Priority
0.0.0.0/0	port1	10	20
0.0.0.0/0	port2	10	10

After increasing port1 priority, existing SNAT sessions keep using port1 because the route is still active (even though it is no longer the best route)



FORTINET

© Fortinet Inc. All Rights Reserved.

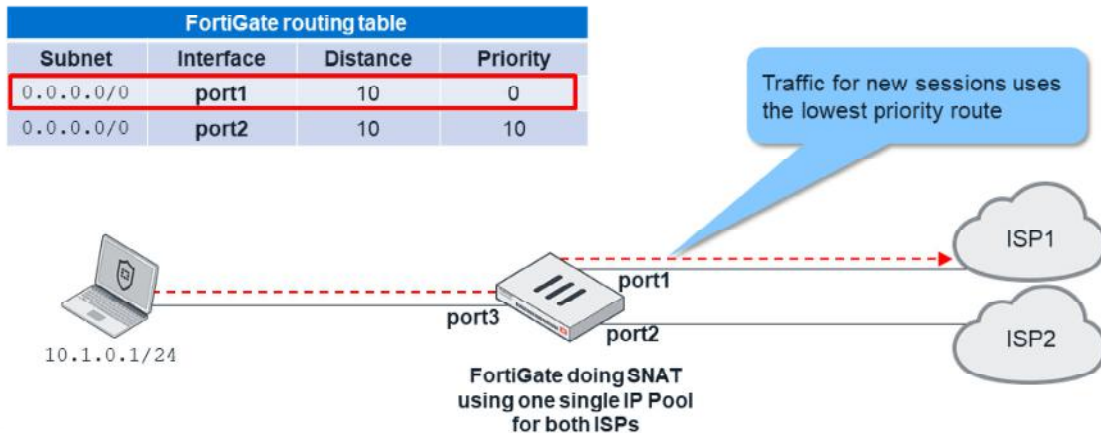
22

If you increase the priority assigned to port1 to a value that is higher than the value assigned to port2, and if `snat-route-change` is disabled, all *new* sessions start using port2, because it has the lowest priority. However, all the *existing* sessions continue to use port1. The default route is through **port1**. Even though the default route is no longer the best route, it is still active. If FortiGate is doing SNAT, the existing sessions will continue to use the original route until they expire. If FortiGate isn't doing SNAT, all the existing sessions will switch to **port2** after the change.

DO NOT REPRINT
© FORTINET

SNAT Route Change Enabled

- When `snat-route-change` is enabled, after a routing change, routing information is flushed from existing SNAT sessions; so, the existing SNAT sessions can use any new best route



FORTINET

© Fortinet Inc. All Rights Reserved.

23

When this setting is enabled, after a routing change, the actions are the same as they are for sessions without SNAT:

- Routing information is flushed from the session table
- Route cache entries are removed
- Routing lookups are done again for the next packets, which can potentially change the outbound interface being used to route the traffic
- RPF check is done again for the first packet in the original direction

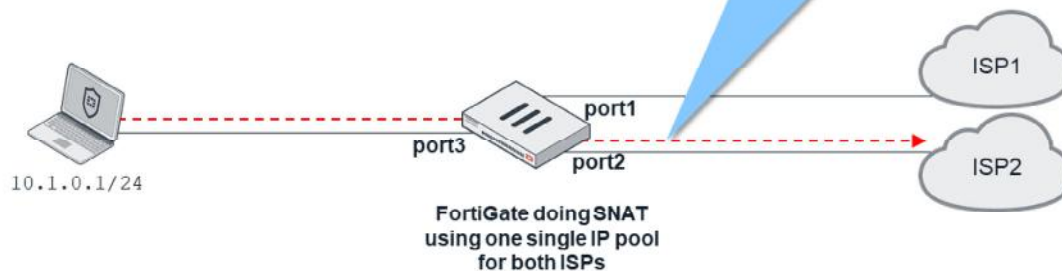
In the example shown on this slide, FortiGate is connected to two different ISPs. A client with the IP address 10.1.0.1/24 is connected behind a FortiGate device. The FortiGate routing table contains two default routes: one for each ISP. The two default routes are the same distance, but have different priorities. The route with the lowest priority (port1) is the primary. When both ISP connections are up, the primary route is selected by FortiGate for internet traffic. So, all sessions to the internet are created using port1 as the outbound interface.

DO NOT REPRINT
© FORTINET

SNAT Route Change Enabled (Contd)

- If the new best route shared a common IP pool with the old best route, the SNAT session will continue to use the same public IP address to translate the original source IP address

FortiGate routing table			
Subnet	Interface	Distance	Priority
0.0.0.0/0	port1	10	20
0.0.0.0/0	port2	10	10



FORTINET

© Fortinet Inc. All Rights Reserved.

24

The scenario shown on this slide has multiple ISPs. If the customer owns a pool of public IP addresses, the customer can configure a single IP pool for SNAT for all the internet providers. The advantage is that if the main ISP goes down, sessions are routed through a secondary ISP, maintaining the same public source IP address. In this way, sessions can remain up.

So, in the example shown on this slide, if you increase the priority for port1 to a value higher than the priority for port2, and if `snat-route-change` is enabled, after a routing change, routing information is flushed from existing SNAT sessions. All sessions start using port2, because it has the lowest priority. Additionally, if the port2 route shared a common IP pool with the old best route of port1, the SNAT session will keep using the same public IP addresses for the translation of the private IP addresses.

DO NOT REPRINT
© FORTINET

ECMP Acceleration With Auxiliary Session

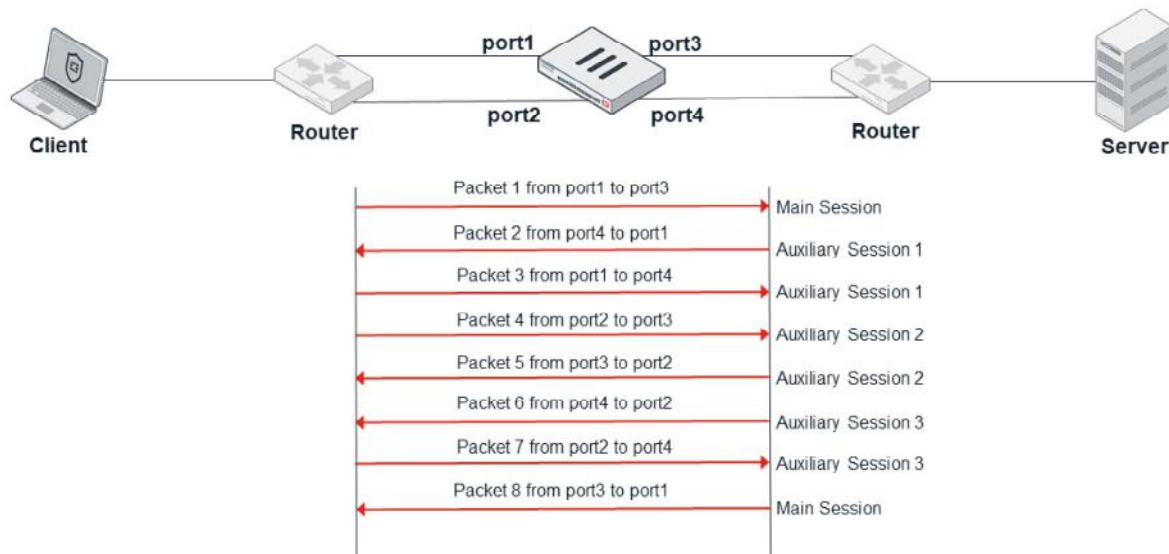
- With this setting enabled, ECMP traffic is accelerated to the NP6 processor

```
config system settings
    set auxiliary-session [disable | enable]
end
```
- Two sessions will be created in case of a route change: main session and auxiliary session
- The main session and the auxiliary session can be offloaded to the NP6 processor, if the policy allows offloading

With auxiliary-session enabled, the FortiGate kernel will create a new auxiliary session and attach it to the main session. For each traffic path (incoming or outgoing), FortiGate will continue to create a new auxiliary session.

DO NOT REPRINT
© FORTINET

ECMP Acceleration With Auxiliary Session (Contd)



FORTINET

© Fortinet Inc. All Rights Reserved.

26

In this example, ECMP is configured for both client and server. FortiGate uses ECMP through port1 and port2 to the client, and ECMP through port3 and port4, to the server.

Based on this example, you will see how sessions are handled on FortiGate:

- Initially, traffic is coming from port1 to port3. FortiGate creates a new session: the main session.
- The reply from the server comes from port4 to port1. FortiGate creates auxiliary session 1 and attaches it to the main session.
- The client sends traffic from port1 to port4. FortiGate matches auxiliary session 1.
- The client sends traffic from port2 to port3. FortiGate creates auxiliary session 2 and attaches it to the main session.
- The server replies back from port3 to port2. FortiGate matches auxiliary session 2.
- The server replies back from port4 to port2. FortiGate creates auxiliary session 3 and attaches it to the main session.
- The client sends traffic from port2 to port4. FortiGate matches auxiliary session 3.
- Finally, the server replies back from port3 to port1. FortiGate matches main session.

All of these sessions can be offloaded if the policy allows offloading.

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

* - candidate default

Routing table for VRF=0

```
O*E2 0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C      172.16.78.0/24 is directly connected, wan2
C      192.168.3.0/24 is directly connected, dmz
C      192.168.11.0/24 is directly connected, internal
S      192.168.96.0/19 [10/0] is directly connected, linkA0
S      192.168.192.0/19 [10/0] is directly connected, linkB0
O      192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
```

Route source

Distance

Metric

FORTINET

© Fortinet Inc. All Rights Reserved.

27

The command shown on this slide displays all the active routes in the routing table. The left column indicates the source for the route. The first number inside the square brackets is the distance, and the second number is the metric.

This command shows only installed routes in the RIB. For example, if you had two static routes to the same destination subnet with different distances, the one with the shorter distance would be installed, and the one with the longer distance would not.

Routing Table (Contd)

```
# 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

> - selected route, * - FIB route, p - stale info

Routing table for VRF=0

```
S      0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive
```

```
C      *> 10.1.0.0/24 is directly connected, port3
```

```
S      *> 10.1.4.0/24 [10/0] via 10.1.0.100, port3
```

```
S      *> 10.1.10.0/24 [10/0] via 10.1.0.1, port3
```

```
C      *> 100.64.2.0/24 is directly connected, port2
```

Shows all routes in the routing database, including inactive routes

FORTINET

© Fortinet Inc. All Rights Reserved.

28

If you want to display both installed and non-installed routes, use the command shown on this slide. In the example shown on this slide, the output shows one inactive route. The route is shown as inactive when:

- Its gateway is detected dead by link monitor
- Its interface is administratively down
- Its interface has a link down

Other routes that exist only in a routing database and are not marked as inactive, are there because they were not selected as the best route for a destination and thus were not installed in the RIB. For example:

- Two static default routes with different distances. The one with the lower distance appears in the RIB and the one with the higher distance appears in the database only.
- Two default routes, one of them is static and the other is BGP. The static one is preferred and thus appears in the RIB, but the BGP one is listed in the database only.

DO NOT REPRINT
© FORTINET

Forwarding Information Base

```
# get router info kernel
```

Priority

```
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>192.168.171.120/25 pref=192.168.171.227 gwy=0.0.0.0 dev=2(port1)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>192.168.109.0/24 pref=192.168.109.130 gwy=0.0.0.0 dev=3(port2)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0
pref=0.0.0.0 gwy=192.168.171.254 dev=2(port1)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>127.255.255.255/32 pref=127.0.0.1 gwy=0.0.0.0 dev=7(root)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>192.168.109.255/32 pref=192.168.109.130 gwy=0.0.0.0 dev=3(port2)
```

FORTINET

© Fortinet Inc. All Rights Reserved.

29

This low-level command shows the FIB, which is the routing information that the kernel uses to route traffic. All active routes in the routing table must be present in the FIB. Additionally, the FIB may contain routes that are not in the routing table, but were automatically added by FortiGate, such as routes that are dynamically added to reach SSL VPN users.

DO NOT REPRINT
© FORTINET

Route Cache

```
# diagnose ip rtcache list

family=02 tab=254 vrf=0 vf=0 type=01 tos=0 flag=00000200
172.25.188.162@0->172.25.181.152@2(port1) gwy=172.25.188.1 prefsrc=0.0.0.0
ci: ref=2 lastused=0 expire=0 err=00000000 used=2 br=0 pmtu=1500

family=02 tab=254 vrf=0 vf=0 type=01 tos=0 flag=00000200
10.4.0.1@8(port3)->10.1.0.1@5(port2) gwy=10.2.0.2 prefsrc=0.0.0.0
ci: ref=2 lastused=6 expire=0 err=00000000 used=0 br=0 pmtu=1500
```

FORTINET

© Fortinet Inc. All Rights Reserved.

30

The route cache contains recently used routing entries in a quick-to-search table. It is consulted before the routing table, to speed up the routing lookup process.

DO NOT REPRINT
© FORTINET

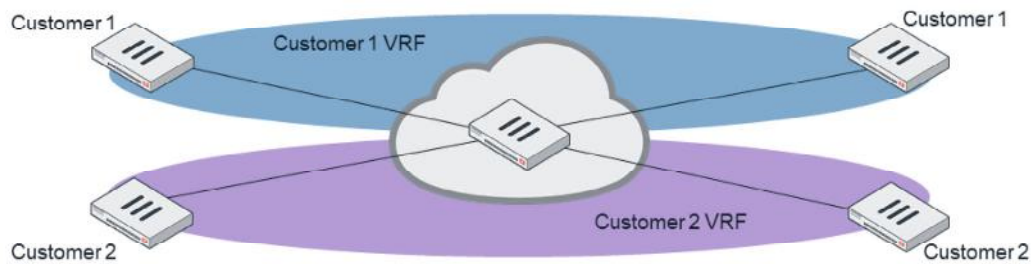
Virtual Routing and Forwarding

In this section, you will learn about virtual routing and forwarding.

DO NOT REPRINT
© FORTINET

Virtual Routing and Forwarding

- Multiple instances of a routing table in a single router
- Allows network segmentation without needing more devices
 - Traffic segregation increases security
- Commonly used by ISPs to create separate VPNs for customers
 - Because the routing instances are independent, overlapping IP addresses at customer site aren't an issue



FORTINET

© Fortinet Inc. All Rights Reserved.

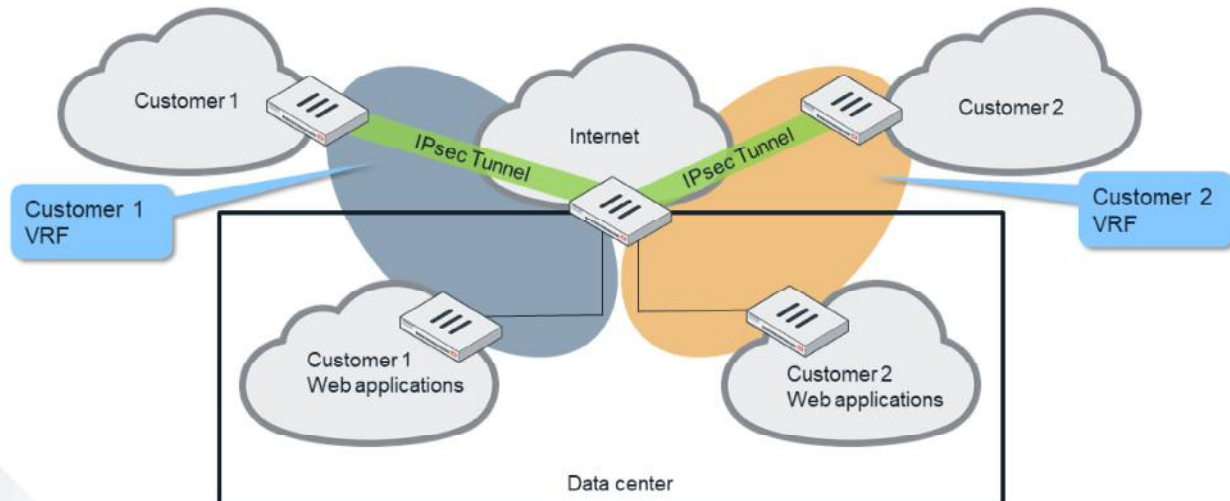
32

Virtual routing and forwarding (VRF) is a technology included in some routers that allows multiple instances of a routing table to exist in a router. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security. Internet service providers often take advantage of VRFs to create separate VPNs for customers.

DO NOT REPRINT
© FORTINET

Multi-Tenant Data Centers

- Separate VRFs for each customer, and their application traffic



© Fortinet Inc. All Rights Reserved.

33

This slide shows another example of a data center service provider. Using VRFs, the service provider achieves full Layer 3 path isolation. VRFs can include IPsec interfaces, so the routing isolation stretches all the way to the tunnel termination at the data center edge. This setup reduces the configuration complexity, when compared to a similar solution you can achieve using VLANs.

DO NOT REPRINT
© FORTINET

Configuring VRF

- VRF ID is configured on interfaces
 - Physical, VLAN, IPsec, switch, and aggregate interfaces are supported
 - Interfaces with matching IDs are isolated to that specific VRF instance
- Supports up to 32 VRFs
- OSPF and BGP supports VRF
- RIP does not support VRF
- Supports route leaking between VRFs

```
# config system interface
edit "port1"
    set vrf 2
next
edit "port2"
    set vrf 2
next
edit "port3"
    set vrf 1
next
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

34

FortiGate supports Layer 3 routing isolation using VRFs. You can configure a VRF ID on an interface. A wide range of interfaces are supported, such as physical, VLAN, IPsec, switch, and aggregate interfaces. Interfaces with matching VRF IDs are isolated to a VRF instance.

This slide shows the commands required to configure a VRF ID on an interface. The VRF ID is an integer between 0 and 31.

OSPF and BGP are the only dynamic routing protocols that support VRF. RIP does not support VRF.

FortiGate also supports route leaking capabilities between locally defined VRFs.

DO NOT REPRINT
© FORTINET

VRF Routing Table

```
# get router info routing-table all
```

Routing table for VRF=1

```
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
* - candidate default
```

```
S* 0.0.0.0/0 [10/0] via 100.64.1.254, port1
C 10.1.0.0/24 is directly connected, port3
S 10.1.4.0/24 [10/0] via 10.1.0.100, port3
S 10.1.10.0/24 [10/0] via 10.1.0.1, port3
C 100.64.1.0/24 is directly connected, port1
```

port1 and port3 are
in the same VRF
instance

Routing table for VRF=2

```
C 100.64.2.0/24 is directly connected, port2
```

port2 is isolated to a
separate VRF
instance

FORTINET

© Fortinet Inc. All Rights Reserved.

35

After you configure VRF IDs on interfaces, the routing table diagnostic command output changes. FortiGate groups routes based on VRF ID. From the routing table output shown on this slide, you can see that port1 and port3 are in the same VRF instance (VRF=1), and port2 is segregated in a separate VRF instance (VRF=2).

DO NOT REPRINT
© FORTINET

VRF Routing Table Database

```
# get router info routing-table database
```

Routing table for VRF=1

```
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
        > - selected route, * - FIB route, p - stale info
```

```
S      0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive
C      *> 10.1.0.0/24 is directly connected, port3
S      *> 10.1.4.0/24 [10/0] via 10.1.0.100, port3
S      *> 10.1.10.0/24 [10/0] via 10.1.0.1, port3
```

Routing table for VRF=2

```
C      *> 100.64.2.0/24 is directly connected, port2
```

FORTINET

© Fortinet Inc. All Rights Reserved.

36

The routing table database output also changes. Both active and inactive routes are grouped based on their VRF instance.

DO NOT REPRINT
© FORTINET

VRF Route Cache

```
# diagnose ip rtcache list
```

```
family=02 tab=254 vrf=1 vf=0 type=03 tos=0 flag=90000200
0.0.0.0@0->10.1.0.255@9(port3) gwy=0.0.0.0 prefsrc=10.1.0.254
ci: ref=0 lastused=58 expire=0 err=00000000 used=4 br=0 pmtu=1500
```

```
family=02 tab=254 vrf=1 vf=0 type=01 tos=0 flag=04000200
10.1.0.241@9(port3)->100.64.5.1@3(port1) gwy=100.64.1.254
prefsrc=10.1.0.254
ci: ref=1 lastused=10 expire=0 err=00000000 used=0 br=0 pmtu=1500
```

```
family=02 tab=254 vrf=2 vf=0 type=03 tos=0 flag=90000200
0.0.0.0@0->100.64.2.255@6(port2) gwy=0.0.0.0 prefsrc=100.64.2.1
ci: ref=0 lastused=58 expire=0 err=00000000 used=4 br=0 pmtu=1500
```

FORTINET

© Fortinet Inc. All Rights Reserved.

37

The route cache entries will also show VRF ID information for recently used route entries.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand routing table lookup
- ✓ Describe the route selection process
- ✓ Configure reverse path forwarding check
- ✓ Configure return packet routing
- ✓ Understand routing changes and existing sessions
- ✓ Review general routing debug commands

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

DO NOT REPRINT
© FORTINET

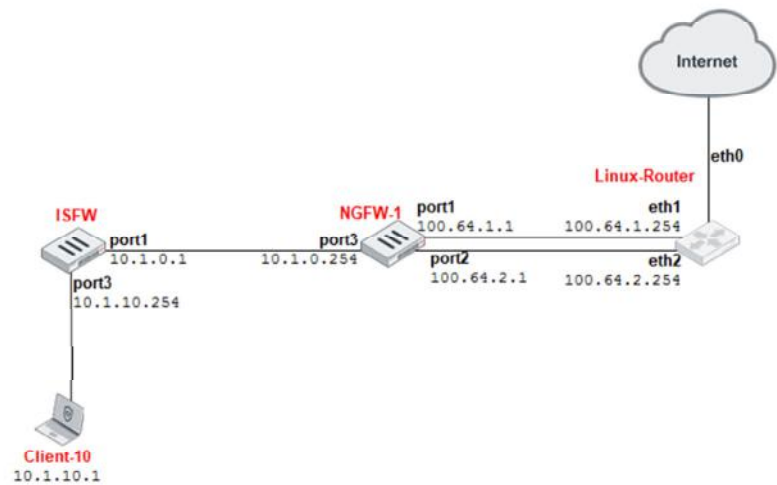
Lab 4—Routing

Now, you will work on *Lab 5—Routing*.

DO NOT REPRINT
© FORTINET

Lab 4—Routing

- Analyze the information in the routing table
- Troubleshooting:
 - Both default routes must be active
 - **port1** must be the primary default route



FORTINET

© Fortinet Inc. All Rights Reserved.

40

In this lab, you will use routing debug information on FortiGate to troubleshoot routing problems.

DO NOT REPRINT
© FORTINET



In this lesson you will learn about FortiGuard. You will also learn how to troubleshoot problems that occur when FortiGate is connecting to public FortiGuard services, and when FortiManager is acting as a local FortiGuard server.

DO NOT REPRINT
© FORTINET

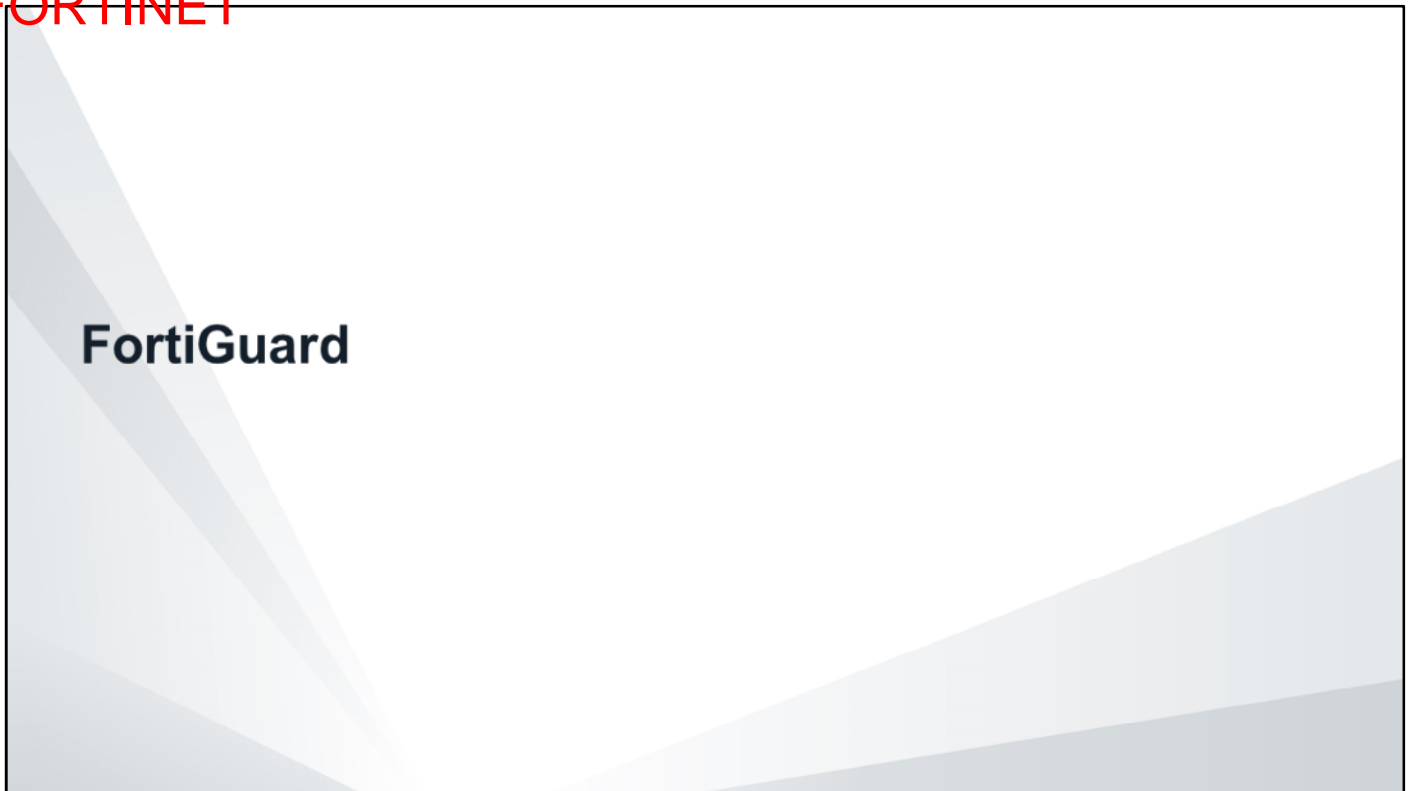
Objectives

- Monitor the status of FortiGuard updates
- Use FortiManager as a local FortiGuard server
- Troubleshoot common FortiGuard issues

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

By demonstrating competence in FortiGuard, and how FortiGate connects to public FortiGuard servers, you will be able to troubleshoot problems that occur when FortiGate is connecting to public FortiGuard services, and when FortiManager is acting as a local FortiGuard server.

DO NOT REPRINT
© FORTINET



In this section, you will learn how FortiGate connects to public FortiGuard servers.

DO NOT REPRINT
© FORTINET

FortiGuard Distribution Network



FORTINET

© Fortinet Inc. All Rights Reserved.

4

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

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

DO NOT REPRINT
© FORTINET

FortiGuard Ports

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

5

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

In the case of rating services, and when communicating with public FortiGuard services, FortiGate uses one of these ports:

- UDP port 8888
- UDP port 53
- HTTPS port 8888
- HTTPS port 53
- HTTPS port 443

In the case of rating services, and when communicating with a FortiManager configured as a local FortiGuard server, FortiGate uses one of these ports:

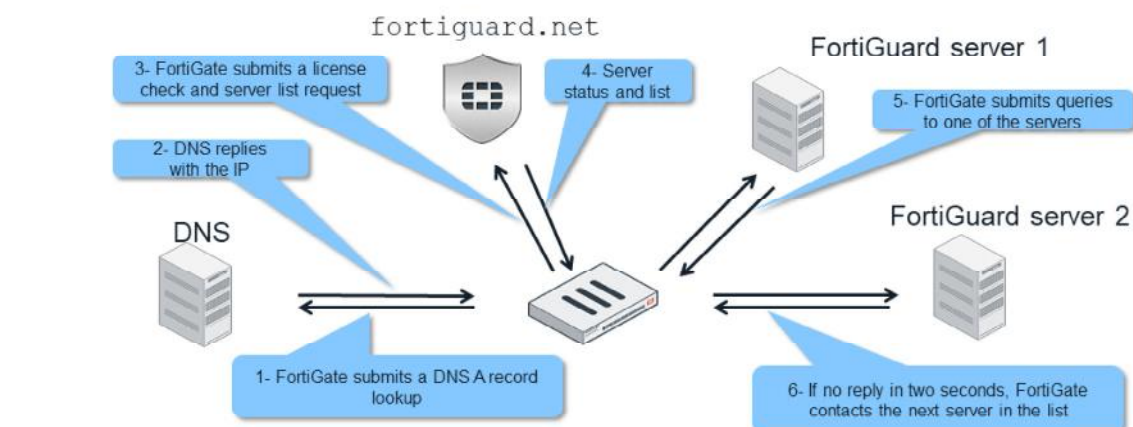
- UDP port 8888
- UDP port 53
- HTTP port 8888
- HTTPS port 53

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

By default, FortiGate uses public FortiGuard servers located worldwide. You can configure FortiGate to use public FortiGuard servers located only in USA.

DO NOT REPRINT
© FORTINET

FortiGuard Web Filtering and Antispam



- FortiGate submits a DNS lookup to get the IP address for one of these names:

- `service.fortiguard.net`: UDP and worldwide servers
- `securewf.fortiguard.net`: HTTPS and worldwide servers
- `usservice.fortiguard.net`: UDP and USA-based-only servers
- `ussecurewf.fortiguard.net`: HTTPS and USA-based-only servers

FORTINET

© Fortinet Inc. All Rights Reserved.

6

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

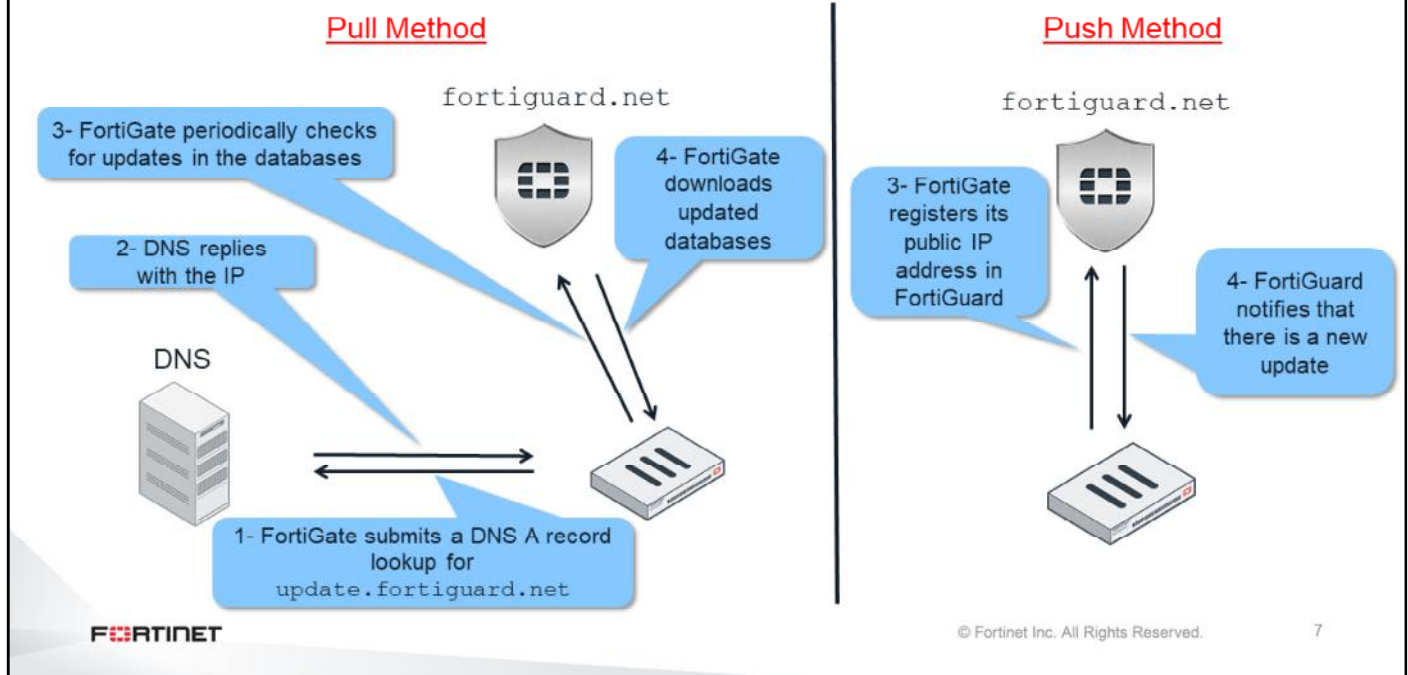
1. FortiGate contacts the DNS server to resolve the FortiGuard service name.
2. FortiGate gets a list of IP addresses for servers (usually two or three) that can be contacted to validate the FortiGuard license.
3. FortiGate contacts one of those servers to check the license, and obtains a list of servers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

The FortiGuard service name depends on the FortiGate configuration:

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

DO NOT REPRINT
© FORTINET

FortiGuard Antivirus and IPS



Now you will look at how antivirus and IPS work. How FortiGuard communication works for antivirus and IPS depends on the method used: pull or push.

The steps in the pull method are:

1. FortiGate contacts the DNS server to resolve the name `update.fortiguards.net`.
2. FortiGate gets a list of server IP addresses (usually two or three) that can be contacted.
3. FortiGate periodically connects to one of the servers to check for pending updates.
4. If there is an update, FortiGate downloads the update.

The first two steps used for the push method are also used for the pull method: FortiGate gets a list of IP addresses from a DNS server for the domain name `update.fortiguards.net`. After that, FortiGate registers its public IP address in FortiGuard. With this information, FortiGuard starts sending notifications each time there are new updates. FortiGate then proceeds to download the updates.

DO NOT REPRINT
© FORTINET

FDN Status on FortiGate

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



FORTINET

System > FortiGuard

FortiGuard Distribution Network		
License Information		
Entitlement	Status	
FortiCare Support	Registered - courseware@fortinet.com	Launch Portal
Enhanced Support	24x7 support - expires on 2020/11/10	
Virtual Machine	Valid	FortiGate VM License
Allocated vCPUs	100% 1/1	
Allocated RAM	49% 1002 MiB/ 2 GiB	
Firmware & General Updates	Licensed - expires on 2020/11/10	
Application Control Signatures	Version 14.00626	Upgrade Database
Device & OS Identification	Version 1.00075	
Internet Service Database Definitions	Version 6.00143	
Intrusion Prevention	Licensed - expires on 2020/11/10	
IPS Definitions	Version 14.00626	Upgrade Database
IPS Engine	Version 4.00219	
Malicious URLs	Version 2.00323	
Botnet IPs	Version 4.00494	View List
Botnet Domains	Version 2.00259	View List
AntiVirus	Licensed - expires on 2020/11/10	
AV Definitions	Version 1.00000	Upgrade Database
AV Engine	Version 6.00127	
Mobile Malware	Version 69.00056	
Outbreak Prevention	Licensed - expires on 2020/11/10	
Industrial DB	Licensed - expires on 2020/11/10	
Industrial Attack Definitions	Version 14.00626	
Security Rating	Licensed - expires on 2020/11/10	
Security Rating Package	Version 2.00020	
Web Filtering	Licensed - expires on 2020/11/10	

© Fortinet Inc. All Rights Reserved.

8

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

DO NOT REPRINT
© FORTINET

FortiGuard Troubleshooting (Web Filtering and Antispam)

FortiGate # diagnose debug rating

Locale : english
Service : Web-filter
Status : Enable
License : Contract
Service : Antispam
Status : Disable
Service : Virus Outbreak Prevention
Status : Disable

Round trip delay

Server's
time zone

Consecutive requests
sent with no reply

Historical requests sent
with no reply; resets upon
device reboot

-- Server List (Tue Jun 4 15:32:55 20xx) --

IP	Weight	RTT	Flags	TZ	Packets	Curr Lost	Total Lost
69.195.205.101	10	45		-5	262432	0	846
69.195.205.102	10	46		-5	329072	0	6806
209.222.147.43	10	75		-5	71638	0	275
96.45.33.65	20	71		-8	36875	0	92
208.91.112.196	20	103	DI	-8	34784	0	1070
208.91.112.198	20	107	D	-8	35170	0	1533
80.85.69.41	60	144		0	33728	0	120
62.209.40.73	71	226		1	33797	0	192
121.111.236.180	150	97		9	33754	0	145
69.195.205.103	45	44	F	-5	26410	26226	26227

FORTINET

© Fortinet Inc. All Rights Reserved.

9

The command shown on this slide displays the list of servers for web filtering and antispam queries. For each IP address, the table shows:

- The round trip delay
- The server's time zone
- The number of recent and consecutive queries without reply
- The historical total number of queries without reply. These values are reset when the device restarts.

DO NOT REPRINT
© FORTINET

FortiGuard Weight Calculation

- Initial value is the delta between the FortiGuard server's time zone and the FortiGate's system time zone, multiplied by 10
- The weight goes up with each packet lost
- The weight goes down over time if no packets are lost, but never goes below the initial value
- FortiGate uses the server with the lowest weight
 - If the weights are the same, FortiGate uses the lowest RTT

FORTINET

© Fortinet Inc. All Rights Reserved.

10

This is how FortiGate selects the server to send the rating requests to:

- FortiGate initially uses the delta between the server's time zone and the FortiGate's system time zone multiplied by 10.
 - This is the server's initial weight. To lower the possibility of using a remote server, the weight is not allowed to drop below the initial weight.
- The weight goes up with each packet lost
- The weight goes down over time if there are no packets lost
- FortiGate uses the server with the lowest weight as the one for the rating queries. If two or more servers have the same weight, FortiGate uses the server with the lowest round-trip delay (RTT).

DO NOT REPRINT
© FORTINET

FortiGuard Flags

- **I = Initial**
 - Server contacted to request contract information and updates
- **D = Default**
 - IP addresses of servers received from DNS resolution
- **S = Serving**
 - IP addresses of servers received from FortiManager
- **T = Timing**
 - Actively timing this connection
 - Server remains in this state for 15 seconds (default) before being considered as failed
- **F = Failed**
 - Server connection has failed
 - FortiGate pings every 15 minutes to check if server has come back

FORTINET

© Fortinet Inc. All Rights Reserved.

11

The output of the command `diagnose debug rating` shows flags beside some of the servers:

- **I** = The server initially contacted to validate the license and get the server list
 - Usually, there is only one server with this flag
- **D** = The IP address FortiGate got when resolving the name `service.fortiguard.net`. If the administrator has not overwritten the FortiGuard FQDN or IP address in the FortiGate configuration, there are usually two or three servers with this flag.
- **S** = The IP address FortiGate got from FortiManager
- **T** = The server is not replying to FortiGate queries
- **F** = The server is down

DO NOT REPRINT
© FORTINET

FortiGuard Common Issues (Web Filtering and Antispam)

- Some ISPs block non-standard traffic over port 53
 - Solution: Use port 8888
- Some ISPs block port-8888 traffic
 - Solution: Use port 53
- Some ISPs block traffic based on the source port
 - Solution

```
config sys global
    set ip-src-port-range 1031-4999
end
```



© Fortinet Inc. All Rights Reserved.

12

In many cases, problems related to FortiGuard are caused by ISPs. Some ISPs block traffic on port 53 that is not DNS or that contains large packets. In those cases, the solution is to switch FortiGuard traffic from port 53 to port 8888.

Other ISPs (or upstream firewalls) block traffic to port 8888. In those cases, the solution is to use port 53.

There are also a few cases where ISPs block traffic based on source ports. Changing the source port range for FortiGuard to the range shown on this slide usually fixes the issue.

DO NOT REPRINT
© FORTINET

FortiGuard Troubleshooting (Antivirus and IPS)

- FortiGate uses port TCP 443 to get updates
 - Can be configured to connect through a web proxy:

```
config system autoupdate tunneling
  set address <proxy_address>
  set password <password>
  set port <proxy_port>
  set status {enable | disable}
  set username <name>
end
```
- When connecting through a web proxy, FortiGate can access FortiGuard without DNS resolution

FORTINET

© Fortinet Inc. All Rights Reserved.

13

For antivirus and IPS, communication between FortiGate and FortiGuard happens much less frequently. In the case of web filtering and antispam, FortiGate goes to FortiGuard each time it needs to rate a website or email (if the information is not in the FortiGate cache). In the case of the pull method for antivirus and IPS, by default FortiGate contacts FortiGuard every two hours to check and download any new version of the antivirus or IPS databases and engines. This is done using port TCP 443.

This slide shows the commands you use if FortiGate must connect through a web proxy. Usually, clients connecting through a web proxy do not contact the DNS server to resolve names, because it is the web proxy that does it. When connecting through a web proxy, FortiGate can access FortiGuard without DNS resolution.

DO NOT REPRINT
© FORTINET

FortiGuard Troubleshooting (Antivirus and IPS) (Contd)

```
# diagnose test application dnsproxy 7
vfid=0, name=service.fortiguard.net, ttl=4879:3562:483
    208.91.112.196 (ttl=4879) 208.91.112.198 (ttl=4879)
vfid=0, name=update.fortiguard.net, ttl=49304:47956:452
    208.91.112.68 (ttl=49304) 208.91.112.91 (ttl=49304) 96.45.33.88
    (ttl=49304) 96.45.33.89 (ttl=49304)

# diagnose autoupdate status
FDN availability:  available at Tue Apr 28 10:49:32 2020

Push update:  disable
Scheduled update:  enable
    Update daily:  at 1 after 40 minutes
Virus definitions update:  enable
IPS definitions update:  enable
Push address override:  disable
Web proxy tunneling:  disable
```

FORTINET

© Fortinet Inc. All Rights Reserved.

14

The command `diagnose test application dnsproxy 7` displays the FQDN and IP addresses of the FortiGuard servers available for antivirus and IPS updates.

The command `diagnose autoupdate status` provides a summary of the FortiGuard configuration on FortiGate.

DO NOT REPRINT
© FORTINET

FortiGuard Update Status

```
diagnose autoupdate versions
```

```
AV Engine
```

```
-----
```

```
Version: 6.00144
```

```
Contract Expiry Date: Sun Nov 6 2022
```

```
Last Updated using manual update on Mon Mar 2 11:53:16 2020
```

```
Last Update Attempt: Wed Apr 29 09:04:04 2020
```

```
Result: No Updates
```

```
Virus Definitions
```

```
-----
```

```
Version: 78.00683
```

```
Contract Expiry Date: Sun Nov 6 2022
```

```
Last Updated using manual update on Mon Apr 13 15:15:00 2020
```

```
Last Update Attempt: Wed Apr 29 10:04:04 2020
```

```
Result: No Updates
```

```
Extended set
```

```
-----
```

```
Version: 76.00683
```

```
Contract Expiry Date: Sun Nov 6 2022
```

```
Last Updated using manual update on Mon Apr 13 19:29:20 2020
```

```
Last Update Attempt: Wed Apr 29 10:31:06 2020
```

```
Result: No Updates
```

```
*****
```

FORTINET

- List includes, but is not limited to:

- Antivirus
- IPS engine
- Mobile malware definitions
- Attack definitions
- IPS malicious URL database
- Botnet definitions
- Device and OS identification
- Internet service
- IP geography
- FortiGuard security rating
- Certificate bundle
- Malicious certificate

© Fortinet Inc. All Rights Reserved.

15

The command shown on this slide lists all the FortiGuard databases and engines installed. The information includes the version, contract expiration date, time it was updated, and what happened during the last update.

DO NOT REPRINT
© FORTINET

FortiGuard Real-Time Debug (Antivirus and IPS)

- Enable real-time debug:

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

FORTINET

© Fortinet Inc. All Rights Reserved.

16

If there are problems updating the antivirus or the IPS, or if there are problems validating the license, you can use the FortiGuard real-time debug to get more information.

After enabling debug, you can force a manual update from the CLI using the command `execute update-now`.

DO NOT REPRINT
© FORTINET

FortiGuard Troubleshooting Tips

- Can the management VDOM access the Internet?
 - FortiGuard traffic originates from the management VDOM
- Does DNS work?
 - Antivirus/IPS (`update.fortiguard.net`)
 - Web filtering/AS (`service.fortiguard.net`)
- Updates to FortiGuard contracts are not instantaneous
 - It usually takes one or two hours to update a contract on all FortiGuard servers. In some cases, it can take up to 24 hours.

FORTINET

© Fortinet Inc. All Rights Reserved.

17

Remember that FortiGuard traffic always originates from the management VDOM. So, the management VDOM (which is `root` by default) must have internet access.

Correct DNS access from the management VDOM is also important. FortiGate must be able to resolve the names:

`update.fortiguard.net`
`service.fortiguard.net`

Also, keep in mind that, although it usually takes one or two hours to update a contract on all the servers, it could take up to 24 hours in some cases. So, if you have just changed or renewed your FortiGuard contract and you do not see the change on FortiGate, most likely you need to wait a bit longer, to give FortiGuard time to synchronize the information on all the servers.

DO NOT REPRINT
© FORTINET

FortiManager As a Local FDS

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

DO NOT REPRINT
© FORTINET

FortiManager—Your Local FortiGuard Cache

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



FORTINET

© Fortinet Inc. All Rights Reserved.

19

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

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

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

DO NOT REPRINT
© FORTINET

FortiGate Configuration—Use FortiManager FDS

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

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

Configure server list to override default FDS servers

Server that FortiGate can use for updates and ratings

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

FORTINET

© Fortinet Inc. All Rights Reserved.

20

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

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

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

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

DO NOT REPRINT
© FORTINET

FortiGuard Licenses Status

FortiManager: FortiGuard > Licensing Status

<input type="checkbox"/>	Device Name	Serial Number	Platform	ADOM	AntiVirus	IPS	Email Filtering	Web Filtering	Support
<input checked="" type="checkbox"/>	ISFW	FGVM010000077646	FortiGate-VM64	Access	2020-11-08	2020-11-08	2020-11-08	2020-11-08	2020-11-08
<input type="checkbox"/>	Spoke-2	FGVM010000077652	FortiGate-VM64	Core	2020-11-08	2020-11-08	2020-11-08	2020-11-08	2020-11-08
<input type="checkbox"/>	Spoke-1	FGVM010000077651	FortiGate-VM64	Core	2020-11-08	2020-11-08	2020-11-08	2020-11-08	2020-11-08
<input type="checkbox"/>	NGFW-1	FGVM010000077649	FortiGate-VM64	Core	2020-11-08	2020-11-08	2020-11-08	2020-11-08	2020-11-08
<input type="checkbox"/>	DCFW	FGVM010000077648	FortiGate-VM64	DC	2020-11-08	2020-11-08	2020-11-08	2020-11-08	2020-11-08

```
# diagnose fmgupdate dbcontract
FGVM010000077651 [SERIAL_NO]
```

```
...
Contract: 12
  AVDB-1-06-20201108
  AVEN-1-06-20201108
  COMP-1-20-20201108
  NIDS-1-06-20201108
  SPRT-1-20-20201108
...
```

Contract Raw Data:

```
Contract=AVDB-1-06-20201108*AVEN-1-06-20201108*COMP-1-20-20201108*ENHN-1-20-20201108*FMSS-1-06-20201108*FMWR-1-06-20201108*FURL-1-06-20201108*HWDR-1-05-20201108*NIDS-1-06-20201108*SBCL-1-06-20201108*SPAM-1-06-20201108*SPRT-1-20-20201108|AccountID=XXXXXXX|Industry=Technology|Company=Fortinet
```

FORTINET

© Fortinet Inc. All Rights Reserved.

21

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

DO NOT REPRINT
© FORTINET

Update Services—Receive Status

- **Receive Status** shows packages received from FortiGuard:

FortiManager: FortiGuard > Package Management > Received Status

<input type="checkbox"/>	Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Version	Update History
<input type="checkbox"/>	Application Signature Dat	FortiGate	6.4.0+	FortiCare	06004000APDB00105	15.00815 (2020-04-10 01:39:00)	265.11 KB	Latest	Change
<input type="checkbox"/>	AntiVirus Signature Data1	FortiGate	6.4.0+	AntiVirus	06004000AVDB00201	76.00683 (2020-04-13 23:20:00)	1.94 MB	Latest	Change
<input type="checkbox"/>	AntiVirus Signature Data1	FortiGate	6.4.0+	AntiVirus	06004000AVDB00701	76.00683 (2020-04-13 23:20:00)	10.82 MB	Latest	Change
<input type="checkbox"/>	Device Detection DB	FortiGate	6.4.0+	Firmware & General Upd	06004000CIDB00000	1.00098 (2020-03-23 13:07:00)	111.08 KB	Latest	Change
<input type="checkbox"/>	Internet Service DB	FortiGate	6.4.0+	Internet Service DB	06004000FFDB00307	76.00607 (2020-04-13 18:42:00)	73.91 KB	Latest	Change

Change Version

Current Version

Change to Version

Latest

76.00683 (2020-04-13 23:20:00)

<input type="checkbox"/>	Date	Event	Status	Download
<input type="checkbox"/>	2020-04-13 16:38:00	Poll Update	Success	76.683(1.94 MB)
<input type="checkbox"/>	2020-04-13 15:46:14	Poll Update	Success	76.681(1.94 MB)
<input type="checkbox"/>	2020-04-13 13:31:46	Poll Update	Success	76.680(1.94 MB)

- This information can also be viewed on the FortiManager CLI using:
 - # diagnose fmupdate fds-getobject

FORTINET

© Fortinet Inc. All Rights Reserved.

22

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

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

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

DO NOT REPRINT
© FORTINET

Update Services—Service Status

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

FortiManager: FortiGuard > Package Management > Service Status

<input type="checkbox"/>	Device Name	Serial Number	Status	Last Update Time
<input type="checkbox"/>	ISFW	FGVM010000077646	Up to Date	2020-05-03 11:17:47
<input type="checkbox"/>	DCFW	FGVM010000077648	Pending	2020-05-03 11:16:52
<input type="checkbox"/>	NGFW-1	FGVM010000077649	Pending	2020-05-03 11:16:42

FORTINET

© Fortinet Inc. All Rights Reserved.

23

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

There are five possible statuses:

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

DO NOT REPRINT
© FORTINET

Update Services—FortiGate Databases

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

```
# diagnose fupdate show-dev-obj
DEVICE(SN:FGVM010000077651):
ID              Status      DeviceVer  ServerVer  PreferVer  License  LicenseType  Description
--              -
02000000FNSD00000 up-to-date 00000.00008 00000.00008 00000.00000 valid      FTMWR        FTM Push Cred
06004000APDB00105 up-to-date 00015.00819 00015.00819 00000.00000 valid      APMS:FMWR    Application
06004000AVDB00201 pending    00076.00753 00076.00755 00000.00000 valid      APMS:AVDB    FGT AVDB
06004000AVDB00701 pending    00076.00753 00076.00755 00000.00000 valid      APMS:AVDB    FGT ETDB.High
06004000CIBD00000 up-to-date 00001.00098 00001.00098 00000.00000 valid      FMWR         Client ID DB
06004000FFDB00307 pending    00007.00618 00007.00619 00000.00000 valid      FMWR         Internet Servi
06004000ISDB00105 up-to-date 00015.00820 00015.00820 00000.00000 no-license APMS:ISSS    Industrial Def
06004000MMDB00101 pending    00076.00753 00076.00755 00000.00000 valid      AVDB         FGT MobileDB
06004000MUDB00103 up-to-date 00002.00615 00002.00615 00000.00000 valid      FMWR         Malicious URL
06004000NIDS02505 up-to-date 00015.00820 00015.00820 00000.00000 valid      APMS:NIDS    Attack Definit
06004000UWDB00100 up-to-date 00002.00742 00002.00742 00000.00000 valid      FMWR         URL Whitelist
...
```



© Fortinet Inc. All Rights Reserved.

24

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

DO NOT REPRINT
© FORTINET

Update Services—Logging

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

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

- These internal log files can be retrieved through SFTP or FTP with the following command:

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



© Fortinet Inc. All Rights Reserved.

25

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

DO NOT REPRINT
© FORTINET

Update Services—Logging (Contd)

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

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

```
2020/05/03 11:23:24.244 info    fds_svr[15858]: [FMG-->FGT] Response: Protocol=3.0|Firmware=FMG-
VM64-FW-6.04-2002|SerialNumber=FMG-VM0A16003351|Response=200|Persistent=false^M ^M
2020/05/03_11:23:24.244 info    fds_svr[15858]: Process client 100.64.5.1:9443 request SUCCESS
2020/05/03_11:23:24.244 notice  fds_worker[15861]: process remote(::ffff:100.64.5.1) SUCCESS!
2020/05/03_11:23:59.219 notice  fds_worker[15861]: accept connection from ::ffff:100.64.3.1.
2020/05/03_11:23:59.249 info    fds_svr[15858]: Start fds server session from 127.0.0.1
2020/05/03_11:23:59.250 info    fds_svr[15858]: [FGT-->FMG] Request:
Protocol=3.0|Command=VMSetup|Firmware=FGVM64-FW-6.04-
1579|SerialNumber=FGVM010000077651|Connection=Internet|Address=100.64.3.1:9443|Language=en-
US|TimeZone=-7|UpdateMethod=0|Uid=ad592e42a0c1c9476c10277b5e04d6d0|VMPlatform=VMWARE^M ^M
2020/05/03 11:23:59.250 info    fds_svr[15858]: [FGT-->FMG] Request:
Protocol=3.0|Command=VMSetup|Firmware=FGVM64-FW-6.04-
1579|SerialNumber=FGVM010000077651|Connection=Internet|Address=100.64.3.1:9443|Language=en-
US|TimeZone=-7|UpdateMethod=0|Uid=ad592e42a0c1c9476c10277b5e04d6d0|VMPlatform=VMWARE^M ^M
2020/05/03 11:23:59.250 info    fds_svr[15858]: [FMG-->FGT] Response: Protocol=3.0|Firmware=FMG-
VM64-FW-6.04-2002|SerialNumber=FMG-VM0A16003351|Response=200|Persistent=false^M ^M
2020/05/03_11:23:59.250 info    fds_svr[15858]: Process client 100.64.3.1:9443 request SUCCESS
2020/05/03_11:23:59.250 notice  fds_worker[15861]: process remote(::ffff:100.64.3.1) SUCCESS!
...
```

FORTINET

© Fortinet Inc. All Rights Reserved.

26





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

DO NOT REPRINT
© FORTINET

Rating Services—Receive Status

- Shows information about rating packages received from FortiGuard:

FortiManager: FortiGuard > Query Server Management > Receive Status

<input type="checkbox"/> History	Package Received	Latest Version (Release D: Size	Update History
<input type="checkbox"/> FURL	Web Filter Database	22.47645(2020-01-05 19:55 6.31 GB	
<input type="checkbox"/> SPAM001	Email Filter Database 1	102.01459(2020-04-16 18:2 777.07 MB	
<input type="checkbox"/> SPAM002	Email Filter Database 2	92.24581(2019-08-28 16:23 51.97 MB	
<input type="checkbox"/> SPAM004	Email Filter Database 4	78.52327(2019-08-28 05:21 25.46 MB	

<input type="checkbox"/> ▼ Date	Event	Status	Download
<input type="checkbox"/> 2020-04-16 18:27:56	Poll Update	✓ Success	22.47645(4.84 GB)
<input type="checkbox"/> 2020-04-16 17:07:16	Manual Updat	✓ Success	22.39451(1.58 GB)
<input type="checkbox"/> 2020-04-16 15:43:08	Manual Updat	✓ Success	22.31257(0B)

FORTINET

© Fortinet Inc. All Rights Reserved.

27

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

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

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

DO NOT REPRINT
© FORTINET

Rating Services—Statistics

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

```
# diagnose fmupdate fgd-wfas-rate
```

```
Webfilter:
```

```
0 queries, 0 rated in 60 minutes
```

```
114 queries, 80 rated in 60 minutes
```

```
...
```

```
Antispam_ip:
```

```
Antispam_url:
```

```
Antispam_hash:
```

```
Antivirus:
```

```
0 queries, 0 rated in 60 minutes
```

```
...
```

```
FileQuery:
```

```
0 queries, 0 rated in 60 minutes
```

```
...
```

- Rate interval can be configured:

```
# config fmupdate web-spam fgd-setting
```

```
# set stat-log-interval <integer>
```

- These statistics are also periodically logged to the event log

FORTINET

© Fortinet Inc. All Rights Reserved.

28

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

DO NOT REPRINT
© FORTINET

Rating Services—Logging

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

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

- To display the logs:

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



© Fortinet Inc. All Rights Reserved.

29

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

DO NOT REPRINT
© FORTINET

Rating Services—Troubleshooting

- Restarting the rating service:
diagnose fmupdate service-restart fgd
- Resetting the web filtering and antispam databases:
 1. Disable the rating services on the FortiManager interface(s)
 2. Stop the rating services under **FortiGuard > Advanced Settings**
 3. Delete the database(s)
diagnose fmupdate fgd-del-db wf
diagnose fmupdate fgd-del-db as
 4. Start the rating services service under **FortiGuard > Advanced Settings**
 5. Wait for the entire rating databases to be downloaded and fully merged (may take 4-12 hours)
 6. Enable the rating services on the FortiManager interface(s)

You can use the steps shown on this slide to reinitialize the web filtering and antispam databases and services.

DO NOT REPRINT
© FORTINET

Other FortiGuard Troubleshooting Commands

Commands	Description
<code>diagnose fmupdate vm-license</code>	Lists FortiGate VM license information
<code>diagnose fmupdate get-device [fct fds fgd fgc]</code>	Lists the latest package information downloaded by FortiGate/FortiClient through FortiManager
<code>diagnose fmupdate service-restart [fct fds fgd fgc]</code>	Restarts the linkd service for fct, fds, fgd, and fgc
<code>diagnose fmupdate fds-get-downstream-device <serialnum></code>	Gets information of all downstream FortiGate antivirus-IPS devices. Optionally, enter the device serial number
<code>diagnose fmupdate fds-getobject</code>	Lists downloaded antivirus, IPS, and vulnerability scanner packages
<code>diagnose fmupdate fds-update-info</code>	Displays scheduled update information
<code>diagnose fmupdate fgd-dbver</code>	Gets the version of the database
<code>diagnose fmupdate fgd-get-downstream-device</code>	Gets information on all downstream FortiGate web filter and spam devices
<code>diagnose fmupdate fgd-url-rating</code>	Rate URLs within the FortiManager database using the FortiGate serial number. Optionally, enter the category version and URL.



© Fortinet Inc. All Rights Reserved.

31

These are other debug commands available on FortiManager to troubleshoot FortiGuard-related problems.

DO NOT REPRINT
© FORTINET

Review

- ✓ Explore FortiGuard services
- ✓ Verify FortiGuard connectivity status
- ✓ Monitor current update version and status
- ✓ Examine real-time debug commands
- ✓ Learn about FortiManager troubleshooting commands
- ✓ Troubleshoot common FortiGuard issues

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

By mastering the objectives covered in this lesson, you learned about FortiGuard. You also learned how to troubleshoot problems that occur when FortiGate is connecting to public FortiGuard services, and when FortiManager is acting as a local FortiGuard server.

DO NOT REPRINT
© FORTINET

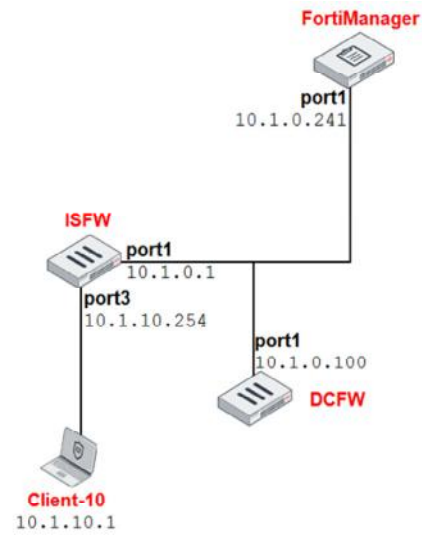
Lab 5—FortiGuard

Now, you will work on *Lab 6—FortiGuard*.

DO NOT REPRINT
© FORTINET

Lab 5—FortiGuard

- Troubleshooting:
 - DCFW not receiving FortiGuard updates
 - Web filtering rating errors occurring on ISFW



FORTINET

© Fortinet Inc. All Rights Reserved.

34

In this lab you will troubleshoot FortiGuard issues on DCFW, and rating lookup issues on ISFW.

DO NOT REPRINT
© FORTINET



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

DO NOT REPRINT
© FORTINET

Objectives

- Describe how HA virtual MAC addresses are assigned
- Monitor an HA cluster
- Check the status of the HA configuration and session synchronization
- Sniffer the HA heartbeat traffic
- Discuss FGCP virtual clustering
- Troubleshoot some common HA problems

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

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

DO NOT REPRINT
© FORTINET

HA Operations

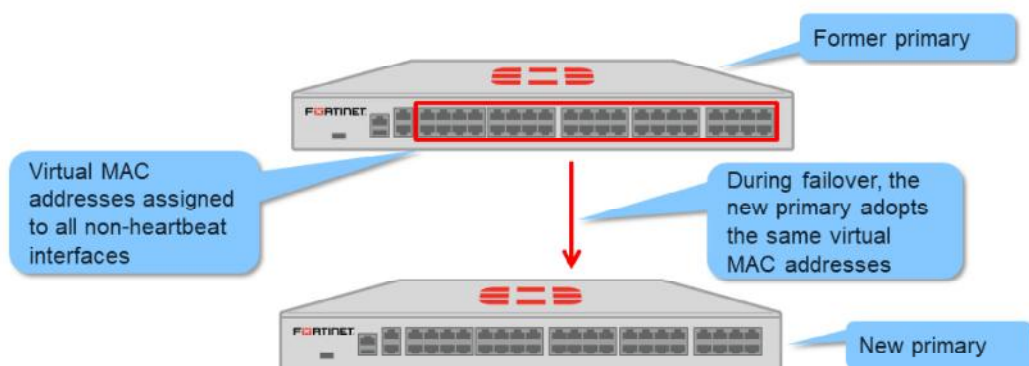


In this section, you will review HA operations.

DO NOT REPRINT
© FORTINET

Virtual MAC Addresses and Failover

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



FORTINET

© Fortinet Inc. All Rights Reserved.

4

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

DO NOT REPRINT
© FORTINET

How the Virtual MAC Addresses Are Assigned

- The virtual MAC address is determined by the following formula:
00 : 09 : 0f : 09 : group_id : (vcluster_id+interface_id)
 - group_id is the HA group ID converted to hexadecimal
 - vcluster_id is 0x00 for virtual cluster 1 and 0x80 for virtual cluster 2
 - interface_id is the interface index
- Therefore, two or more HA clusters in the same LAN segment should use different HA group IDs, to prevent virtual MAC address conflicts

The HA virtual MAC addresses assigned to each interface are determined by the HA group ID, the virtual cluster ID, and the interface index. 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.

DO NOT REPRINT
© FORTINET

Verifying the HA Virtual MAC Address

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

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

Physical MAC address

FORTINET

© Fortinet Inc. All Rights Reserved.

6

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

DO NOT REPRINT
© FORTINET

Virtual MAC Addresses and Failover

- After a failover, gratuitous ARP informs the network that the virtual MAC addresses are now reachable through a different device
- Some switches might not clear their MAC tables fast enough, so they would keep sending packets to the former primary device
- To shut down the interfaces of the former primary FortiGate (except the heartbeats) for 1 second during failover, use the following commands:

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

7

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

In most networks, that's enough for the switches to update their MAC forwarding tables with the new information. However, some high-end switches might not clear their MAC tables properly after a failover. So, they keep sending packets to the former primary even after receiving the gratuitous ARPs. In these cases, you should use the command shown on this slide to force the former primary to shut down all its non-heartbeat interfaces for 1 second when the failover happens. This simulates a link failure that clears the related entries from the switches' MAC tables.

DO NOT REPRINT
© FORTINET

FortiGate Clustering Protocol

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

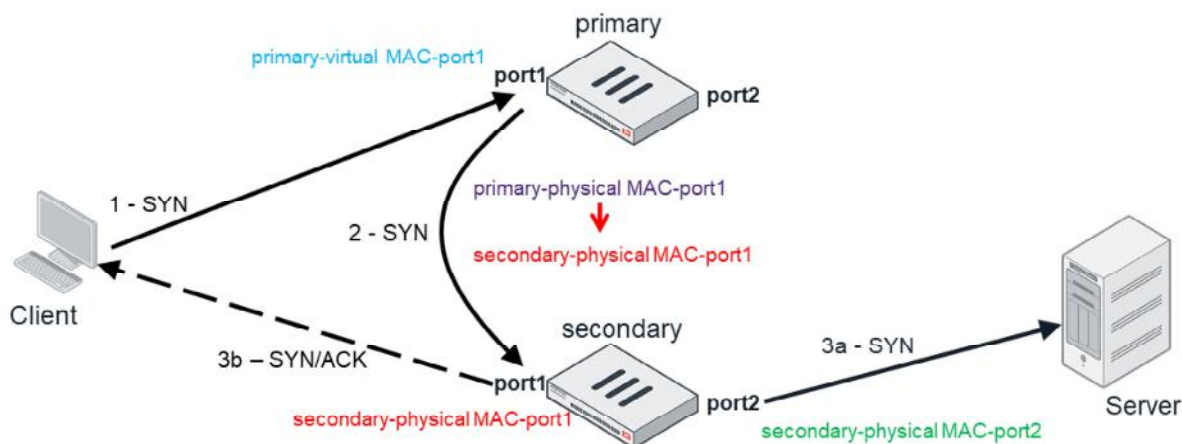
8

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

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

DO NOT REPRINT
© FORTINET

Active-Active Load Balancing



1. srcMAC X, dstMAC **primary-virtual MAC-port1**, TCP SYN dport 80
2. srcMAC **primary-physical MAC-port1**, dstMAC **secondary-physical MAC-port1**, TCP SYN dport 80
- 3a. srcMAC **secondary-physical MAC-port2**, dstMAC Y, TCP SYN dport 80
- 3b. srcMAC **secondary-physical MAC-port1**, dstMAC X, TCP SYN ACK sport 80

FORTINET

© Fortinet Inc. All Rights Reserved.

9

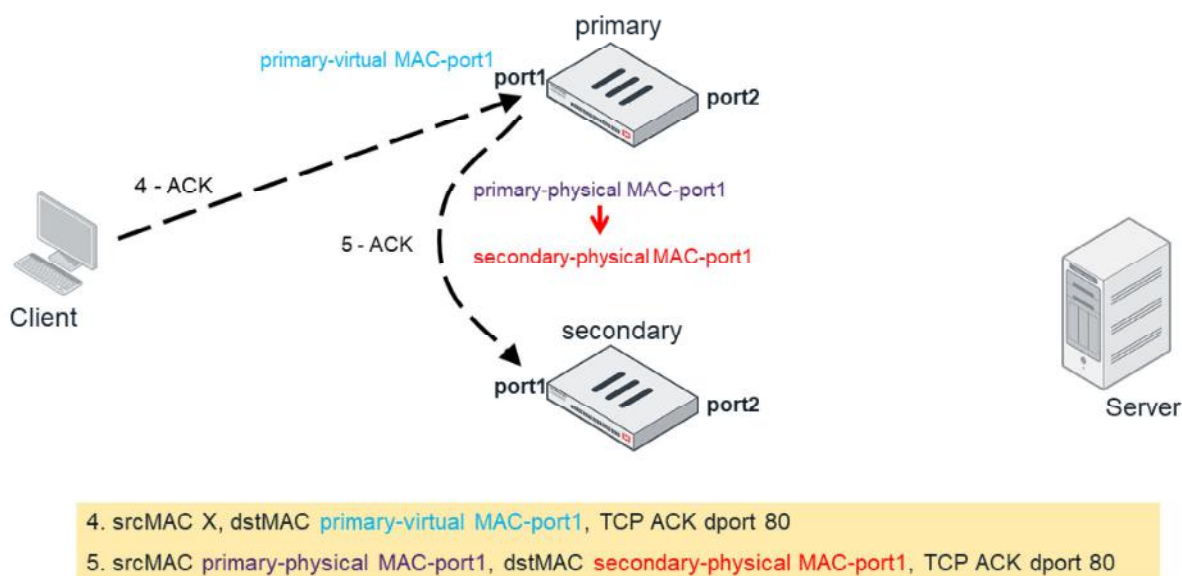
Let's look at how an HA cluster in active-active mode handles traffic.

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

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

DO NOT REPRINT
© FORTINET

Active-Active Load Balancing (Contd)



FORTINET

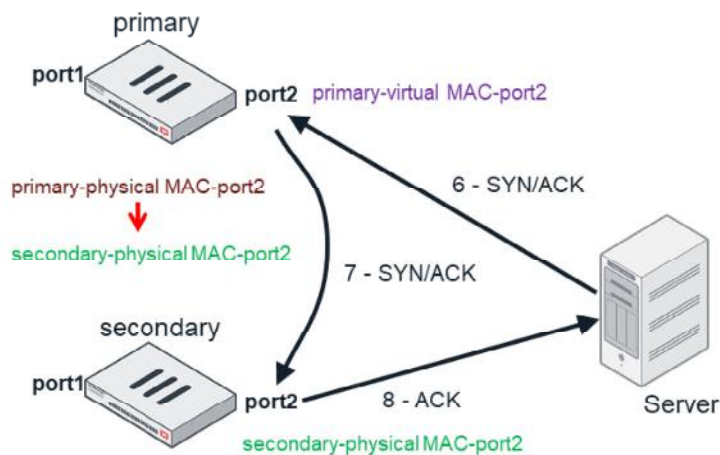
© Fortinet Inc. All Rights Reserved.

10

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

DO NOT REPRINT
© FORTINET

Active-Active Load Balancing (Contd)



6. srcMAC Y, dstMAC **primary-virtual MAC-port2**, TCP SYN ACK sport 80
7. srcMAC **primary-physical MAC-port2**, dstMAC **secondary-physical MAC-port2**, TCP SYN ACK sport 80
8. srcMAC **secondary-physical MAC-port2**, dstMAC Y, TCP ACK dport 80

FORTINET

© Fortinet Inc. All Rights Reserved.

11

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

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

Secondary Console Messages

- A secondary's console shows these messages when joining the cluster

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

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

DO NOT REPRINT
© FORTINET

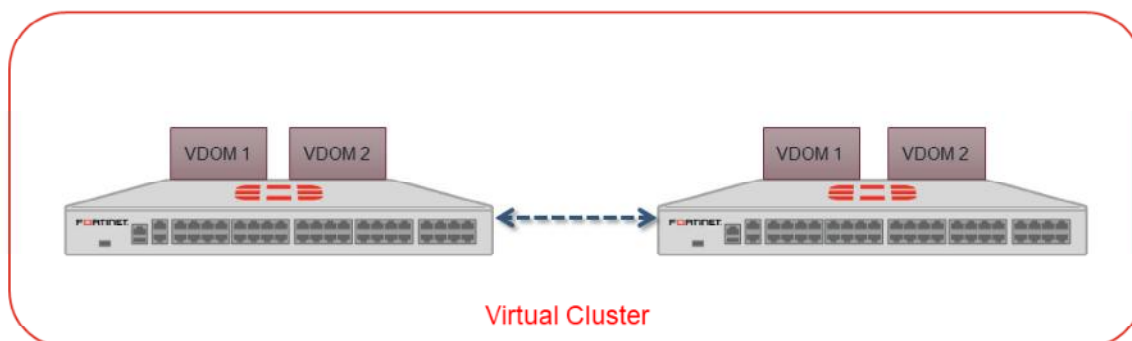
FGCP Virtual Clustering

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

DO NOT REPRINT
© FORTINET

What is Virtual Clustering

- Extension of FGCP for a cluster of two FortiGate units with multiple VDOMs enabled
- Virtual clustering operates in active-passive as well as active-active mode
- FortiGate virtual clustering is limited to a cluster of two FortiGate units with multiple VDOMs enabled



FORTINET

© Fortinet Inc. All Rights Reserved.

14

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

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

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

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

DO NOT REPRINT
© FORTINET

Active-Active Virtual Clustering

- Virtual cluster can be set up in active-active mode to load balance sessions between cluster units
- For virtual clustering, setting HA mode to active-active is similar to an active-active HA cluster without virtual domains
 - Primary device will receive all sessions and load balance them among other cluster devices
 - All devices in a cluster process traffic for all virtual domains

FORTINET

© Fortinet Inc. All Rights Reserved.

15

There are two ways to configure load balancing for virtual clustering. The first method is to set the HA mode to active-active, and the second method is to configure VDOM partitioning.

For virtual clustering, setting the HA mode to active-active, the primary device receives all sessions and load balances them among the cluster devices according to the load balancing schedule. All cluster devices process traffic for all VDOMs.

DO NOT REPRINT
© FORTINET

VDOM Partitioning

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



© Fortinet Inc. All Rights Reserved.

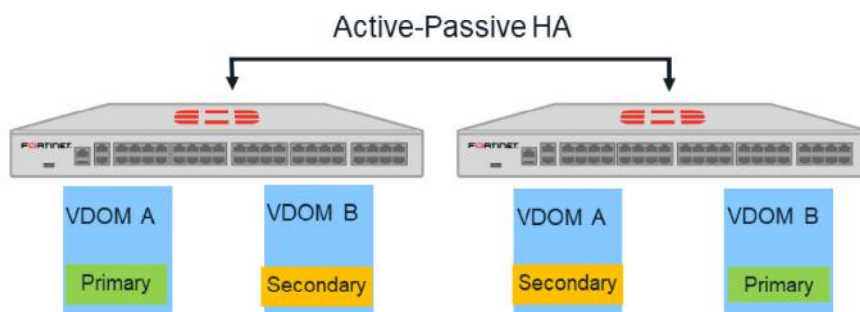
16

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

DO NOT REPRINT
© FORTINET

VDOM Partitioning (Contd)

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



FORTINET

© Fortinet Inc. All Rights Reserved.

17

In this example, HA is configured in active-passive mode. Traffic for VDOM A will be processed by FortiGate 1 and for VDOM B, FortiGate 2 will process all traffic. In case of a failover, one device in the cluster will process all traffic for all VDOMs.

DO NOT REPRINT
© FORTINET

HA Troubleshooting

In this section, you will learn about some HA troubleshooting commands.

DO NOT REPRINT
© FORTINET

Checking the Status of the HA Through the GUI

System > HA

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
<div> <div>FortiGate VM64</div> <div> <div>1 3 5 7 9 11 13 15 17 19 21 23</div> <div>2 4 6 8 10 12 14 16 18 20 22 24</div> </div> </div>	200	NGFW-1	FGVM010000077648	Master	00:00:06:00	116	30.00 kbps
<div> <div>FortiGate VM64</div> <div> <div>1 3 5 7 9 11 13 15 17 19 21 23</div> <div>2 4 6 8 10 12 14 16 18 20 22 24</div> </div> </div>	100	NGFW-2	FGVM010000077652	Slave	00:00:05:23	11	15.00 kbps

Cluster members
are synchronized

FORTINET

© Fortinet Inc. All Rights Reserved.

19

If the HA cluster forms successfully, the GUI displays all the FortiGate members with their hostnames, serial numbers, role, uptime, and synchronization status.

DO NOT REPRINT
© FORTINET

Connecting to a Secondary's CLI

- Using the primary CLI, you can connect to any secondary CLI:

```
# execute ha manage <HA_unit_index> <Admin_Username>
```
- To list the index numbers for each device, use a question mark:

```
# execute ha manage ?  
<id>    please input peer box index.  
<0>    Subsidiary unit FGVM01000001xxxx
```

FORTINET

© Fortinet Inc. All Rights Reserved.

20

When troubleshooting a problem in an HA cluster, it is useful to know that you can connect to the CLI of any secondary device from the CLI of the primary device. Using the command shown on this slide with the HA index of the secondary device, you can connect to the CLI of the secondary device. To get the list of secondary FortiGate devices and their HA indexes, use the question mark at the end of that same command.

DO NOT REPRINT
© FORTINET

HA Status

```
# diagnose sys ha status
HA information
Statistics
```

```
traffic.local = s:0 p:980056 b:152606366
traffic.total = s:0 p:980087 b:152619104
activity.ha_id_changes = 2
activity.fdb = c:0 q:0
```

Heartbeat

```
Model=80005, Mode=2 Group=2 Debug=0
nvcluster=1, ses_pickup=0, delay=0
```

Serial numbers

Assigned priorities

```
[Debug_Zone HA information]
```

```
HA group member information: is manage master=1.
```

```
FGVM010000077649: Master, serialno_prio=1, usr_priority=128, hostname=NGFW-1
FGVM010000077650: Slave, serialno_prio=0, usr_priority=120, hostname=NGFW-2
```

```
[Kernel HA information]
```

```
vcluster 1, state=work, master_ip=169.254.0.2, master_id=0:
```

```
FGVM010000077649: Master, ha_prio/o_ha_prio=0/0
```

```
FGVM010000077650: Slave, ha_prio/o_ha_prio=1/1
```

FORTINET

© Fortinet Inc. All Rights Reserved.

21

Using the CLI, you can get more information about the status of the HA. For example, the command shown on this slide displays heartbeat traffic statistics, as well as the serial number and HA priority of each FortiGate. This command also shows the heartbeat interface IP address automatically assigned to the primary FortiGate.

DO NOT REPRINT
© FORTINET

HA Status

```
# get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:15:10
Cluster state change time: 2020-04-29 12:34:01
Master selected using:
  <2020/04/29 12:34:01> FGVM010000077649 is selected as the master because it has the
  largest value of override priority.
ses_pickup: disable
override: enable
Configuration Status:
  FGVM010000077649(updated 4 seconds ago): in-sync
  FGVM010000077650(updated 3 seconds ago): in-sync
System Usage stats:
  FGVM010000077649(updated 4 seconds ago):
    sessions=16, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=81%
  FGVM010000077650(updated 3 seconds ago):
    sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=78%
...
```

How the master device
was selected

System usage stats
from all cluster
members

FORTINET

© Fortinet Inc. All Rights Reserved.

22

You can use the command shown on this slide to display following information:

- HA health status
- Cluster uptime
- Criteria used to select the master unit
- Override status
- Status of the monitored interfaces
- Status of the HA ping servers

DO NOT REPRINT
© FORTINET

Checking the HA Time Difference

```
# diagnose sys ha dump-by vcluster
<hatalk> HA information.
```

```
vcluster_nr=1
```

```
vcluster_0: start_time=1588188799(2020-04-29 12:33:19),
state/o/chg_time=2(work)/2(work)/1588188801(2020-04-29 12:33:01)
```

```
mondev: port1(prio=50,is_aggr=0,status=1)
port2(prio=50,is_aggr=0,status=1)
```

```
'FGVM010000077649': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0,
flag=0x00000001, uptime/reset_cnt=0/1
```

```
'FGVM010000077650': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0,
flag=0x00000000, uptime/reset_cnt=196/0
```

How many times the device uptime has been reset with the `diagnose sys ha reset-uptime` command

Device uptime

FORTINET

© Fortinet Inc. All Rights Reserved.

23

The HA uptime is one of variables used to elect the primary device. Depending on other variables and configuration, the device might compare their system uptimes to elect the primary. If that happens, and if there is one member whose system uptime is five minutes more than the system uptimes of all the other devices, that member is elected primary. You can use this command to compare the system uptimes of all the devices in a cluster.

The `reset_cnt` value shows you how many times the HA uptime has been reset with the `diagnose sys ha reset-uptime` command.

DO NOT REPRINT
© FORTINET

Checking the Configuration Synchronization

```
# diagnose sys ha checksum show
is_manage_master()=1, is_root_master()=1
debugzone
global: ee 89 a1 71 0b c5 2a ed 99 f3 a8 4a 27 6f 1b 5c
root: 86 54 58 00 9a 6c ef 30 19 62 a3 c9 84 a8 c6 8a
all: 94 52 d7 bf e5 29 d0 9a 58 d2 47 f4 f5 d0 a7 94

checksum
global: ee 89 a1 71 0b c5 2a ed 99 f3 a8 4a 27 6f 1b 5c
root: 86 54 58 00 9a 6c ef 30 19 62 a3 c9 84 a8 c6 8a
all: 94 52 d7 bf e5 29 d0 9a 58 d2 47 f4 f5 d0 a7 94
```

Run this command
on all HA members

Checksum
numbers must
match between
debugzone and
checksum zone

All members must
have the same
sequences of
checksum numbers

FORTINET

© Fortinet Inc. All Rights Reserved.

24

A good indication of the health of an HA cluster is the status of the configuration synchronization. To verify that all the secondary configurations are synchronized with the primary configuration, you can use the command shown on this slide on all the HA devices. If a secondary FortiGate displays exactly the same sequence of numbers as the primary, its configuration is synchronized. Also, and as long as there are no configuration changes happening, on each of the devices, the `debugzone` and the `checksum` zone must display the same sequence of numbers. Later in this lesson, you will learn some tips for troubleshooting when this is not the case.

The `checksum` zone contains the checksum of the configuration that is actually running on the device. The `debugzone` is where configuration changes are first stored before applying them to the running configuration. So, during a configuration change you might see that the `debugzone` checksum differs from the `checksum` for a short time, while the configuration changes are copied to the running configuration. After that short time, both checksums should match again.

DO NOT REPRINT
© FORTINET

Checking the Configuration Synchronization

```
# diagnose sys ha checksum cluster
===== FGVM010000077649 =====
is manage master()=1, is root master()=1
debugzone
global: ee 89 a1 71 0b c5 2a ed 99 f3 a8 4a 27 6f 1b 5c
root: 86 54 58 00 9a 6c ef 30 19 62 a3 c9 84 a8 c6 8a
all: 94 52 d7 bf e5 29 d0 9a 58 d2 47 f4 f5 d0 a7 94
checksum
global: ee 89 a1 71 0b c5 2a ed 99 f3 a8 4a 27 6f 1b 5c
root: 86 54 58 00 9a 6c ef 30 19 62 a3 c9 84 a8 c6 8a
all: 94 52 d7 bf e5 29 d0 9a 58 d2 47 f4 f5 d0 a7 94
===== FGVM010000077650 =====
is manage master()=0, is root master()=0
debugzone
global: ee 89 a1 71 0b c5 2a ed 99 f3 a8 4a 27 6f 1b 5c
root: 86 54 58 00 9a 6c ef 30 19 62 a3 c9 84 a8 c6 8a
all: 94 52 d7 bf e5 29 d0 9a 58 d2 47 f4 f5 d0 a7 94
checksum
global: ee 89 a1 71 0b c5 2a ed 99 f3 a8 4a 27 6f 1b 5c
root: 86 54 58 00 9a 6c ef 30 19 62 a3 c9 84 a8 c6 8a
all: 94 52 d7 bf e5 29 d0 9a 58 d2 47 f4 f5 d0 a7 94
```

Alternatively, you can use this command on the primary device

Primary

Secondary

FORTINET

© Fortinet Inc. All Rights Reserved.

25

Instead of using the `checksum show` command on each of the cluster devices, you can use the command shown on this slide only on the primary. It shows the checksum for all the cluster members. This command is easier to use; however, if there are communication problems between one of the secondary devices and the primary, you might need to use the `checksum show` command instead.

DO NOT REPRINT
© FORTINET

Checking HA Session Synchronization

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 socktype=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/..._cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
tx speed(Bps/kbps): 7/0 rx speed(Bps/kbps): 16/0
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000098 tos=ff/ff ips_view=0 app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Check the primary's session table

HA ID of the device processing this traffic

Session has been synchronized to all secondary devices

FORTINET

© Fortinet Inc. All Rights Reserved.

26

By default, HA session synchronization is disabled. If you enable it, you can check the primary's session table to see which sessions have been synchronized to the secondary devices. They are the ones with the `synced` flag. Additionally, and in the case of all sessions, the `ha_id` field shows the HA member ID of the device that is processing the traffic.

DO NOT REPRINT
© FORTINET

Types of Failover

- Loss of keep-alive packets
 - Primary fails to reply
- A monitored interface becomes disconnected
 - The new primary will be the device with the fewest failed monitored interfaces
 - Port monitoring takes precedence over device priority
- Remote link failover
 - Uses detect (ping) servers to test IP connectivity
 - Pings originated only from the primary
 - If it does not get a reply, the cluster renegotiates the primary
- Solid state disk (SSD) failover
 - An SSD fails
 - Only for devices with SSDs

FORTINET

© Fortinet Inc. All Rights Reserved.

27

There are four occurrences that can trigger a failover:

- When the primary stops replying to heartbeats.
- When the link status of a monitored interface goes down. You can configure an HA cluster to monitor the link status of one or more interfaces.
- When a server (IP address) stops replying to the ping sent by the primary. You can configure an HA cluster to periodically send a ping to one or more servers to test the connectivity between the primary device and the network services.
- When FortiOS detects a failure in an SSD. Only available for devices with SSDs.

DO NOT REPRINT
© FORTINET

HA Logs Sample

- Primary device fails and is removed from the cluster
- These messages are recorded by a secondary device, which becomes the new primary device:

```
20xx-06-06 14:49:44 Heartbeat device(interface) down
20xx-06-06 14:50:00 Virtual cluster detected member dead
20xx-06-06 14:50:02 Virtual cluster's member state moved
```

FORTINET

© Fortinet Inc. All Rights Reserved.

28

If a failover happens, the best tool to use to get information about the failover is the FortiGate logs. If the failover happened because the primary device failed, the secondary device's logs should show these log entries.

DO NOT REPRINT
© FORTINET

HA Logs Sample

- Link failure of a monitored interface
- These log messages, recorded by the primary device, show the monitored port1 interface:

```
20xx-06-06 16:59:39 Link monitor: Interface port1 was turned down
20xx-06-06 16:59:39 HA device(interface) fail
20xx-06-06 16:59:41 Virtual cluster's member state moved
```

FORTINET

© Fortinet Inc. All Rights Reserved.

29

If a new primary was elected because one or more monitored interfaces failed, the former primary displays logs similar to the ones shown on this slide. In the example shown here, the primary unit is reporting a problem with the monitored interface port1.

DO NOT REPRINT
© FORTINET

HA History

- Provides information about past HA events

```
# diagnose sys ha history read
version=1.1
HA state change time: 2020-04-29 12:34:01
message_count=4/512
<2020-04-29 12:34:01> FGVM010000077648 is elected as the cluster master of 2 members
<2020-04-29 12:34:01> new member 'FGVM010000077652' joins the cluster
<2020-04-29 12:33:22> FGVM010000077648 is elected as the cluster master of 1 members
<2020-04-29 12:33:19> hatalk started
```

FORTINET

© Fortinet Inc. All Rights Reserved.

30

Another useful way to determine the reason of a HA failover is by running the command shown on this slide. This command provides details about past HA events, allowing admins to identify the reason for previous failover events. This is a useful HA command, especially when HA logs are not available.

DO NOT REPRINT
© FORTINET

HA Troubleshooting Tips

- If a device can't join the cluster, follow these steps:

1. Verify that the HA settings match
2. Verify that the firmware and hardware match
3. Verify physical layer connections
4. Use the HA real-time debug:


```
diagnose debug application hataalk -l
diagnose debug application hasync -l
diagnose debug enable
```

- If the checksums between the `debugzone` and `checksum` zones do not match, you can force the recalculation:

```
# diagnose sys ha checksum recalculate [<vdom_name> | global]
```

FORTINET

© Fortinet Inc. All Rights Reserved.

31

If a device can't join a cluster, follow these steps:

1. Verify the HA settings.
2. Verify the firmware versions and hardware models.
3. Verify the physical layer connections.
4. Use the HA real-time debug while the unit tries to join the cluster. Run the debug on both the primary device and the device with the problem.

If the problem is that the checksums between the `debugzone` and `checksum` zones don't match, you can try to fix it by forcing the recalculation.

DO NOT REPRINT
© FORTINET

HA Heartbeat Troubleshooting Tips

- High session synchronization traffic might delay heartbeats
 - Solutions:
 - Separate session synchronization and heartbeat traffic:


```
config system ha
  set session-sync-dev <port_name_1> [port_name_2] ...
end
```
 - Delay new session synchronization by 30 seconds. Short-lived sessions won't be synced, which results in less session traffic:


```
config system ha
  set session-pickup-delay enable
end
```
- High CPU problems can also create HA heartbeat issues

FORTINET

© Fortinet Inc. All Rights Reserved.

32

Traffic from session synchronization is bandwidth intensive. If the session creation rate is high, session synchronization traffic can interfere with heartbeat traffic, creating delays in heartbeat replies. There are two configuration changes that you can make that might help:

- Use a different interface from the heartbeat interface for session synchronization.
- Delay the synchronization of new sessions by 30 seconds, so short-lived sessions are not synchronized.

High CPU issues could also create HA heartbeat problems. In those cases, troubleshoot and fix the high CPU problem first, before checking the HA status.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand HA virtual MAC addresses
- ✓ Understand traffic flow in HA active-active
- ✓ Monitor an HA cluster
- ✓ Check configuration and session synchronization
- ✓ Examine FGCP and HA log samples
- ✓ Review HA troubleshooting tips

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

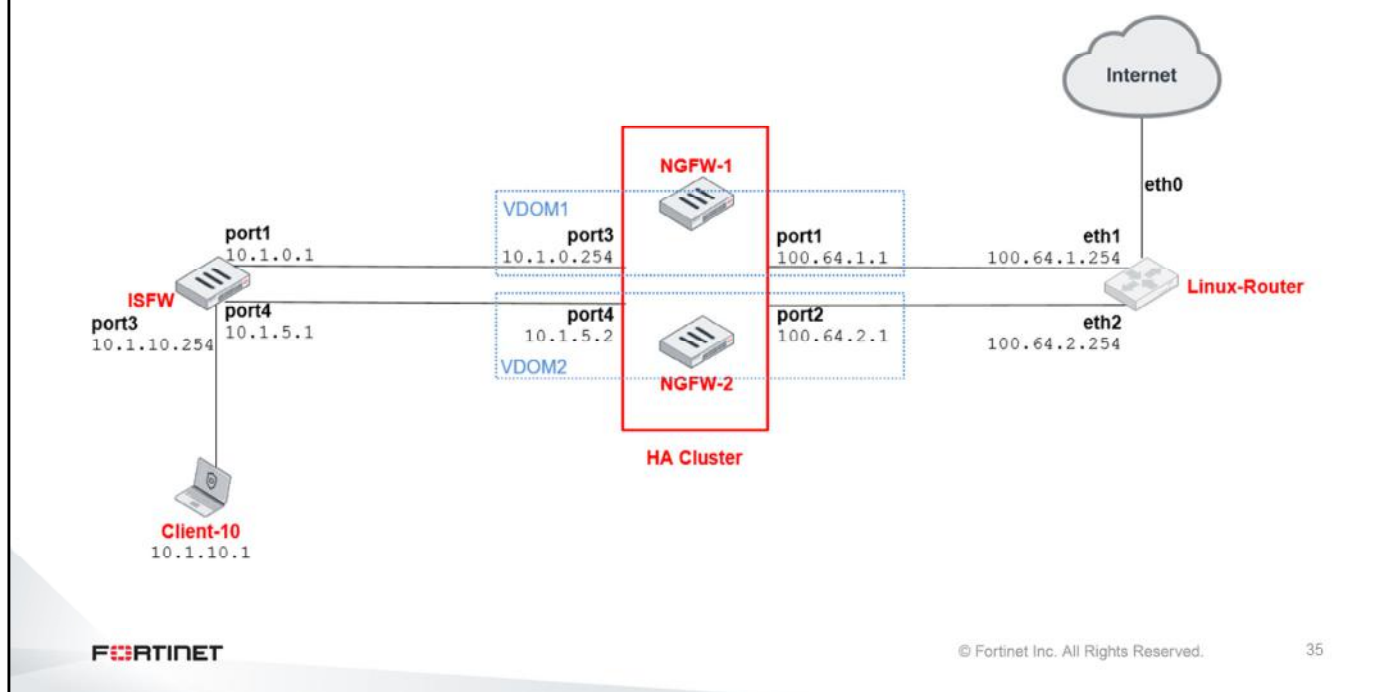
DO NOT REPRINT
© FORTINET

Lab 6—High Availability

Now, you will work on *Lab 3—System Troubleshooting*.

DO NOT REPRINT
© FORTINET

Lab 6–High Availability



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

DO NOT REPRINT
© FORTINET



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

DO NOT REPRINT
© FORTINET

Objectives

- Review FortiManager key features
- Use FortiManager to centralize the management of the enterprise network
- Configure IPsec using the FortiManager VPN manager
- Use scripts to apply individualized configuration changes to FortiGate devices

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

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

DO NOT REPRINT
© FORTINET

FortiManager Overview

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

DO NOT REPRINT
© FORTINET

What Is FortiManager?

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

FORTINET

© Fortinet Inc. All Rights Reserved.

4

When should you use FortiManager in your network?

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

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

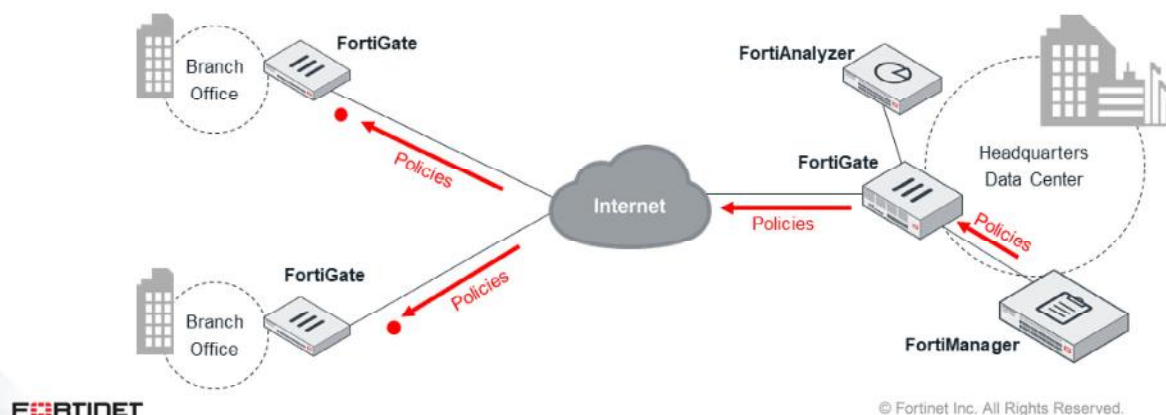
What can FortiManager do?

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

DO NOT REPRINT
© FORTINET

Key Features

- Centralized management
- Administrative domains (ADOMs)
- Configuration revision control and tracking
- Local FortiGuard service
- Firmware management
- Scripting
- Managers – VPN, FortiAP, FortiSwitch, and Fabric View (Security Fabric)
- Logging and reporting
- Pay-as-you go licensing through the Fortinet VM on-demand program



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

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

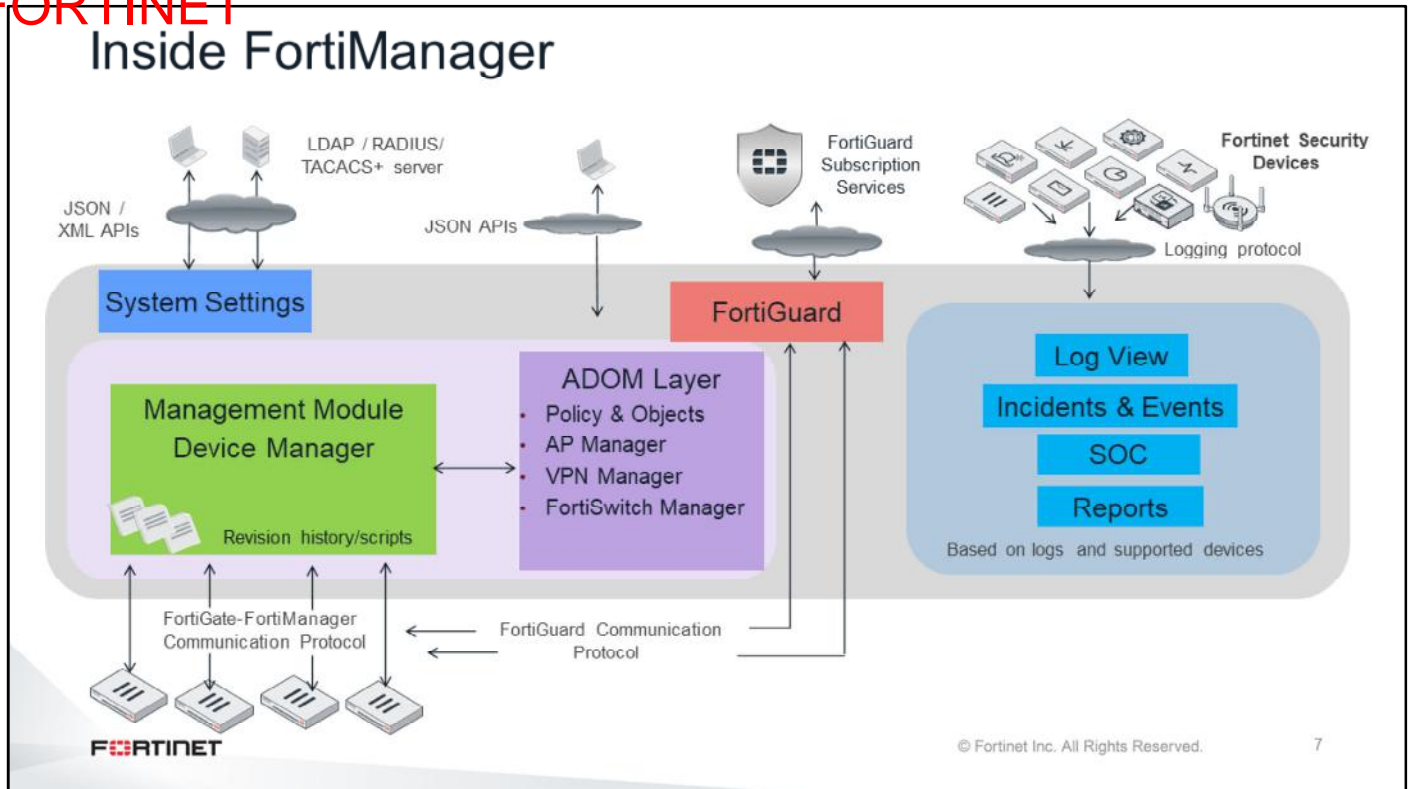
DO NOT REPRINT
© FORTINET

Software Architecture



In this section, you will examine FortiManager software architecture.

DO NOT REPRINT
© FORTINET



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

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

DO NOT REPRINT
© FORTINET

Management Layers

- Global ADOM layer
 - Global objects
 - All header and footer policies
- ADOM layer
 - Common object database, devices, device groups, policy packages
- Device Manager layer
 - Name and type of managed devices, their IP addresses, revision history and real-time status

FORTINET

© Fortinet Inc. All Rights Reserved.

8

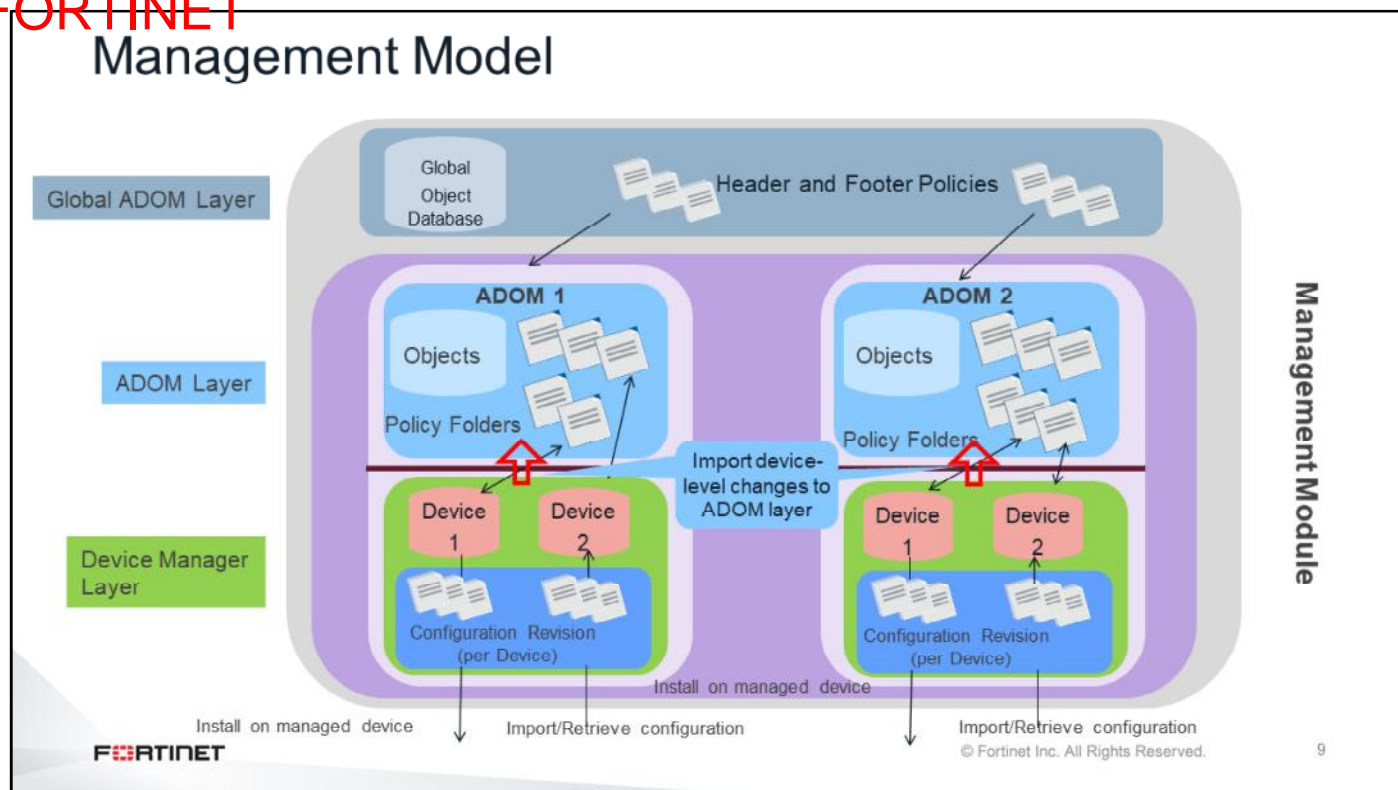
To organize and efficiently manage a large-scale network, FortiManager has multiple management layers.

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

The ADOM layer is where policy packages are created, managed, and installed on managed devices or device groups. Multiple policy packages can be created here. The ADOM layer includes one common object database for each ADOM. The common object database contains information such as addresses, services, and security profiles.

The Device Manager layer records information on devices that are centrally managed by the FortiManager device, such as the name of the device, type of device, model, IP address, current firmware installed, revision history, and real-time status.

DO NOT REPRINT
© FORTINET



Understanding the layers of FortiManager's management model is important.

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

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

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

DO NOT REPRINT
© FORTINET

Administrative Domains

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



© Fortinet Inc. All Rights Reserved.

10

What is an ADOM?

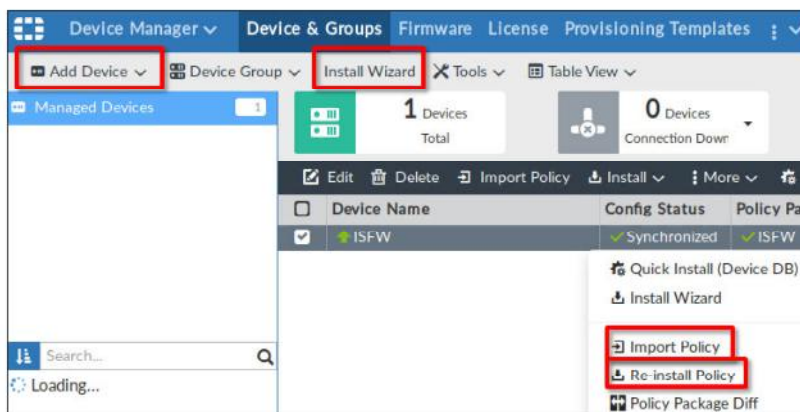
ADOMs enable the admin account to create groupings of devices for administrators to monitor and manage. For example, administrators can manage devices specific to their geographic location or business division. ADOMs are not enabled by default and must be enabled by the administrator.

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

DO NOT REPRINT
© FORTINET

Wizards

- Assist with various tasks
- Main wizards:
 - Add Device
 - Install Wizard
 - Import Policy
 - Re-install Policy



FORTINET

© Fortinet Inc. All Rights Reserved.

11

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

- **Add Device** is used to add devices to central management and import their configurations.
- **Install Wizard** is used to install configuration changes from the **Device Manager** pane or **Policies & Objects** pane to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.
- **Import Policy** is used to import interface mappings, policy databases, and objects associated with the managed devices into a policy package under the **Policy & Object** pane. It runs with the **Add Device** wizard, by default, and may be run at any time from the managed device list.
- **Re-install Policy** is used to perform a quick install of the policy package. It provides the ability to preview the changes that will be installed on the managed device.

You can open the **Import policy** and **Re-install Policy** wizards by right-clicking your managed device in the **Device Manager**.

DO NOT REPRINT
© FORTINET

Central VPN Management

In this section, you will learn how to configure IPsec VPNs using the FortiManager VPN manager.

DO NOT REPRINT
© FORTINET

FortiManager VPN Manager

- VPN manager simplifies the administration of multiple VPNs
- You can install common IPsec VPN settings on multiple FortiGate devices at the same time
 - Settings are stored as objects and pushed to the devices as part of the policy packages
- VPN manager is enabled for each ADOM
- Steps:
 1. Create a VPN community
 2. Add gateways (members) to the community
 3. Install the VPN community and gateways configuration
 4. Add the firewall policies
 5. Install the firewall policies

FORTINET

© Fortinet Inc. All Rights Reserved.

13

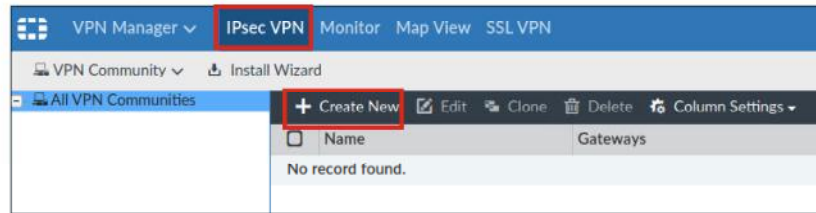
On the VPN manager screen, you can configure IPsec VPN settings that you can install on multiple devices. The settings are stored as objects in the objects database. You push the IPsec VPN settings to one or more devices by installing a policy package. Follow these steps to configure VPNs with the VPN manager:

1. Create a VPN community.
2. Add gateways (members) to the community.
3. Install the VPN community and gateways configuration.
4. Add the firewall policies.
5. Install the firewall policies.

DO NOT REPRINT
© FORTINET

VPN Communities

- Contain the common IPsec settings that are shared by all the IPsec gateway members of the community



- Three types of communities:
 - Full meshed
 - Star
 - Dial-up

FORTINET

© Fortinet Inc. All Rights Reserved.

14

Depending on the VPN topology you are installing, there are three types of communities:

- Full meshed
- Star
- Dial-up

DO NOT REPRINT
© FORTINET

VPN Communities Configuration

- Enter the common phase 1 and phase 2 settings:
 - These settings will be applied to all the members in the community

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication: ☒ Pre-shared Key ☐ Certificates

☐ Generate (random)

☒ Specify:

Encryption:

IKE Security (Phase 1) Properties

IKE Version: ☒ 1 ☒ 2

Encryption: 1 Authentication:

Network Overlay: ☐ OFF

IPsec Security (Phase 2) Properties

Encryption: Authentication:

VPN Topology Setup Wizard

VPN Zone ☒ ON

☒ Create Default Zones ☐ Use Custom Zone

IKE Security Phase 1 Advanced Properties

Diffie-Hellman Group(s): ☐ 1 ☐ 2 ☒ 5 ☒ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Key Life: 28800 (120-172800 seconds)

Dead Peer Detection: ☐ Disable ☐ On Idle ☒ On Demand

IPsec Security Phase 2 Advanced Properties

Diffie-Hellman Group(s): ☐ 1 ☐ 2 ☒ 5 ☒ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Replay Detection: ☒ ON ☐ OFF

Perfect Forward Secrecy(PFS): ☒ ON ☐ OFF

FORTINET

© Fortinet Inc. All Rights Reserved.

15

The VPN community contains the IPsec phase 1 and 2 settings that are common to all the gateways.

DO NOT REPRINT
© FORTINET

VPN Gateways

- After the community is created, it is time to add the VPN gateways
- Two types of gateways:
 - Managed gateways are FortiGate devices managed by FortiManager in the current ADOM
 - External gateways are devices not managed by FortiManager, or devices in a different ADOM
 - VPN configuration must be handled manually by the administrator in that ADOM

FORTINET

© Fortinet Inc. All Rights Reserved.

16

The next step is to add gateways to the community. There are two types of gateways:

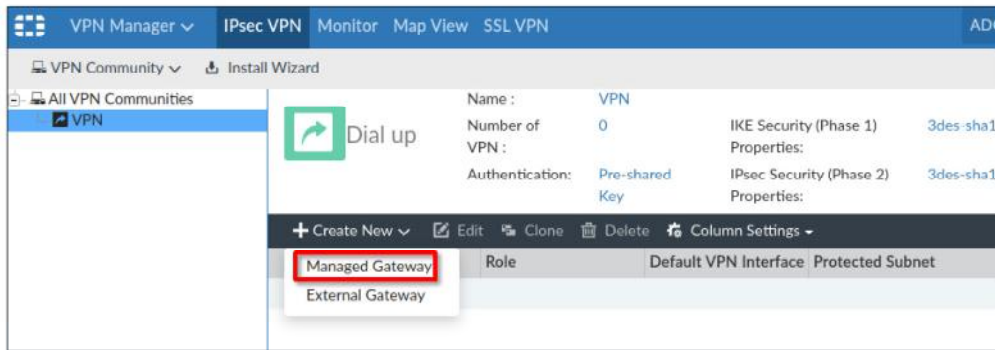
- Managed gateways
- External gateways

Managed gateways are managed by FortiManager in the current ADOM. Devices in a different ADOM or other vendor devices can be treated as external gateways. VPN configuration must be handled manually by the administrator in that ADOM.

DO NOT REPRINT
© FORTINET

VPN Gateway Configuration

- For each managed gateway, you configure:
 - Protected subnets
 - Gateway role (hub, spoke, and so on)
 - Interface where the tunnel terminates
 - Advanced settings: peer ID, IKE mode configuration



FORTINET

© Fortinet Inc. All Rights Reserved.

17

In VPN gateways, you configure the node type (hub, spoke, and so on), depending on the VPN topology you select. For example, hub and spoke options are available only in star and dial-up topologies.

For each gateway, you can also configure the protected subnet, interfaces, and some advanced settings.

DO NOT REPRINT
© FORTINET

Scripts



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

Scripts

- Can make many changes to multiple managed devices
 - Can be used to provisioning FortiGate devices
 - Can be used to automate configuration changes
- Help consistency and simplify bulk configuration changes
- There are two types of scripts:
 - Command Line Interface (CLI)
 - A sequence of FortiGate CLI commands, as you would type on the FortiGate CLI
 - Tool Command Language (TCL)
 - A dynamic scripting language which provides more functionality to your scripts, including global variables and decision structures
- Three ways to run CLI scripts:
 - Device database
 - Policy package, ADOM database
 - Remote FortiGate directly (through the CLI)



© Fortinet Inc. All Rights Reserved.

19

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

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

CLI scripts are enabled by default.

CLI scripts can be run in three different ways:

- **Device database:** By default, a script is run on the device database. It is recommend that you run the changes on the device database (default setting), because this allows you to check what configuration changes you will send to the managed device. After scripts run on the device database, you can install these changes to a managed device using the installation wizard.
- **Policy package, ADOM database:** If a script contains changes related to ADOM-level objects and policies, you can change the default selection to run on policy package, ADOM database and then install it using the installation wizard.
- **Remote FortiGate directly (through CLI):** A script can be run directly on the device and you don't need to install these changes using the installation wizard. Because the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

DO NOT REPRINT
© FORTINET

TCL Scripts

- TCL scripts can be enabled from the FortiManager CLI

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

- TCL scripts are not run via the FGFM tunnel like the CLI scripts
- TCL scripts use SSH and requires SSH authentication to work
- Can run only on:
 - Remote FortiGate directly (through the CLI)

FORTINET

© Fortinet Inc. All Rights Reserved.

20

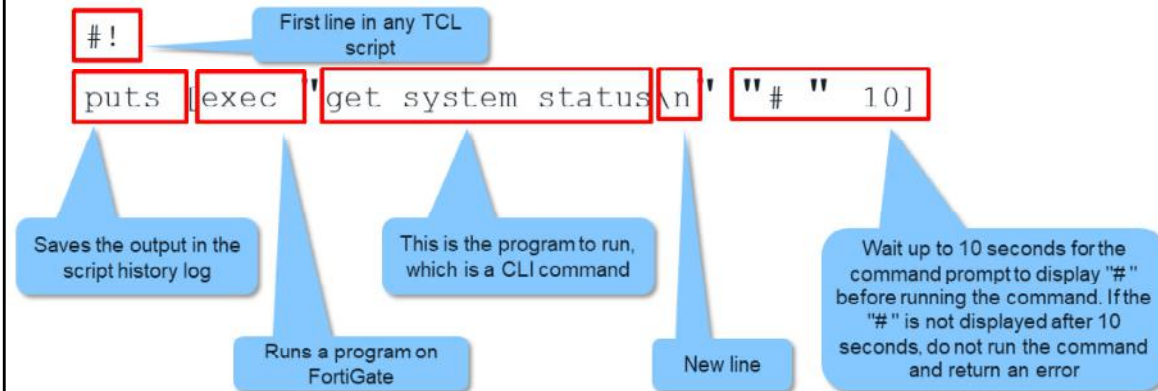
For TCL scripts, you need to enable `show` command for TCL scripts on the FortiManager CLI.

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

TCL scripts can only be run on Remote FortiGate directly (through the CLI).

DO NOT REPRINT
© FORTINET

How to Run CLI Commands Using TCL



FORTINET

© Fortinet Inc. All Rights Reserved.

21

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

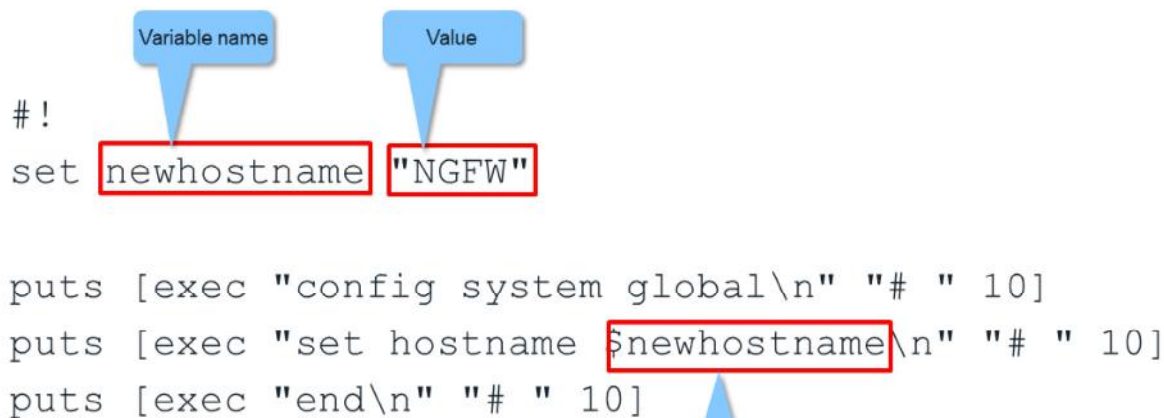
The next line, `exec` TCL, runs the CLI command `get system status`.

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

The output of the CLI command is saved to the FortiManager script history log using the TCL command `puts`.

DO NOT REPRINT
© FORTINET

TCL Variables



```
#!
set newhostname "NGFW"

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

The diagram illustrates the use of TCL variables. A callout labeled 'Variable name' points to the text 'newhostname' in the 'set' command. Another callout labeled 'Value' points to the text '"NGFW"' in the same command. Below, the variable is used in two 'puts' commands, where its value is expanded. A third callout points to the '\$' sign in '\$newhostname', explaining its purpose.

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

FORTINET

© Fortinet Inc. All Rights Reserved.

22

This slide shows an example of using TCL variables.

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

The value of the variable is then used (prepending the `$` sign) to configure the FortiGate hostname.

DO NOT REPRINT
© FORTINET

Creating and Calling TCL Procedures

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

23

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

In the example shown on this slide, we are creating a TCL procedure called `do_cmd`. This procedure instructs the interpreter to run a CLI command (received through the parameter `cmd`) if the `#` is received within 10 seconds.

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

DO NOT REPRINT
© FORTINET

TCL Example Using Loops

- Creates 150 firewall addresses:

numhosts contains the number of addresses to create

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

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

Increment the value of *i* after each loop

Script Results:

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

FORTINET

© Fortinet Inc. All Rights Reserved.

24

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

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

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

DO NOT REPRINT
© FORTINET

Best Practices for Scripts

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


```
config router static ✓
conf rout stat ✗
```
- Commands that start with a number sign (#) are not run


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


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

Default is more
Change it to standard

FORTINET

© Fortinet Inc. All Rights Reserved.

25

When creating CLI scripts, follow these best practices:

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Examine FortiManager key features
- ✓ Explore FortiManager architecture
- ✓ Explore Device Manager wizards
- ✓ Deploy IPsec using VPN manager on FortiManager
- ✓ Learn about scripts

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

DO NOT REPRINT
© FORTINET

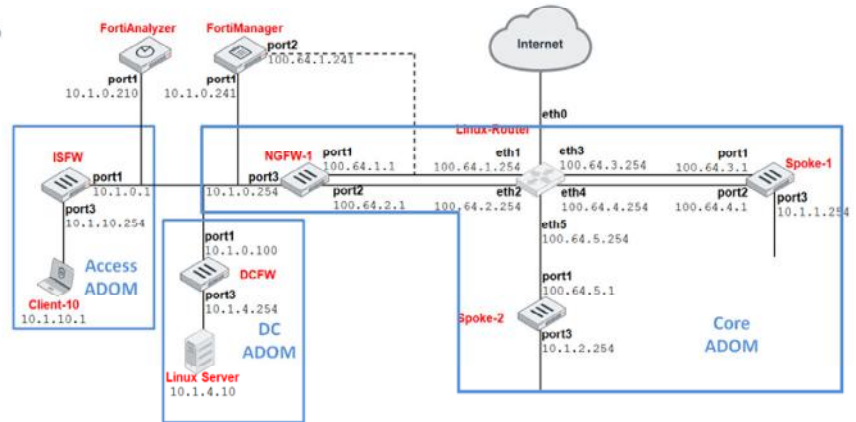
Lab 7—Central Management

You will now work on *Lab 7—Central Management*.

DO NOT REPRINT
© FORTINET

Lab 7—Central Management

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



FORTINET

© Fortinet Inc. All Rights Reserved.

28

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

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about Open Shortest Path First (OSPF) concepts, and how to configure and troubleshoot OSPF.

DO NOT REPRINT
© FORTINET

Objectives

- Understand OSPF components
- Segment an OSPF network into areas
- Identify different types of link state advertisements
- Determine the OSPF cost for any route
- Establish OSPF adjacencies
- Differentiate between a designated router and a backup designated router in a multi-access network
- Troubleshoot common OSPF problems
- Monitor the status of an OSPF network

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

By demonstrating competence in understanding OSPF, you will be able to understand, configure, and troubleshoot OSPF.

DO NOT REPRINT
© FORTINET

OSPF Review

In this section, you will review OSPF.

DO NOT REPRINT
© FORTINET

OSPF Overview

- Link state protocol
- Advantages:
 - Scalable to large networks
 - Faster convergence than distance-vector routing protocols
 - Relatively quiet during steady-state conditions
 - Periodic refresh every 30 minutes
 - Otherwise, updates only sent when there are changes
- Disadvantages:
 - May require planning and tuning to optimize performance
 - May be difficult to troubleshoot in large networks

FORTINET

© Fortinet Inc. All Rights Reserved.

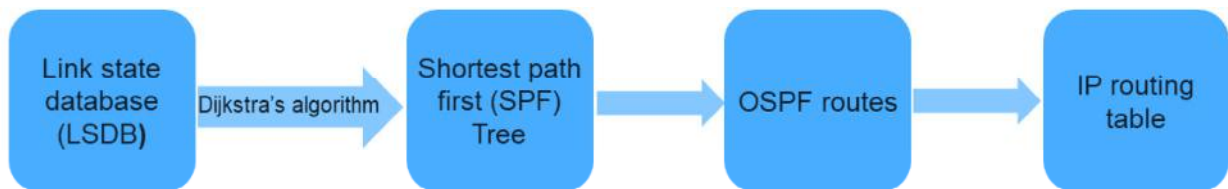
4

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

DO NOT REPRINT
© FORTINET

OSPF Components

- Link state database (LSDB): Each router maintains identical databases describing the network topology
- From the LSDB and using Dijkstra's algorithm, each router builds a tree with the shortest paths
- The tree gives an OSPF route to each destination
- OSPF routes can be injected into the IP routing table



Each router in the same area has identical and synchronized databases. You will learn about OSPF areas later in this lesson. An OSPF router uses the information in the LSDB and Dijkstra's algorithm to generate an OSPF tree, which contains the shortest path from the local router to each other router and network. This tree gives the best route to each destination, which is the information that OSPF can inject into the device's routing table.

DO NOT REPRINT
© FORTINET

Link State Advertisement

- Routers exchange link state advertisements (LSAs) to maintain consistent databases
 - Network changes generate LSAs
 - The LSDBs are composed of all received LSAs
- A link state update consists of an OSPF header and a string of LSAs
 - Each LSA has its own header
 - Routers acknowledge the receipt of any LSA

IP Header	OSPF Header	Number of LSAs	LSA 1	LSA 2	...	LSA <i>n</i>
-----------	-------------	----------------	-------	-------	-----	--------------

The topology information interchanged by OSPF peers is contained in LSAs. A router's LSDB is populated with the information from the local LSAs and all the LSAs received from other routers.

DO NOT REPRINT
© FORTINET

OSPF Cost

- Metric in OSPF is cost:
 - 16-bit positive number (1 to 65,535)
- The lower, the more desirable
- Route decisions made on total cost of a path to the final destination

If there are multiple OSPF routes to the same destination subnet, OSPF selects the route with the lowest cost. Each router interface is associated with an interface cost, which is usually related with how fast or preferable that interface is. An OSPF route cost is the sum of all interfaces' costs to the final destination.

DO NOT REPRINT
© FORTINET

LSDB

- Each router advertises its locally connected subnets
- LSDBs in all routers contain information about the network topology

Link State Database (network/cost)

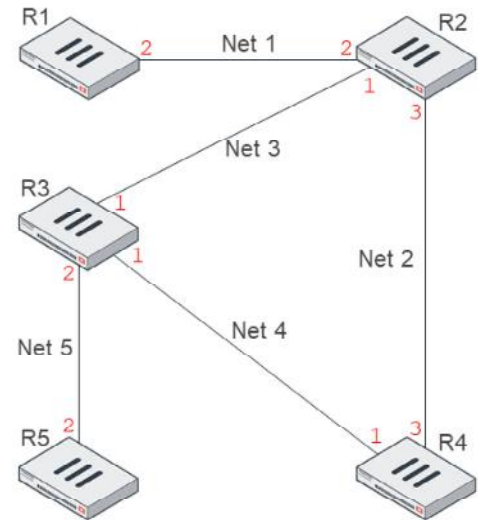
R2 Net 1/2, Net 2/3, Net 3/1

R1 Net 1/2

R3 Net 3/1, Net 4/1, Net 5/2

R4 Net 2/3, Net 4/1

R5 Net 5/2



FORTINET

© Fortinet Inc. All Rights Reserved.

8

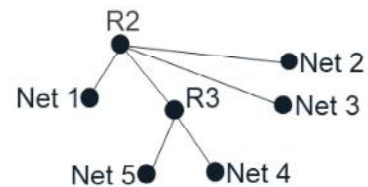
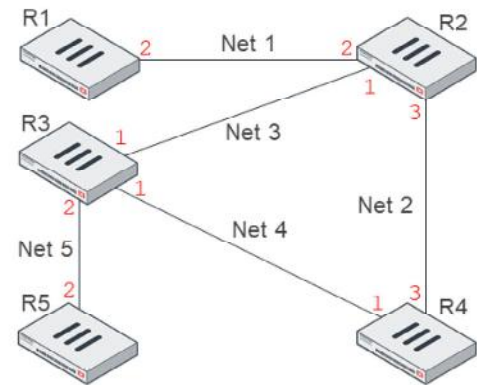
The next two slides explain how an OSPF router builds its OSPF tree. The initial information for each router is the locally connected networks, together with the OSPF cost for each interface. In the example shown on this slide, the router R2 has three locally connected subnets: subnet Net 1 with a cost of 2, subnet Net 2 with a cost of 3, and subnet Net 3 with a cost of 1. Router R1 has only one subnet connected: Net 1 with a cost of 2, and so on.

Each router starts advertising its locally connected subnets by sending LSAs.

DO NOT REPRINT
© FORTINET

OSPF Tree

- Routers use Dijkstra's algorithm to determine the best path to each destination
 - The best path has the lowest overall cost
 - The destination is either a network or a router
- Routers build an OSPF tree
 - During each iteration, all known paths to a destination are mapped and the lowest path is chosen
 - This process is repeated until the best path to each destination is discovered



© Fortinet Inc. All Rights Reserved.

9

OSPF routers use Dijkstra's algorithm to determine the best route to each destination. The best routes can be represented as a tree with the local router at the root. Dijkstra's algorithm is a recursive process that is repeated multiple times until the best routes are found. For example, this slide shows the OSPF tree for router R2. It indicates that the best route to Net 5 and Net 4 is through R3, and that Net 1, Net 2, and Net 3 are locally connected.

DO NOT REPRINT
© FORTINET

OSPF Area

- A logical collection of OSPF networks and routers
- Defined with a 32-bit number
 - IP address format
0.0.0.10
 - As a single decimal value
10

FORTINET

© Fortinet Inc. All Rights Reserved.

10

An OSPF network can be segmented into areas. Each area is identified by a unique number, which can be represented either in decimal or IP address format.

DO NOT REPRINT
© FORTINET

OSPF Areas

- When a network is broken up into areas, routers maintain separate LSDBs for each area
- Advantages:
 - Smaller LSDB tables
 - Impact of a topology change is minimized outside the area
 - Routes can be summarized on the area borders
- Disadvantages:
 - More complex to troubleshoot
 - Network design considerations

Each area has its own separate LSDB. All routers in the same area maintain an identical copy of the area's LSDB. As you will learn in this lesson, a router can belong to more than one area. In those cases, the router maintains multiple LSDBs—one LSDB for each area connected to it.

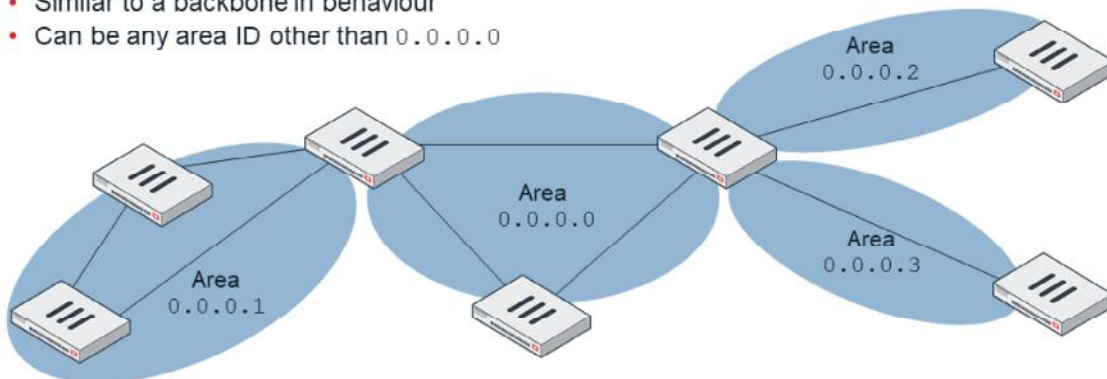
Segmenting big OSPF networks into areas reduces the sizes of the LSDB tables. Additionally, a topology change does not impact the whole network, but only the area where the change happens.

Using OSPF areas requires good planning and may complicate the troubleshooting process.

DO NOT REPRINT
© FORTINET

Types of Areas

- **Backbone area**
 - Must have the area ID 0.0.0.0
 - All other areas must connect to the backbone by physical or virtual links
 - Distributes information between areas
- **Normal area**
 - Similar to a backbone in behaviour
 - Can be any area ID other than 0.0.0.0



FORTINET

© Fortinet Inc. All Rights Reserved.

12

All OSPF networks must have at least one area—the backbone area. The backbone is the core of the network, and all the other areas connect to it in a hub-and-spoke topology.

DO NOT REPRINT
© FORTINET

OSPF Router Types

- Internal router
 - All connected interfaces belong to the same area
 - Maintains one LSDB and one OSPF tree
- Area border router (ABR)
 - A router with interfaces in multiple areas
 - One LSDB and one OSPF tree for each connected area
 - Always connected to the backbone
- Backbone router
 - Has at least one interface in the backbone area
- Autonomous system boundary router (ASBR)
 - Imports external (non-OSPF) routes into OSPF
 - Has at least one source of routing information that is not of OSPF origin

FORTINET

© Fortinet Inc. All Rights Reserved.

13

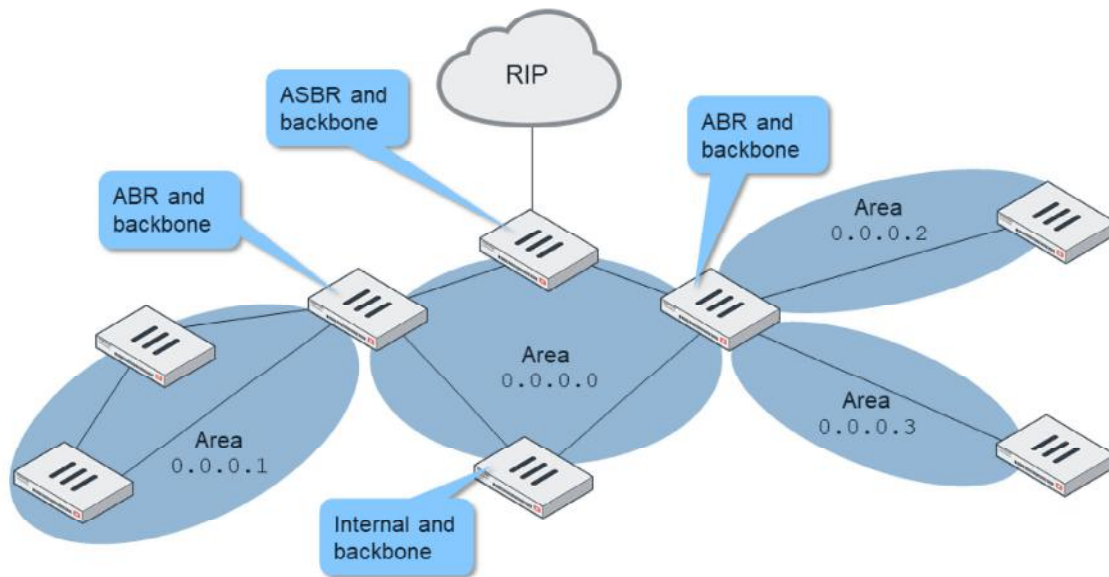
An internal OSPF router has all its interfaces connected to the same area. So, it maintains only one LSDB. On the other hand, an ABR is connected to multiple areas, so it keeps multiple LSDBs.

A backbone router has at least one interface connected to the backbone area.

An ASBR redistributes non-OSPF routes into the OSPF network.

DO NOT REPRINT
© FORTINET

OSPF Router Types Example



FORTINET

© Fortinet Inc. All Rights Reserved.

14

This slide shows an example of each router type.

DO NOT REPRINT
© FORTINET

Network Types

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

FORTINET

© Fortinet Inc. All Rights Reserved.

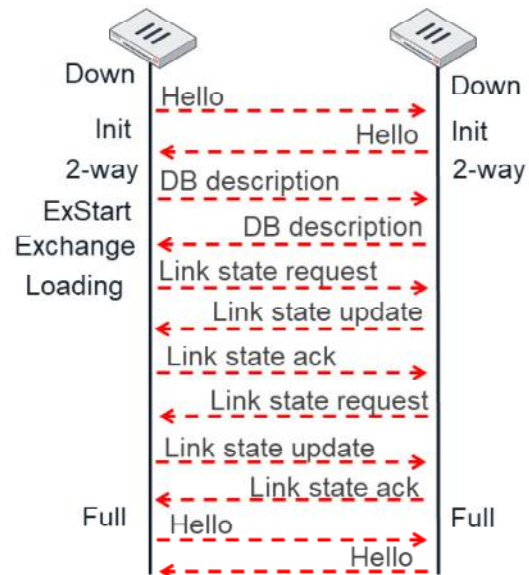
15

There are three types of OSPF networks:

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

Forming an Adjacency

- **Down:** Initial state
- **Init:** A hello packet was seen from a non-adjacent neighbor
- **2-Way:** Communication is bidirectional between the two routers
- **ExStart:** A primary and secondary relationship is negotiated
- **Exchange:** DB description packets are exchanged
- **Loading:** LSA information is exchanged
- **Full:** LSDBs are identical



An OSPF session between two OSPF peers is called an adjacency. This slide shows the initial interchange between two peers that are forming an adjacency. Any new adjacency goes through different states: Init, 2-way, ExStart, Exchange, Loading, and Full. The Full state indicates that the adjacency has successfully formed, and both routers have identical copies of the LSDB.

DO NOT REPRINT
© FORTINET

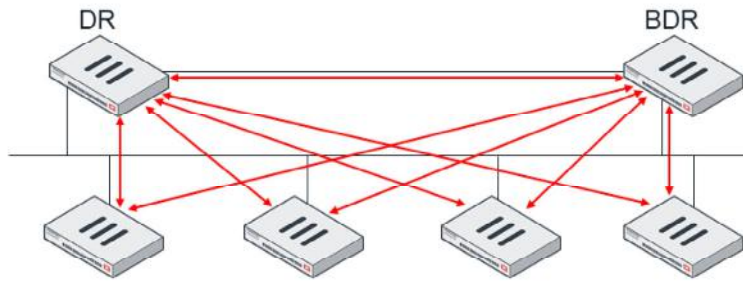
Adjacency Requirements

- Requirements for forming an adjacency:
 - Peers' primary IP addresses are in the same subnet with the same mask
 - Peers' interfaces are the same type and in the same OSPF area
 - Peers' hello and dead interval match
 - Each peer has an unique router ID
 - OSPF IP MTUs match
 - OSPF authentication, if enabled, is successful

This slide lists the requirements for two peers to form an OSPF adjacency. If any of the requirements are not met, the adjacency fails and will not reach the full state.

Designated Router

- In multi-access networks, one designated router (DR) and one backup DR (BDR) are elected
 - Router priority: highest priority wins, 0 = never become a DR
 - Router ID: highest ID wins
- If the DR fails, the BDR takes the DR role
- Full adjacencies are only formed to the DR and BDR to reduce resource utilization



In any multiaccess network there is one DR and one BDR. The router with the highest priority is elected as the DR. If two or more routers are tied with the highest priority, the router with the highest OSPF ID is elected.

The BDR monitors the DR status. If the DR fails, the BDR takes the DR role.

Other routers form adjacencies only with the DR and the BDR. The DR forwards the link state information from one router to another. This simplifies the amount of adjacencies required in multi-access networks.

DO NOT REPRINT
© FORTINET

OSPF Destination Addresses

- On broadcast networks, OSPF uses two multicast destination addresses
 - 224.0.0.5 AllSPFRouters
 - Hello packets
 - LSA updates and acknowledgements sent by either the DR or BDR
 - 224.0.0.6 AllDRouters
 - LSA updates and acknowledgements sent by all other routers
- On point-to-point networks
 - 224.0.0.5 AllSPFRouters
 - All packets are sent to this address
- Some OSPF packets may be unicast
 - Database description (DD) packets exchanged
 - LSA retransmissions

This slide shows the multicast addresses used by OSPF in broadcast multiaccess, and point-to-point networks. Keep in mind that OSPF also uses unicast addresses for LSA retransmissions and database description packets.

DO NOT REPRINT
© FORTINET

LSA Types

- There are 11 LSA types. These are the five most common:
 - Type 1: Router link advertisement
 - Describes a router's links. Confined within an area
 - Type 2: Network link advertisement
 - Describes all the routers (if more than one) in a multiaccess network. Confined within an area.
 - Type 3: Summary link advertisement
 - Describes summarized networks within an area. Generated by the ABR.
 - Type 4: AS summary link advertisement
 - Describes the path to an ASBR router
 - Type 5: AS external link advertisement
 - Describes external destinations originated on an ASBR. Generated by the ASBR.

FORTINET

© Fortinet Inc. All Rights Reserved.

20

There are 11 LSA types. This lesson covers the five most commonly used:

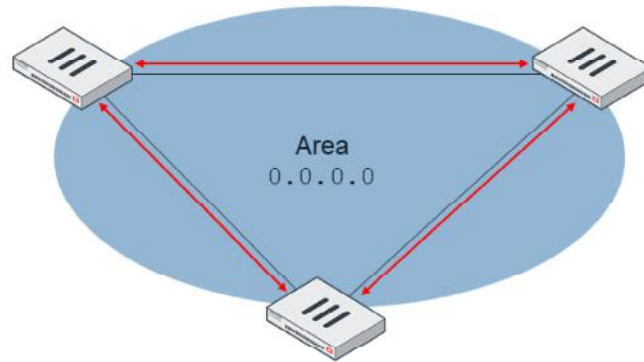
- Type 1 describes all the links connected to a router
- Type 2 describes all the routers (if more than one) in a multiaccess network
- Type 3 describes the networks within an area (only generated by an ABR)
- Type 4 describes the path to reach an ASBR
- Type 5 describes the external destinations originated by an ASBR

You will see examples of each of these five types in the next slides.

DO NOT REPRINT
© FORTINET

Router Link Advertisements (Type 1)

- Advertised by every OSPF router in an area
- Describe router network connections within that area



FORTINET

© Fortinet Inc. All Rights Reserved.

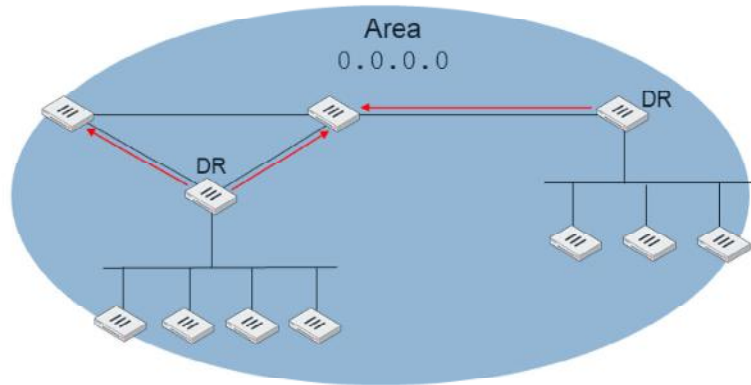
21

Type 1 describes the networks connected to a router. They are advertised by all the routers in an area. Type 1 LSAs are not advertised outside the area where they originate.

DO NOT REPRINT
© FORTINET

Network Link Advertisements (Type 2)

- Advertised by every DR
- Contains the list of routers connected to a multiaccess network



FORTINET

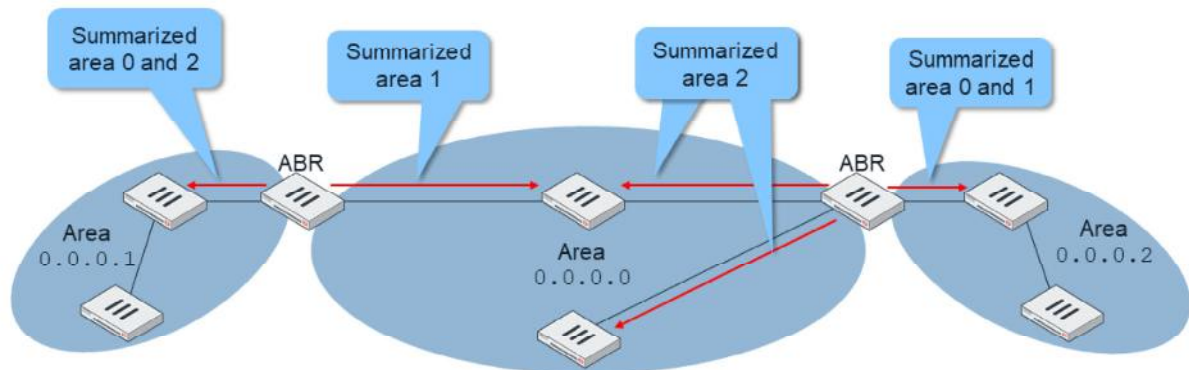
© Fortinet Inc. All Rights Reserved.

22

Type 2 LSAs are advertised only by DRs. In this example, the area has two multi-access networks, each of them with one DR. The two DRs advertise type 2 LSAs, which contain information about the other routers connected to their multiaccess networks.

Summary Link Advertisements (Type 3)

- Generated only by area border routers
- Can be used to summarize networks
 - One LSA can represent a range of networks



FORTINET

© Fortinet Inc. All Rights Reserved.

23

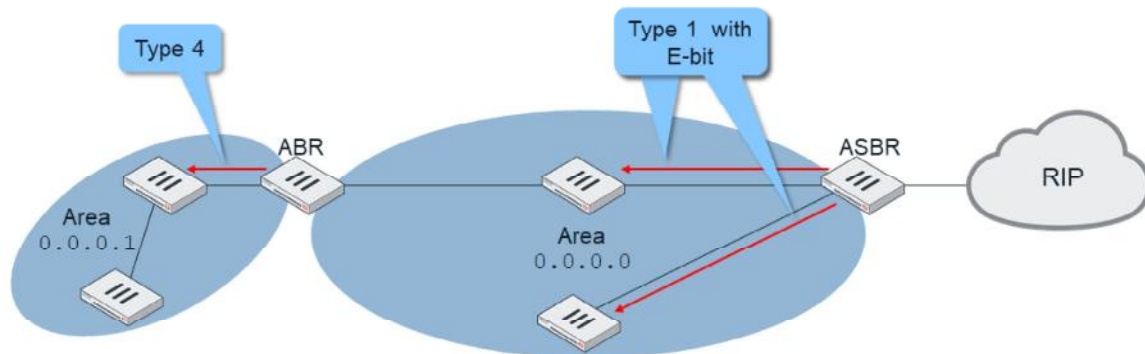
Type 3 LSAs contain summarized link state information. They are advertised only by ABRs. In this example, the ABR on the left sends type 3 LSAs to area 1. They contain link state information for the summarized subnets in areas 0 and 2. This same ABR also sends type 3 LSAs to the backbone area, with a summary of the subnets in area 1.

Something similar happens with the ABR shown on the right side of the diagram. It sends type 3 LSAs to area 2. They contain link state information for the summarized subnets in areas 0 and 1. This same ABR also sends type 3 LSAs to the backbone area, with a summary of the subnets in area 2.

DO NOT REPRINT
© FORTINET

AS Summary Link Advertisements (Type 4)

- An ASBR announces itself by setting the E-bit in its router link advertisements
- The ABRs in the same area generate a type 4 advertisement to the other areas

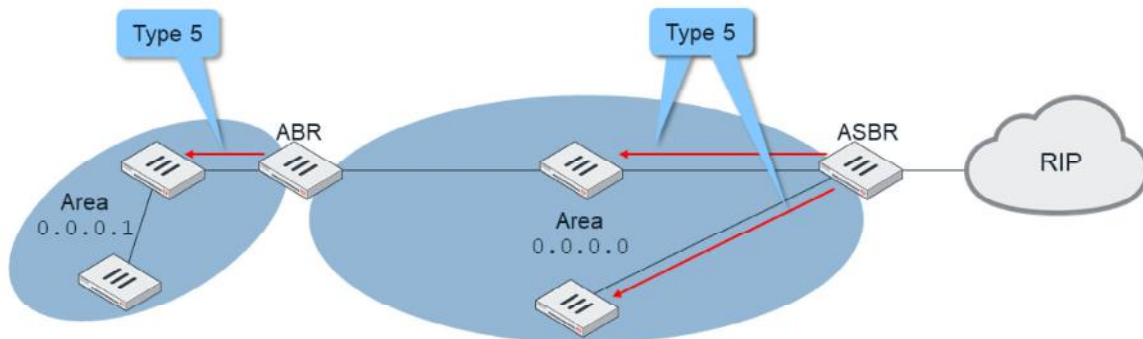


An ASBR advertises itself by sending type 1 LSAs. These LSAs have the E-bit on in the OSPF header. Like any other type 1, the LSAs with the E-bit are confined to the area where they originate. However, ABRs in the same area send a type 4 LSA to the other areas with information about how to reach the ASBR. In this example, an ASBR that is redistributing RIP routes into OSPF announces itself by sending type 1 LSAs to the backbone area. The ABR receives that LSA and sends a type 4 LSA to the area 1.

DO NOT REPRINT
© FORTINET

AS External Link Advertisements (Type 5)

- OSPF views non-OSPF networks as external
- The following are considered to be external:
 - A directly connected interface not running OSPF
 - A static route
 - A route derived from a different routing protocol



FORTINET

© Fortinet Inc. All Rights Reserved.

25

The last type of LSA covered in this lesson is type 5. Type 5 LSAs are sent only by the ASBRs and are not confined to one area. They reach all the standard areas. They contain link state information for routes redistributed to OSPF (also called external routes).

Note that all the area examples in this lesson are standard areas. There are also stub and not-so-stubby areas (NSSA), which are not covered in this lesson. Type 5 LSAs are not advertised to stub or NSSAs.

DO NOT REPRINT
© FORTINET

External Route Metrics Types

- Type 1
 - Are considered *close* to the AS
 - Metric is based on the sum of the internal and external costs
- Type 2
 - Are considered *far away* from the AS
 - Metric is based on the external cost only
- A type 1 external route is preferred over a type 2

Each external route is assigned a metric. There are two types of external-route metrics. A type 1 metric is the sum of the external cost plus the internal cost to reach the ASBR. A type 2 metric is only the external cost (the internal cost is not considered). If there are two external routes to the same destination, one type 1 and one type 2, an OSPF router selects the type 1 over the type 2.

DO NOT REPRINT
© FORTINET

Basic OSPF Configuration

- Configure the router ID
- Define the OSPF area
- Select the networks on which to enable OSPF

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

FORTINET

© Fortinet Inc. All Rights Reserved.

27

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

DO NOT REPRINT
© FORTINET

ASBR Configuration

- By enabling route redistribution, the FortiGate becomes an ASBR:

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

FORTINET

© Fortinet Inc. All Rights Reserved.

28

Any FortiGate that is redistributing non-OSPF routes into OSPF is an ASBR.

DO NOT REPRINT
© FORTINET

OSPF Troubleshooting

In this section, you will learn about tools and tips for troubleshooting OSPF problems.

DO NOT REPRINT
© FORTINET

OSPF Status

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

FORTINET

© Fortinet Inc. All Rights Reserved.

30

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

DO NOT REPRINT
© FORTINET

OSPF Status

....

Number of non-default external LSA 1

External LSA database is unlimited.

Number of LSA originated 36

Number of LSA received 13

Number of areas attached to this router: 1

Area 0.0.0.0 (BACKBONE)

Backbone router

Number of interfaces in this area is 3(3)

Number of fully adjacent neighbors in this area is 2

Shows number of fully adjacent neighbors

Area has no authentication

SPF algorithm last executed 00:02:38.780 ago

SPF algorithm executed 32 times

Number of LSA 5. Checksum 0x028b9c

FORTINET

© Fortinet Inc. All Rights Reserved.

31

This command also shows information about each area the router belongs to.

DO NOT REPRINT
© FORTINET

OSPF Interfaces

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

  Designated Router (ID) 0.0.0.2, Interface Address 10.10.2.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 10.10.2.1
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5

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

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

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

Local router is a DR

Number of adjacencies

FORTINET

© Fortinet Inc. All Rights Reserved.

32

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

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

DO NOT REPRINT
© FORTINET

OSPF Neighbours

```
Spoke1 # get router info ospf neighbor
```

OSPF process 0, VRF 0:

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

This represents a
point-to-point network

FORTINET

© Fortinet Inc. All Rights Reserved.

33

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

DO NOT REPRINT
© FORTINET

OSPF LSDB

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

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

```
Router Link States (Area 0.0.0.0)
```

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

```
Net Link States (Area 0.0.0.0)
```

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

```
AS External Link States
```

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

FORTINET

© Fortinet Inc. All Rights Reserved.

34

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

DO NOT REPRINT
© FORTINET

Self-Originated LSAs

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

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

```
Router Link States (Area 0.0.0.0)
```

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

```
Net Link States (Area 0.0.0.0)
```

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

FORTINET

© Fortinet Inc. All Rights Reserved.

35

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

DO NOT REPRINT
© FORTINET

LSA Details

```
Spoke1 # get router info ospf database router lsa
      OSPF Router with ID(0.0.0.1) (Process ID 0, VRF 0)
      Router Link States (Area 0.0.0.0)

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

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

...

FORTINET

© Fortinet Inc. All Rights Reserved.

36

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

DO NOT REPRINT
© FORTINET

LSA Details

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

37

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

DO NOT REPRINT
© FORTINET

OSPF Troubleshooting

- Enable real-time debug

```
# diagnose ip router ospf all enable
# diagnose ip router ospf level info
# diagnose debug enable
```
- Disable real-time debug

```
# diagnose ip router ospf all disable
# diagnose debug disable
```
- Restart OSPF process

```
# execute router clear ospf process
```
- By default, routing real-time debugs stop running after you restart the routing process
 - Enable the `z1` flag to have the real-time debug persist after the process restart:

```
# diagnose ip router z1 enable
```

diagnose debug reset does
not stop OSPF real time debug

FORTINET

© Fortinet Inc. All Rights Reserved.

38

The OSPF real-time debug displays information about adjacency establishments and OSPF errors. It also shows information about network topology changes.

You can enable the `z1` flag for the real-time debug to persist after a routing-process restart.

DO NOT REPRINT
© FORTINET

Sample Debug Output

```
OSPF: SEND[Hello]: To 224.0.0.5 via port3:10.1.0.254, length 52
```

```
OSPF: -----  
OSPF: Header  
OSPF:   Version 2  
OSPF:   Type 1 (Hello)  
OSPF:   Packet Len 52  
OSPF:   Router ID 0.0.0.1  
OSPF:   Area ID 0.0.0.0  
OSPF:   Checksum 0xe78d  
OSPF:   AuType 0  
OSPF: Hello  
OSPF:   NetworkMask 255.255.255.0  
OSPF:   HelloInterval 10  
OSPF:   Options 0x2 (*|---|---|E|---)  
OSPF:   RtrPriority 1  
OSPF:   RtrDeadInterval 40  
OSPF:   DRouter 10.1.0.254  
OSPF:   BDRouter 10.1.0.1  
OSPF:   # Neighbors 2  
OSPF:     Neighbor 0.0.0.3  
OSPF:     Neighbor 0.0.0.4  
...
```

Hello packet sent
to OSPF multicast
address

FORTINET

© Fortinet Inc. All Rights Reserved.

39

This is a sample of output generated by the OSPF real-time debug. This sample shows the Hello packet being sent.

DO NOT REPRINT
© FORTINET

Sample Debug Output

```
OSPF: RECV[Hello]: From 0.0.0.4 via port3:10.1.0.254 (10.1.0.100 -> 224.0.0.5)
```

```
OSPF: -----
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 52
OSPF:   Router ID 0.0.0.4
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0xe78d
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*|---|---|E|)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 10.1.0.254
OSPF:   BDRouter 10.1.0.1
OSPF:   # Neighbors 2
OSPF:     Neighbor 0.0.0.3
OSPF:     Neighbor 0.0.0.1
OSPF: -----
OSPF: NFSM[port3:10.1.0.254-0.0.0.4]: Full (HelloReceived)
OSPF: NFSM[port3:10.1.0.254-0.0.0.4]: nfsm_ignore called
OSPF: NFSM[port3:10.1.0.254-0.0.0.4]: Full (2-WayReceived)
...
```

Hello packet is
received from
neighbor connected
to wan2

FORTINET

© Fortinet Inc. All Rights Reserved.

40

This is another sample of output generated by the OSPF real-time debug. This sample shows the `Hello` packet being received.

DO NOT REPRINT
© FORTINET

OSPF Logging

- FortiGate logs OSPF routing events, such as:
 - Neighbor down or up
 - OSPF message exchange
 - Negotiation errors
- Enabled by default under:

```
# config router ospf
  set log-neighbour-change enable
  ...
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

41

By default, FortiGate logs the most important OSPF routing events, such as:

- Neighbor down or up
- OSPF message exchange
- Negotiation errors

DO NOT REPRINT
© FORTINET

OSPF Logging

Log & Report > Events > Router Events

#	Level	Message
1	Info	OSPF: %OSPF-5-ADJCHANGE: neighbor port1:10.1.0.1-0.0.0.4 Up
2	Info	OSPF: %OSPF-5-ADJCHANGE: neighbor port1:10.1.0.1-0.0.0.4 Down
3	Info	OSPF: %OSPF-5-ADJCHANGE: neighbor port1:10.1.0.1-0.0.0.1 Up
4	Info	OSPF: %OSPF-5-ADJCHANGE: neighbor port1:10.1.0.1-0.0.0.2 Up
5	Info	OSPF: RECV[LS-Ack]: From 0.0.0.2 via port1:10.1.0.1: State is less than Exchange
6	Info	OSPF: RECV[DD]: From 0.0.0.2 via port1:10.1.0.1: Negotiation fails, packet discarded
7	Info	OSPF: RECV[DD]: From 0.0.0.1 via port1:10.1.0.1: Negotiation fails, packet discarded
8	Info	OSPF: %OSPF-5-ADJCHANGE: neighbor port1:10.1.0.1-0.0.0.2 Up
9	Info	OSPF: %OSPF-5-ADJCHANGE: neighbor port1:10.1.0.1-0.0.0.1 Up
10	Info	OSPF: RECV[DD]: From 0.0.0.1 via port1:10.1.0.1: Negotiation fails, packet discarded

Log Details

General
Date: 2020/04/30
Time: 19:08:09
Virtual Domain: root
Log Description: Routing log

Data
Message: OSPF: RECV[DD]: From 0.0.0.2 via port1:10.1.0.1: Negotiation fails, packet discarded

Security
Level: Info

Other
Log ID: 0103020301
Type: event
Sub Type: router
Log event original timestamp: 1588298889957231900
Timezone: -0700

FORTINET

© Fortinet Inc. All Rights Reserved.

42

You can view OSPF-related router events on the GUI. You can click any logged entry to view the details.

Review

- ✓ Review OSPF components
- ✓ Understand cost and external route metric
- ✓ Identify OSPF area types
- ✓ Identify OSPF router types
- ✓ Understand how OSPF adjacencies are formed
- ✓ Differentiate between a DR and a BDR
- ✓ Understand different types of LSAs
- ✓ Configure OSPF
- ✓ Troubleshoot OSPF issues
- ✓ View OSPF-related logs

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

DO NOT REPRINT
© FORTINET

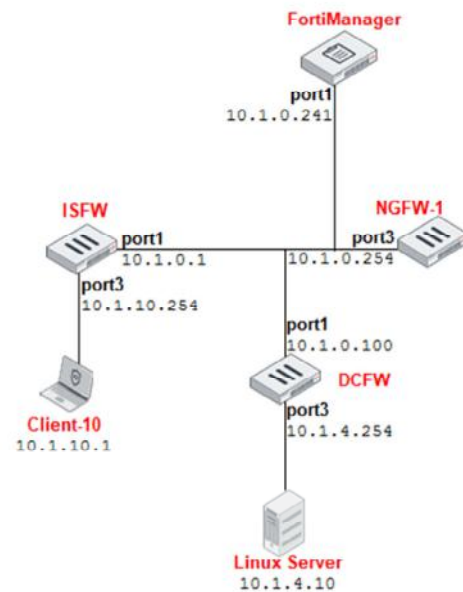
Lab 8—OSPF

Now, you will work on *Lab 8—OSPF*.

DO NOT REPRINT
© FORTINET

Lab 8—OSPF

- For each FortiGate:
 - Add OSPF router ID
 - Add OSPF area
 - Add OSPF network(s)
 - Remove static routes
- Troubleshoot:
 - OSPF problem between the DCFW and the Linux server



FORTINET

© Fortinet Inc. All Rights Reserved.

45

In this lab, you will configure FortiGate devices using FortiManager to use OSPF as the dynamic routing protocol for the enterprise network. You will learn how to use OSPF diagnostics commands, and you will use the debug commands available on FortiGate to troubleshoot an OSPF problem.

DO NOT REPRINT
© FORTINET



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

DO NOT REPRINT
© FORTINET

Objectives

- Configure BGP on FortiGate
- Monitor and verify the status of BGP communication
- Troubleshoot common BGP issues

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

By demonstrating competence in BGP, you will be able to configure FortiGate for BGP, monitor and check the status of a BGP communication and troubleshoot the most common external BGP issues.

DO NOT REPRINT
© FORTINET

BGP Review

In this section, you will review BGP and how to configure it on FortiGate.

DO NOT REPRINT
© FORTINET

Autonomous System (AS)

- Set of routers and networks under the same, consistent administration
- An AS administrator is free to choose any internal routing architecture:
 - OSPF, RIP, and so on
- Each AS is identified by a unique number

An AS is a set of routers and networks under the same administration. Each AS is identified by a unique number, and usually runs an interior gateway protocol, such as OSPF or RIP.

DO NOT REPRINT
© FORTINET

BGP

- You can configure BGP to operate as EBGp or IBGP:
 - External BGP (EBGP) advertises routing updates across multiple ASs
 - Internal BGP (IBGP) advertises routing updates within the same AS
- BGP is typically used when the network requires:
 - Large numbers of routes
 - Strict control over what routes are announced or accepted
- BGP4 is the dominant external gateway protocol today:
 - Example: the Internet

FORTINET

© Fortinet Inc. All Rights Reserved.

5

BGP can serve one of two purposes: EBGp and IBGP.

An exterior gateway protocol (EGP) exchanges routing information between autonomous systems. BGP4, which runs in the Internet, is the dominant EGP protocol today. EBGp is typically used when strict control is required over a large number of routes.

Two EBGp routers exchange AS path information for destination prefixes or subnets. When two routers start a EBGp communication, the whole BGP routing table is interchanged. After that, only network updates are sent.

DO NOT REPRINT
© FORTINET

BGP Components

- Speaker or peer:
 - Router that transmits and receives BGP messages, acting upon those messages
- Session:
 - Connectivity between two peers

FORTINET

© Fortinet Inc. All Rights Reserved.

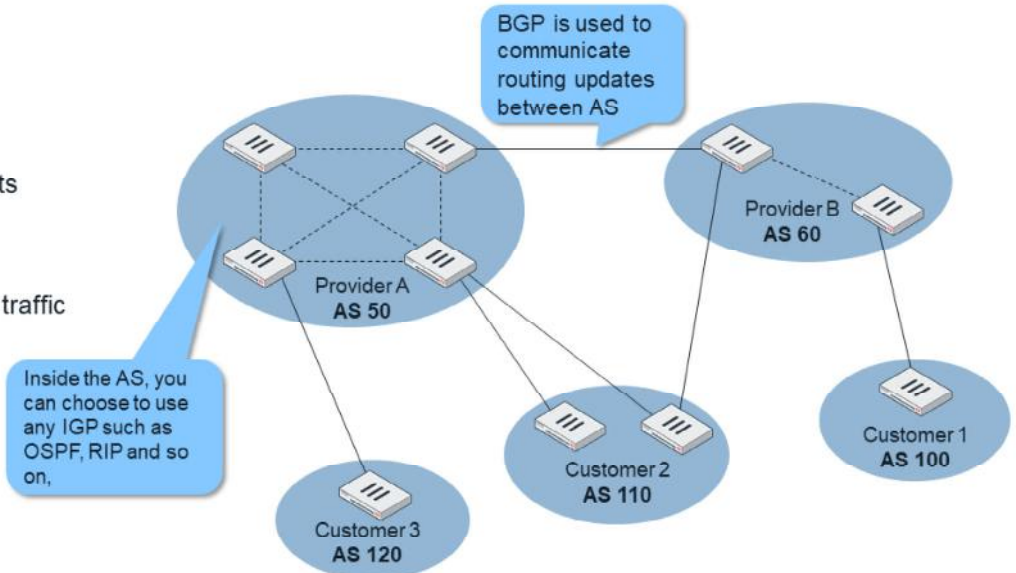
6

A BGP speaker or peer is a router that sends and receives BGP routing information. The connection between two BGP peers is called a BGP session.

DO NOT REPRINT
© FORTINET

AS Types

- Stub AS:
 - Single exit point
 - Local traffic
- Multihomed AS:
 - Multiple exit points
 - Local traffic
- Transit AS:
 - Local and transit traffic



FORTINET

© Fortinet Inc. All Rights Reserved.

7

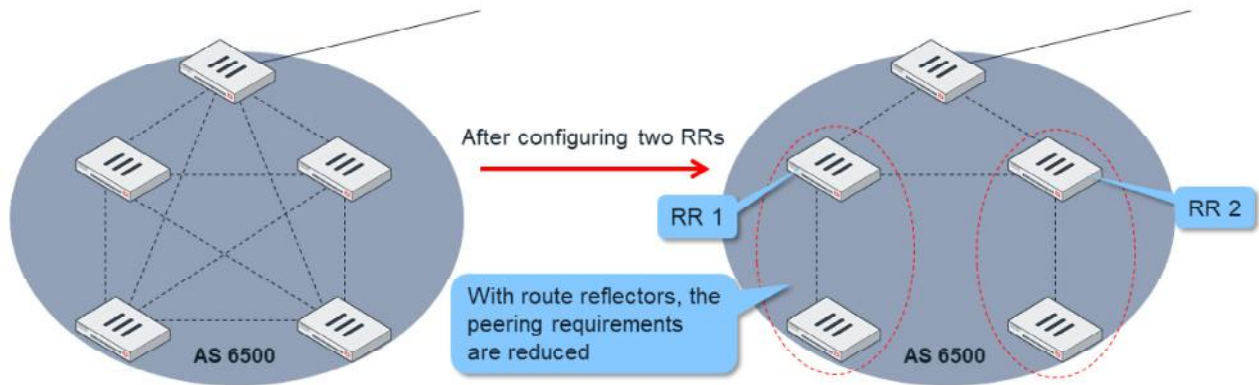
There are three types of autonomous systems:

- A stub AS handles and routes local traffic only and has only one connection to another AS. One example is a company that is running BGP, and has its own AS number and one ISP connection.
- Multihomed AS also handles and routes local traffic only, but it has multiple connections to different autonomous systems. One example is a company that is running BGP, and has its own AS number and multiple ISP connections.
- Transit AS handles and routes local traffic as well as traffic that originates and terminates in different autonomous systems (transit traffic). An ISP is an example of a transit AS.

DO NOT REPRINT
© FORTINET

Route Reflector

- Running IBGP usually requires full mesh peering
- Route reflectors (RR) simplify the network and the configuration by:
 - Reducing the number of IBGP peers
 - Forwarding the routes learned from one peer to the other peers



FORTINET

© Fortinet Inc. All Rights Reserved.

8

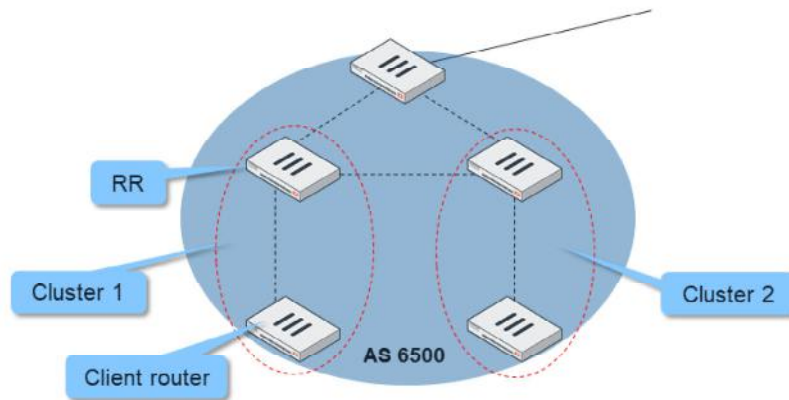
When running IBGP, you usually need to configure full mesh peering between all the routers. In large networks, full mesh peering between routers can be difficult to administer and is not scalable.

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

DO NOT REPRINT
© FORTINET

Route Reflector (Contd)

- An RR and its clients form a cluster
- All clients in a cluster communicate with the RR only for routing updates
- The RR communicates all routing updates to peers external to the cluster



FORTINET

© Fortinet Inc. All Rights Reserved.

9

In a BGP RR configuration, the AS is divided into different clusters that each include an RR and clients. The client routers communicate route updates only to the RR in the cluster. The RR communicates with other RRs and border routers. A FortiGate can be configured as either an RR or client.

DO NOT REPRINT
© FORTINET

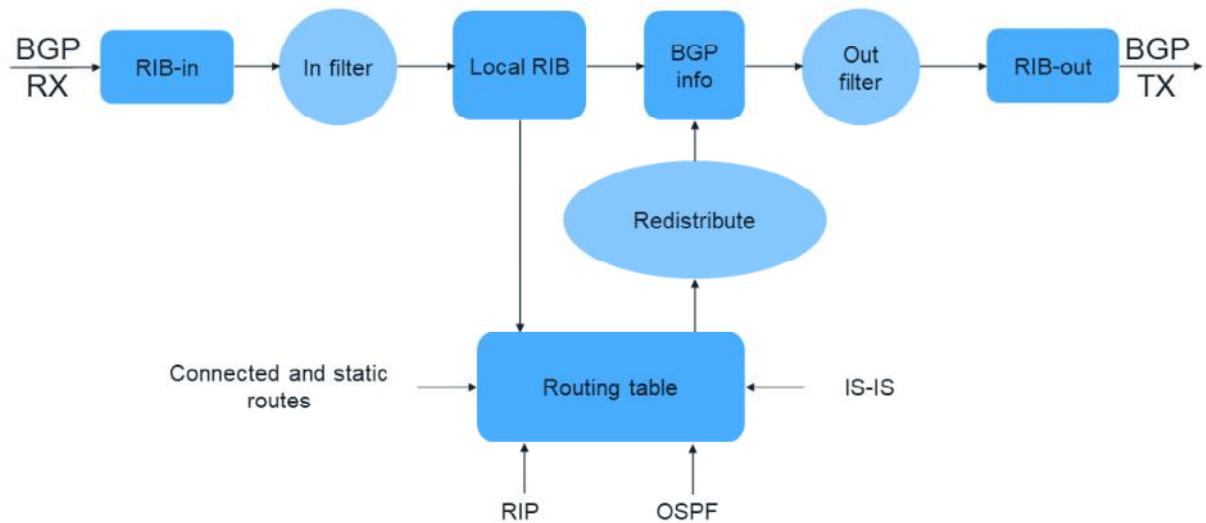
Routing Information Bases

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

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

DO NOT REPRINT
© FORTINET

Routing Information Bases (Contd)



FORTINET

© Fortinet Inc. All Rights Reserved.

11

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

DO NOT REPRINT
© FORTINET

BGP Attributes

- BGP processes routes based on path information
- A path is a route to a destination:
 - Paths are described by a set of attributes, including an AS list
 - The attributes help routers to select the route to each destination

BGP routes traffic based on AS paths. Each AS path includes attributes, which BGP uses to select the best route to each destination. One of the attributes is the AS list, which contains the autonomous systems through which the traffic must pass to reach the destination.

DO NOT REPRINT
© FORTINET

BGP Attribute

- BGP path attribute categories:

- Well-known mandatory:
 - Attributes are mandatory
- Well-known discretionary:
 - Attributes may or may not be included
- Optional transitive:
 - Attributes may or may not be accepted and can be passed outside of the local autonomous system
- Optional non-transitive:
 - Attributes may or may not be accepted and can't be passed outside of the local autonomous system

Supported Attributes	
ORIGIN	Well-known mandatory
AS_PATH	Well-known mandatory
NEXT_HOP	Well-known mandatory
MULTI_EXIT_DISC	Optional non-transitive
LOCAL_PREF	Well-known discretionary
ATOMIC_AGGREGATE	Well-known discretionary
AGGREGATOR	Optional transitive
COMMUNITY	Optional transitive

There are four types of BGP attributes:

- Well-known mandatory
- Well-known discretionary
- Optional transitive, which can be passed from one AS to another
- Optional non-transitive, which can't be passed from one AS to another

This slide shows a list of the BGP attributes and their attribute types that are supported by FortiGate.

DO NOT REPRINT
© FORTINET

Route Selection

- Route selection tie breakers:
 1. Highest weight
 2. Highest local preference
 3. Prefer the path that was locally originated
 4. Shortest AS path
 5. Lowest origin type
 6. Lowest multi-exit discriminator (MED)
 7. Lowest IGP metric to the BGP next-hop
 8. Prefer external paths (EBGP) over internal paths (IBGP)
 9. If ECMP is enabled, insert up to 10 routes in the routing table
 10. Lowest router ID

FortiGate uses some of the attributes during the routing selection process. If all those attributes for multiple routes to the same destination match, and if ECMP is enabled, FortiGate shares the traffic among up to 10 BGP routes. If you don't enable ECMP, FortiGate uses the route that goes to the router with the lowest BGP router ID.

DO NOT REPRINT
© FORTINET

FortiGate BGP Implementation

- Scaling capabilities:
 - No hard limits, system memory is the limitation
 - Number of neighbors, routes, and policies have an impact on the scaling capabilities
- By default, BGP doesn't originate any prefix:
 - Redistribution or policies are required
- By default, all routes received are accepted

FORTINET

© Fortinet Inc. All Rights Reserved.

15

There are three important things to consider when you implement BGP on FortiGate.

First, there are no hardcoded limits. Limitations on the number of neighbors, routes and policies depend exclusively on the available system memory.

Second, by default, FortiGate doesn't originate any prefix. You must enable redistribution, or manually indicate the prefixes that FortiGate originates.

Third, by default, FortiGate accepts all the prefixes it receives. Optionally, you can filter out or modify some prefixes.

DO NOT REPRINT
© FORTINET

Protocol Redistribution

- A non-BGP route can be redistributed into BGP
- Optional route maps can filter out the redistribution of specific routes

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

FORTINET

© Fortinet Inc. All Rights Reserved.

16

By default, FortiGate BGP doesn't advertise prefixes. You can use the redistribution command to configure FortiGate to advertise prefixes. You can redistribute connected and static routes, and routes learned from other routing protocols, into BGP. Optionally, you can add route maps to filter the prefixes or modify some of their BGP attributes.

DO NOT REPRINT
© FORTINET

Network Command

- An alternative to redistribution of protocols into BGP:

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

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

17

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

DO NOT REPRINT
© FORTINET

Prefix Lists

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

```

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

config router bgp
  config neighbor
    edit 10.3.1.254
      set prefix-list-in filter-subnets
    next
  end
end

```

By default, traffic not matching the prefix list will be denied

FORTINET

© Fortinet Inc. All Rights Reserved.

18

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

With a prefix list, you can be more selective about which prefixes to advertise to each neighbor. Additionally, prefix lists allow you to select which prefixes you want to use from each neighbor. In this example, we are creating a prefix list that allows the prefix `10.0.0.0/8`, but blocks the prefix `10.1.0.0/16`. By default, all the traffic that does not match a prefix list is denied. The prefix list is applied in the incoming direction from the neighbor `10.3.1.254`. The local FortiGate applies this filter for all the prefix advertisements coming from `10.3.1.254`.

When applying a prefix list, all the prefixes that don't match an entry in the list are denied by default.

DO NOT REPRINT
© FORTINET

Basic FortiGate Configuration

```
config router bgp
  set as 65100
  set router-id 172.16.1.3
  config neighbor
    edit "172.16.1.1"
      set remote-as 65100
    next
  end
  config network
    edit 1
      set prefix 10.1.0.0 255.255.255.0
    next
  end
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

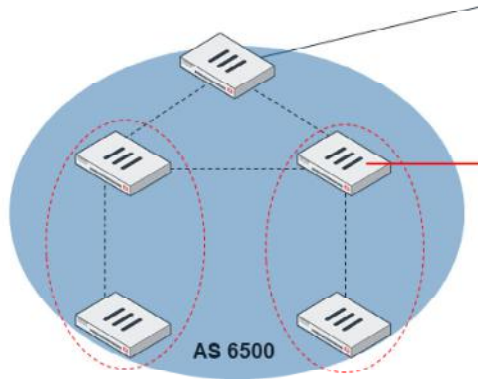
19

This slide shows an example of a basic FortiGate configuration. In this case, `remote-as` is the same as `local` AS, which means it is an IBGP configuration.

DO NOT REPRINT
© FORTINET

RR Configuration

- Configuration is done on the RR only
- Enable the `route-reflector-client` setting in each neighbor configuration section



```
config router bgp
config neighbor
edit <neighbor IPv4 address>
  set route-reflector-client enable
next
end
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

20

When implementing an RR, the configuration is done on the RR only. You can use the commands shown on this slide to configure each neighbor that will be participating in the RR cluster.

DO NOT REPRINT
© FORTINET

RR and Additional Path

- By default an RR propagates only one path for each prefix
- `additional-path` allows RR to propagate multiple paths for the same prefix
 - More efficient use of BGP multipath
 - Can prevent sub-optimal routing
 - Required for combining SDWAN and ADVPN

```
config router bgp
  set additional-path enable
  set additional-path-select <number_of_paths>
  config neighbor
    edit <neighbor_IP>
      set additional-path [send | receive | both | disable]
      set adv-additional-path <number_of_paths>
    end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

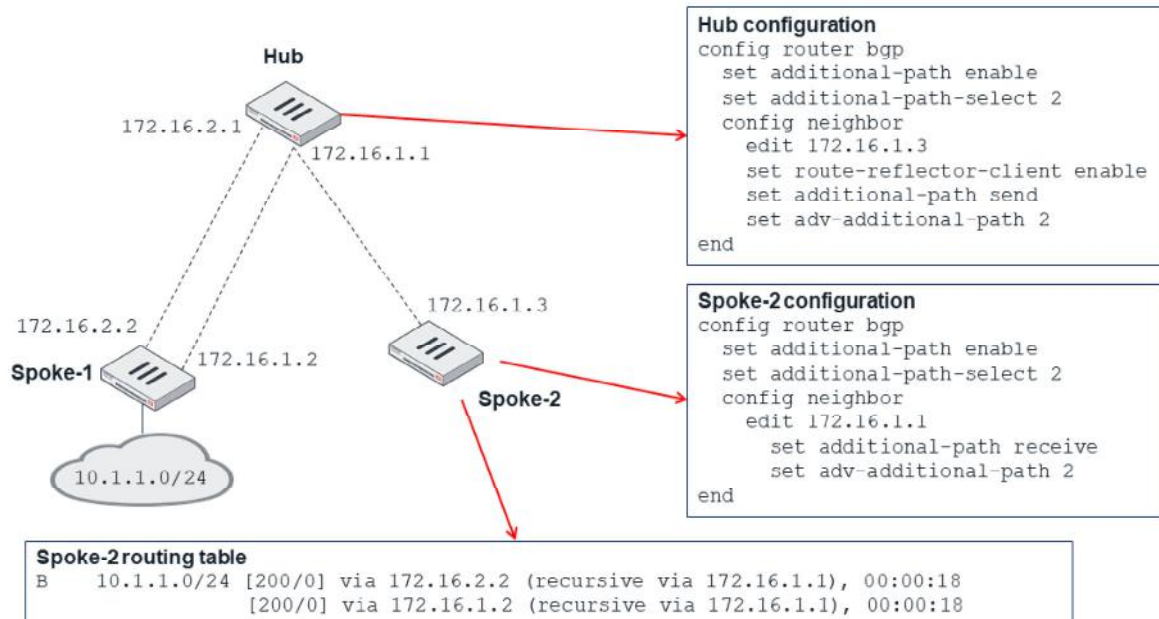
21

By default, a BGP route reflector propagates only one path for each prefix. If you enable `additional-path`, a FortiGate acting as a RR can propagate multiple paths for a same prefix. This allows a more efficient use of BGP, while it can prevent sub-optimal routing.

ADVPN requires all the hubs to be configured as BGP RR. Additionally, scenarios where you want to combine ADVPN with SDWAN requires BGP additional path. In those ADVPN and SDWAN scenarios, it is common to have multiple redundant IPsec tunnels between two locations. BGP additional path enables the ADVPN hub to dynamically propagate all the redundant paths to each remote location through BGP.

DO NOT REPRINT
© FORTINET

RR and Additional Path (Contd)



In this scenario, there are two redundant IPsec tunnels between Spoke-1 and Hub. There is also an IPsec between Spoke-2 and Hub. BGP over IPsec propagates the routing information. Hub is a route reflector with BGP additional path enabled.

As BGP additional path is enabled, Spoke-2 receives two BGP route advertisements from Hub: one for each redundant tunnel. ADVPN can use this routing to dynamically create on-demand IPsec tunnels between Spoke-2 and Spoke-1.

DO NOT REPRINT
© FORTINET

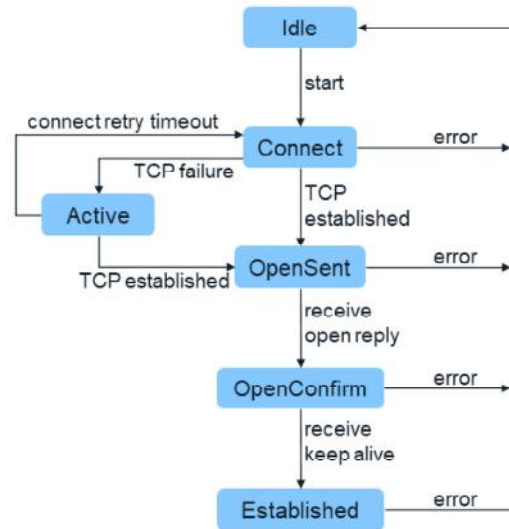
BGP Troubleshooting

In this section, you will learn about tools and tips for troubleshooting BGP.

DO NOT REPRINT
© FORTINET

BGP States

- **Idle:** Initial state
- **Connect:** Waiting for a successful three-way TCP connection
- **Active:** Unable to establish the TCP session
- **OpenSent:** Waiting for an **OPEN** message from the peer
- **OpenConfirm:** Waiting for the keepalive message from the peer
- **Established:** Peers have successfully exchanged **OPEN** and keepalive messages



FORTINET

© Fortinet Inc. All Rights Reserved.

24

This slide shows a flow chart of the BGP neighbor states and how they change:

- **Idle:** Initial state
- **Connect:** Waiting for a successful three-way TCP connection
- **Active:** Unable to establish the TCP session
- **OpenSent:** Waiting for an OPEN message from the peer
- **OpenConfirm:** Waiting for the keepalive message from the peer
- **Established:** Peers have successfully exchanged OPEN and keepalive messages

DO NOT REPRINT
© FORTINET

BGP Summary

```
NGFW-1 # get router info bgp summary
```

```
VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
```

```
BGP table version is 3
```

```
2 BGP AS-PATH entries
```

```
0 BGP community entries
```

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

```
Total number of neighbors 2
```

Remote AS

Packet count
(received and
sent)

How long the
connection
has been up

Neighbor state
and prefixes
received

FORTINET

© Fortinet Inc. All Rights Reserved.

25

This slide shows the debug command you usually use first, to get an overview of the BGP's status, and the status of all of its neighbors. This slide shows the local router ID and AS. For each neighbor, the output also displays the following:

- The AS
- Packet counters
- How long the neighbor has been up

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

DO NOT REPRINT
© FORTINET

BGP Neighbors

```
# get router info bgp neighbors
```

```
BGP neighbor is 100.64.1.254, remote AS 100, local AS 65100, external link  
BGP version 4, remote router ID 100.64.1.254  
BGP state = Established, up for 00:49:26  
Last read 00:00:26, hold time is 180, keepalive interval is 60 seconds  
Configured hold time is 180, keepalive interval is 60 seconds  
Neighbor capabilities:  
  Route refresh: advertised and received (old and new)  
  Address family IPv4 Unicast: advertised and received  
  Address family IPv6 Unicast: advertised  
Received 65 messages, 0 notifications, 0 in queue  
Sent 71 messages, 1 notifications, 0 in queue  
Route refresh request: received 0, sent 0  
Minimum time between advertisement runs is 30 seconds
```

FORTINET

© Fortinet Inc. All Rights Reserved.

26

You can use the command shown on this slide to get detailed information about each BGP neighbor. The information includes peer IP, peer router ID, remote AS, BGP state, various timers, and message counters.

DO NOT REPRINT
© FORTINET

BGP Neighbors (Contd)

```
...
For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes, 1 prefixes in rib
  0 announced prefixes

For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes, 0 prefixes in rib
  0 announced prefixes

Connections established 2; dropped 1
Local host: 100.64.1.1, Local port: 179
Foreign host: 100.64.1.254, Foreign port: 44760
Nexthop: 100.64.1.1
Nexthop interface: port1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:49:34, due to BGP Notification sent
Notification Error Message: (CeaseUnspecified Error Subcode)
```

FORTINET

© Fortinet Inc. All Rights Reserved.

27

The information also shows the number of prefixes announced and accepted, number of times that the session has dropped, and the last time it was reset.

DO NOT REPRINT
© FORTINET

Prefixes Advertised by the Local FortiGate

```
# get router info bgp neighbors 100.64.2.254 advertise
```

```
VRF 0 BGP table version is 3, local router ID is 172.16.1.254
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal  
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	RouteTag	Path
*> 0.0.0.0/0	100.64.2.1		xxx	0	0	100 i <-/->

```
Total number of prefixes 1
```

Next hop IP

Local preference
value

Route weight

AS path and
route origin
codes

FORTINET

© Fortinet Inc. All Rights Reserved.

28

This slide shows the command you can use to get details about the prefixes the local router is advertising. Status codes identifies codes associated with a routing entry. For each prefix, the command displays the following:

- Next hop IP
- Local preference
- Weight
- AS path

DO NOT REPRINT
© FORTINET

Prefixes Advertised by a Neighbor

```
# get router info bgp neighbors 100.64.2.254 route
```

```
VRF 0 BGP table version is 3, local router ID is 172.16.1.254
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	RouteTag	Path
* 0.0.0.0/0	100.64.2.254	0		0	0	100 100 100 i <-/->

```
Total number of prefixes 1
```

This slide shows the command you can use to display the routes advertised by a neighbor.

DO NOT REPRINT
© FORTINET

Real-Time Debug

- Enable real-time BGP debug:

```
# diagnose ip router bgp all enable
# diagnose ip router bgp level info
# diagnose debug enable
```
- Disable real-time BGP debug:

```
# diagnose ip router bgp all disable
# diagnose ip router bgp level none
# diagnose debug disable
```



© Fortinet Inc. All Rights Reserved.

30

This slide shows the commands you can use to enable and disable the BGP real-time debug. Note that this example enables debug output from event and level information.

DO NOT REPRINT
© FORTINET

BGP Neighbors

```

BGP: [NETWORK] Accept Thread: Incoming conn from host 100.64.2.254 (FD=27 VRF=0)
BGP: 100.64.2.254-Outgoing [FSM] State: Connect Event: 14
BGP: 100.64.2.254-Outgoing [FSM] InConnReq: Accepting...
BGP: 100.64.2.254-Outgoing [NETWORK] FD=27, Sock Status: 0-Success
BGP: 100.64.2.254-Outgoing [FSM] State: Connect Event: 17
BGP: 100.64.2.254-Outgoing [ENCODE] Msg-Hdr: Type 1
BGP: 100.64.2.254-Outgoing [ENCODE] Open: Ver 4 MyAS 65100 Holdtime 180
BGP: 100.64.2.254-Outgoing [ENCODE] Open: Msg-Size 61
BGP: 100.64.2.254-Outgoing [DECODE] Msg-Hdr: type 1, length 59
BGP: 100.64.2.254-Outgoing [DECODE] Open: Optional param len 30
BGP: 100.64.2.254-Outgoing [DECODE] Open Opt: Option Type 2, Option Len 6
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: Cap Code 1, Cap Len 4
BGP: 100.64.2.254-Outgoing [DECODE] Open Opt: Option Type 2, Option Len 2
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: Cap Code 128, Cap Len 0
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: RR Cap(old) for all address-families
BGP: 100.64.2.254-Outgoing [DECODE] Open Opt: Option Type 2, Option Len 2
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: Cap Code 2, Cap Len 0
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: RR Cap(new) for all address-families
BGP: 100.64.2.254-Outgoing [DECODE] Open Opt: Option Type 2, Option Len 6
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: Cap Code 65, Cap Len 4
BGP: 100.64.2.254-Outgoing [DECODE] Open Opt: Option Type 2, Option Len 4
BGP: 100.64.2.254-Outgoing [DECODE] Open Cap: Cap Code 64, Cap Len 2
BGP: 100.64.2.254-Outgoing [DECODE] Cap GR: Restart Flag Off, Restart Time 120
BGP: 100.64.2.254-Outgoing [FSM] State: OpenSent Event: 19
BGP: 100.64.2.254-Outgoing [ENCODE] Msg-Hdr: Type 4
BGP: 100.64.2.254-Outgoing [ENCODE] Keepalive: 294 KAlive msg(s) sent
...

```

BGP state
messages

FORTINET

© Fortinet Inc. All Rights Reserved.

31

The next two slides show examples of real-time debug outputs from the successful establishment of a BGP session. In this example, the output shows when the session goes to the OpenSent state.

DO NOT REPRINT
© FORTINET

BGP Neighbors

```

...
BGP: 100.64.2.254-Outgoing [DECODE] Msg-Hdr: type 4, length 19
BGP: 100.64.2.254-Outgoing [DECODE] KAlive: Received!
BGP: 100.64.2.254-Outgoing [DECODE] Msg-Hdr: type 4, length 19
BGP: 100.64.2.254-Outgoing [DECODE] KAlive: Received!
BGP: 100.64.2.254-Outgoing [FSM] State: OpenConfirm Event: 26
BGP: 100.64.2.254-Outgoing [FSM] State: Established Event: 26
id=20300 logdesc="BGP neighbor status changed" msg="BGP: %BGP-5-ADJCHANGED: VRF 0 neighbor
100.64.2.254 Up "
BGP: 100.64.2.254-Outgoing [FSM] State: Established Event: 34
BGP: 100.64.2.254-Outgoing [DECODE] Msg-Hdr: type 2, length 65
BGP: 100.64.2.254-Outgoing [DECODE] Update: Starting UPDATE decoding... Bytes To Read (46),
msg_size (46)
BGP: 100.64.2.254-Outgoing [DECODE] Update: NLRI Len(6)
BGP: 100.64.2.254-Outgoing [FSM] State: Established Event: 27
BGP: 100.64.2.254-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0
BGP: BGP VRF 0 leaking 0.0.0.0/0 all 1, saf1 1
BGP: VRF 0 NSM announce: 0.0.0.0/0
BGP: 100.64.2.254-Outgoing [RIB] Update: Prefix 8.8.8.8/32 denied due to filter

```

BGP state messages

Prefixes received from peer

FORTINET

© Fortinet Inc. All Rights Reserved.

32

This slide shows the real-time debug output containing the OpenConfirm after the keepalive is received from the neighbor, as well as the establishing of the connection. The output also lists the prefixes FortiGate received after the BGP session is established.

DO NOT REPRINT
© FORTINET

BGP Neighbors

```
# execute router clear bgp
all          Clear all BGP peers.
as           Clear BGP peer by AS number.
dampening    Clear route flap dampening information.
external     Clear all external peers.
flap-statistics Clear route flap statistics.
ip           Clear BGP peer by IP address.
ipv6         Clear BGP peer by IPv6 address.
```

```
# execute router clear bgp all
<args...>   Input arguments:
<none>
in
in prefix-filter
out
```

Resets the BGP process
FortiGate will need to
establish BGP peering
again

```
soft [in|out]
```

Resends
complete BGP
table

FORTINET

© Fortinet Inc. All Rights Reserved.

33

The command shown on this slide is used to restart a BGP session between two peers. You can also use this command to run a BGP soft reset, which forces both peers to exchange their complete BGP routing tables.

DO NOT REPRINT
© FORTINET

BGP Event Logging

- BGP event logging displays routing events:
 - Neighbor down or up
 - RIB update
 - BGP message exchange
 - Errors connecting to neighbors
- Enabled by default

```
# config router bgp
  set log-neighbour-change enabled
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

34

Now FortiGate can log routing events, which enables you to get information that used to be available only when you ran the BGP real-time debug. By default, BGP event logging is enabled. You can disable BGP event logging by using the command shown on this slide.

DO NOT REPRINT
© FORTINET

BGP Event Logging (Contd)

Log & Report > Router Events			
Date/Time	Level	Message	Log Details
2020/05/04 17:40:39	Information	BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 100.64.2.254 E	<div>Router Events</div> <div>Details</div> <div>General</div> <div>Date</div> <div>Time</div> <div>Virtual Domain</div> <div>Log Description</div> <div>Data</div> <div>Message</div> <div>Security</div> <div>Level</div> <div>Other</div> <div>Log ID</div> <div>Type</div> <div>Sub Type</div> <div>Log event original timestamp</div> <div>Timezone</div>
2020/05/04 17:40:39	Information	BGP: VRF 0 NSM withdraw: 0.0.0.0/0	
2020/05/04 17:40:39	Information	BGP: BGP VRF 0 leaking 0.0.0.0/0 afi 1, safi 1	
2020/05/04 17:40:39	Information	BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 100.64.2.254 E	
2020/05/04 17:40:39	Information	BGP: %BGP-3-NOTIFICATION: sending to 100.64.2.254 6/0	
2020/05/04 17:40:39	Information	BGP: 100.64.2.254-Outgoing [ENCODE] Msg-Hdr: Type 3	
2020/05/04 17:40:39	Information	BGP: 100.64.2.254-Outgoing [FSM] State: Established Event	
2020/05/04 17:40:39	Information	BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 100.64.1.254 E	
2020/05/04 17:40:39	Information	BGP: VRF 0 NSM announce: 0.0.0.0/0	
2020/05/04 17:40:39	Information	BGP: BGP VRF 0 leaking 0.0.0.0/0 afi 1, safi 1	
2020/05/04 17:40:39	Information	BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 100.64.1.254 E	
2020/05/04 17:40:39	Information	BGP: %BGP-3-NOTIFICATION: sending to 100.64.1.254 6/0	
2020/05/04 17:40:39	Information	BGP: 100.64.1.254-Outgoing [ENCODE] Msg-Hdr: Type 3	
2020/05/04 17:40:39	Information	BGP: 100.64.1.254-Outgoing [FSM] State: Established Event	
2020/05/04 15:05:53	Information	OSPF: %OSPF-5-ADJCHANGE: neighbor port3:10.1.0.254-0	
			<div>General</div> <div>Date</div> <div>Time</div> <div>Virtual Domain</div> <div>Log Description</div> <div>Data</div> <div>Message</div> <div>Security</div> <div>Level</div> <div>Other</div> <div>Log ID</div> <div>Type</div> <div>Sub Type</div> <div>Log event original timestamp</div> <div>Timezone</div>

FORTINET

© Fortinet Inc. All Rights Reserved.

35

You can view BGP-related router events on the GUI. You can click any logged entry to view the details.

DO NOT REPRINT
© FORTINET

BGP Troubleshooting Tips

- Is there an active route to the remote peer?
- Check the status of the TCP session
- Check the status of the BGP session
- Check the prefixes received and advertised

FORTINET

© Fortinet Inc. All Rights Reserved.

36

Follow these steps to troubleshoot a BGP problem between two peers:

- Check that the local router can reach the remote peer
- Check the TCP session
- Check the BGP session
- If the BGP session is established, check the prefixes received and advertised by each peer

DO NOT REPRINT
© FORTINET

Review

- ✓ Review BGP and its components
- ✓ Understand autonomous system
- ✓ Learn about route reflectors
- ✓ Explore routing information bases
- ✓ Explore BGP attributes
- ✓ Explore BGP route selection
- ✓ Explore BGP router event logs
- ✓ Explore BGP troubleshooting

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

DO NOT REPRINT
© FORTINET

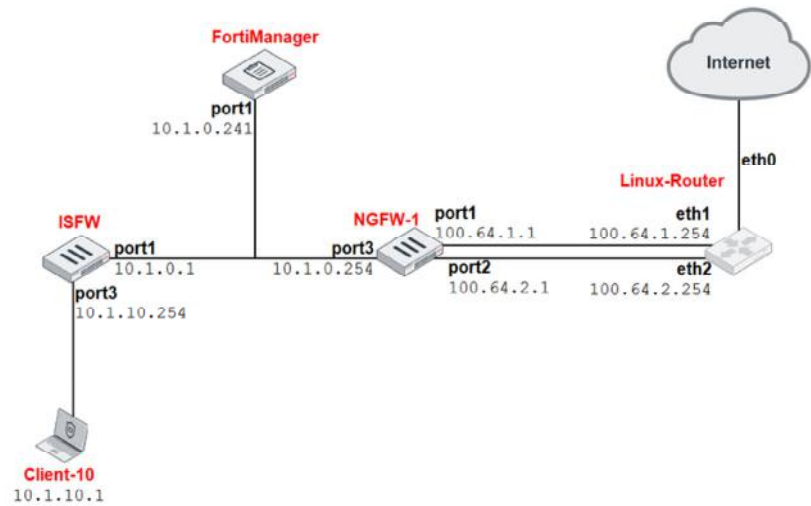
Lab 9—BGP

Now you will work on *Lab 9—BGP*.

DO NOT REPRINT
© FORTINET

Lab 9—BGP

- BGP dual home configuration:
 - port1 is the primary link
- Troubleshooting:
 - BGP neighbor is not coming up
 - Traffic to 8.8.8.8 is taking port2 instead of port1
- Prefix list



FORTINET

© Fortinet Inc. All Rights Reserved.

39

In this lab, you will configure BGP routing between the next generation firewall one (NGFW-1) and the Linux-Router. You will also use the BGP real-time debug to troubleshoot BGP issues.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about web filtering.

DO NOT REPRINT
© FORTINET

Objectives

- Test a web filter configuration
- Inspect HTTPS traffic using different SSL inspection methods
- Check web filtering statistics
- Troubleshoot common web filtering issues

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

By demonstrating competence in web filtering, you will be able to implement, maintain, and troubleshoot web filtering on FortiGate.

DO NOT REPRINT
© FORTINET

Web Filtering Review

- FortiGate queries FortiGuard to get the URL category
 - Caches the FortiGuard answer
 - Cache TTL value is configurable

```
#config system fortiguard
webfilter-cache      : enable
webfilter-cache-ttl  : 3600
...
```
- Supports proxy and flow inspection modes

FORTINET

© Fortinet Inc. All Rights Reserved.

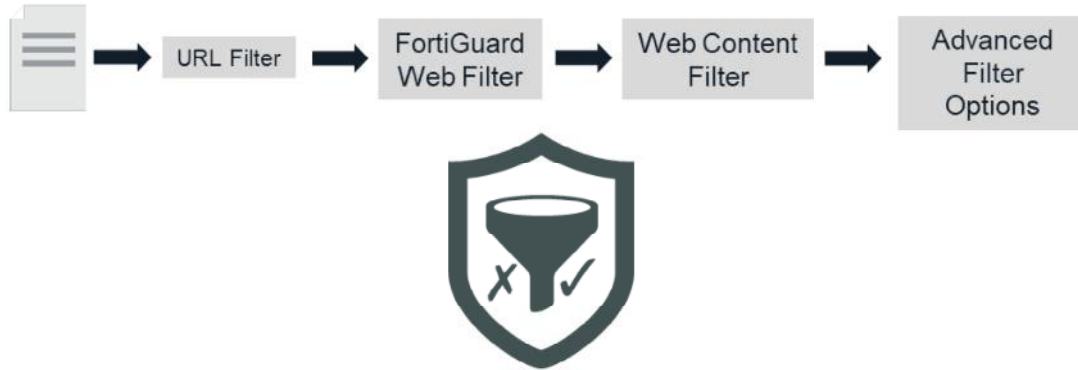
3

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

DO NOT REPRINT
© FORTINET

Order of Inspection

- Web filtering inspection is performed in the following order:



FORTINET

© Fortinet Inc. All Rights Reserved.

4

During web filtering inspection, FortiGate first checks the static URL filter list, then the FortiGuard categories, and then the content filtering list. Finally, FortiGate can execute some advanced options, such as manipulation of HTTP headers.

DO NOT REPRINT
© FORTINET

SSL Inspection

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

Security Profiles > SSL/SSH Inspection

New SSL/SSH Inspection Profile

Name: ProtectCltets
Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers
Protecting SSL Server

Inspection method: SSL Certificate Inspection
Full SSL Inspection

CA certificate: Fortinet_CA_SSL

Blacklisted certificates: Allow Block View Blacklisted Certificates

Untrusted SSL certificates: Allow Block Ignore View Trusted CAs List

Decrypt outbound traffic

FORTINET

© Fortinet Inc. All Rights Reserved.

5

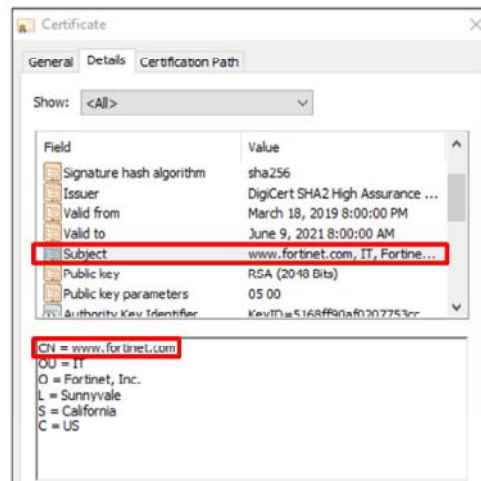
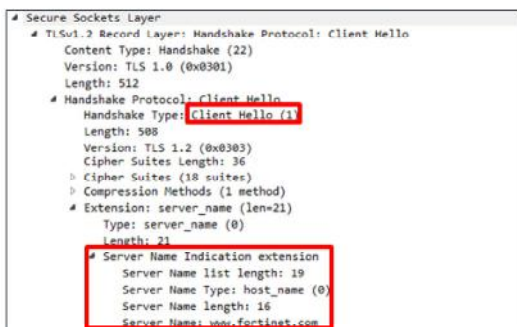
With encrypted traffic making up between 60% to 80% of most organization's traffic, it has become critical that encrypted traffic is inspected in order to maintain a secure network. In the context of web filtering, FortiGate has two methods of inspecting outbound encrypted sessions—SSL certificate inspection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

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

DO NOT REPRINT
© FORTINET

SSL Certificate Inspection

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



FORTINET

© Fortinet Inc. All Rights Reserved.

6

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

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

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

DO NOT REPRINT
© FORTINET

SSL Certificate Inspection and SNI Check

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

7

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

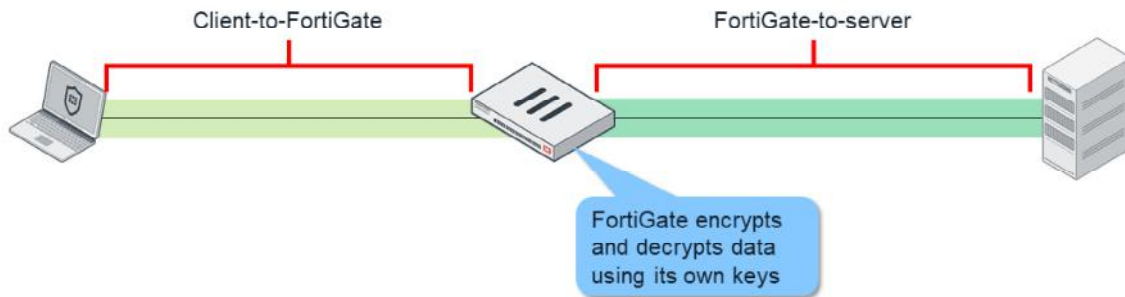
You can configure FortiGate to be more strict, so it closes the client connection if the domain in the **SNI** field does not match any of the domains listed in the **CN** and **SAN** fields.

You can also configure FortiGate to disable SNI checking altogether, so that FortiGate always uses the **SNI** information to obtain the FQDN to rate the site.

DO NOT REPRINT
© FORTINET

Full SSL Inspection

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



FORTINET

© Fortinet Inc. All Rights Reserved.

8

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

DO NOT REPRINT
© FORTINET

Category Lookup

- To verify which category a specific website belongs to:

- <http://fortiguard.com/webfilter>
- You can submit a request for URL reclassification



Type in the URL/IP
in the search box to
check the category

Can check URL
category based on
FortiOS version

FORTINET

© Fortinet Inc. All Rights Reserved.

9

You can access the FortiGuard portal to check which category a URL belongs to. In the portal, you can also request that a URL be reclassified.

You can also view the FortiGuard web filter categories.

DO NOT REPRINT
© FORTINET

Web Filtering Categories

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

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

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

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

FORTINET

© Fortinet Inc. All Rights Reserved.

10

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

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

DO NOT REPRINT
© FORTINET

Category Access Test

- You can test whether a specific category or subcategory is allowed or blocked:

- <http://wfurltest.fortiguard.com/wfurltest/wfurltest/<wf category id here>.html>

Using category number

- <https://fortiguard.com/webfilter/categories>

Test http

Test https



Adult / Mature Content		
Category	Description	Tests
Abortion	Websites pertaining to abortion data, information, legal issues, and organizations.	Web Filter Full SSL Inspection SSL Certificate Inspection
Advertising	This category caters to organizations that campaign or lobby for a cause by building public awareness, raising support, influencing public policy, etc.	Web Filter Full SSL Inspection SSL Certificate Inspection
Alcohol	Websites which legally promote or sell alcohol products and accessories.	Web Filter Full SSL Inspection SSL Certificate Inspection

FORTINET

© Fortinet Inc. All Rights Reserved.

11

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

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

DO NOT REPRINT
© FORTINET

Session Flags and Inspection Mode

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

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

DO NOT REPRINT
© FORTINET

Web Filtering Statistics

```
# diagnose webfilter fortiguard statistics list
```

Rating Statistics:

=====

DNS failures	:	0
DNS lookups	:	0
Data send failures	:	0
Data read failures	:	0
Wrong package type	:	0
Hash table miss	:	0
Unknown server	:	0
Incorrect CRC	:	0
Proxy request failures	:	0
Request timeout	:	3
Total requests	:	32
Requests to FortiGuard servers	:	32
Server errored responses	:	0
Relayed rating	:	0
Invalid profile	:	0
...		

FORTINET

© Fortinet Inc. All Rights Reserved.

13

Use the following CLI command to list error counters and other statistics related to web filtering: `diagnose webfilter fortiguard statistics list`. A continual increase in some of the error counters usually indicates communication problems with FortiGuard.

DO NOT REPRINT
© FORTINET

Web Filtering Statistics

...

Allowed	:	49
Blocked	:	2
Logged	:	2
Blocked Errors	:	0
Allowed Errors	:	0
Monitors	:	0
Authenticates	:	0
Warnings:	:	0
Ovrd request timeout	:	0
Ovrd send failures	:	0
Ovrd read failures	:	0
Ovrd errored responses	:	0

FORTINET

© Fortinet Inc. All Rights Reserved.

14

The output also shows counters for the number of sites that were allowed, blocked, logged, monitored, and so on.

DO NOT REPRINT
© FORTINET

Web Filtering Statistics

Cache Statistics:

```

=====
Maximum memory      : 20885504
Memory usage        : 184320
Nodes               : 15
  Leaves            : 9
  Prefix nodes      : 4
  Exact nodes       : 5
Requests            : 83
Misses              : 64
Hits                : 19
  Prefix hits       : 18
  Exact hits        : 1
No cache directives : 0
Add after prefix    : 0
Invalid DB put      : 0
DB updates          : 1
Percent full        : 1%
  Branches          : 40%
  Leaves            : 60%
    Prefix nodes    : 44%
    Exact nodes     : 56%
Miss rate           : 77%
Hit rate            : 23%
  Prefix hits       : 95%
  Exact hits        : 5%
  
```

Note: All counters display zero if web filtering cache is disabled in config system fortiguard settings

FORTINET

© Fortinet Inc. All Rights Reserved.

15

Use the same command to display counters for the web filtering cache, including memory, requests, and hits and misses.

DO NOT REPRINT
© FORTINET

Web Filtering Test Command

```
# diagnose test application urlfilter 1
1.   This menu
2.   Clear WF cache
7.   Toggle switch for dumping unrated packet
10.  Print debug values
11.  Clear Spam Filter cache
12.  Clear AV Query cache
13.  Toggle switch for dumping expired license packets
14.  Show running timers (except request timers)
144. Show running timers (including request timers)
15.  Send INIT requests.
19.  Display object counts
20.  Display FTGD TCP stats
200. Display FTGD SSL stats
201. Display FTGD fnbam stats
21.  Display FTGD quota list
22.  Reset all user quotas
23.  Display which hardware/software SSL is using
98.  Toggle hardware/software SSL and restart daemon
99.  Restart the urlfilter daemon.
```

FORTINET

© Fortinet Inc. All Rights Reserved.

16

Use the `diagnose test application urlfilter 1` command to display all options available for the web filtering test command. You can use this command to troubleshoot issues related to web filtering.

DO NOT REPRINT
© FORTINET

FortiGuard Web Filtering Cache

```
# diagnose webfilter fortiguard cache dump

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

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

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

FortiGuard category for the domain in hexadecimal

34 Hex = 52 decimal

FortiGuard category for the IP address in hexadecimal

FORTINET

© Fortinet Inc. All Rights Reserved.

17

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

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

DO NOT REPRINT
© FORTINET

FortiGuard Web Filtering Real-Time Debug

```
# diagnose debug urlfilter src-addr <source_IP>
# diagnose debug application urlfilter -1
# diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url=/"

action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url=/"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

18

Another tool you can use to troubleshoot web filtering is the web filter real-time debug. You can use the commands shown on this slide.

This slide shows an example output of the real-time debug when the URL to categorize isn't in the FortiGuard cache. The output shows the URL, category, source, destination IP addresses, and service.

IPS, and WAD will only send request to urlfilter daemon when cache is missed. Once the URL is in the FortiGuard cache, IPS Engine/WAD will start looking up the cache themselves before sending requests to urlfilter.

DO NOT REPRINT
© FORTINET

Web Filtering Troubleshooting Tips

- Get specifics:
 - What URLs?
 - Is it random or consistent?
 - Who is affected? All users or specific users?
- Is there anything in any of the logs?
 - Was something blocked intentionally?
- Is authentication involved?
 - Double check that the user is being handled properly
- Attempt reproduction:
 - You can reproduce most web filtering issues using the same settings
 - Run the real-time debug commands while reproducing the problem

FORTINET

© Fortinet Inc. All Rights Reserved.

19

Tips for troubleshooting web filtering:

- Get the specifics first:
 - What URLs are having the problem?
 - Is it random?
 - Does it happen with all the users?
- Check the logs
- Is the problem caused by an incorrect user group configuration? Are the user access privileges correct?
- Run the real-time debug while reproducing the issue

DO NOT REPRINT
© FORTINET

Web Filtering Troubleshooting Tips (Contd)

- Ensure web filtering isn't globally disabled:

```
# get system fortiguard
...
webfilter-force-off : disable
webfilter-cache      : enable
webfilter-cache-ttl  : 3600
webfilter-license    : Contract
webfilter-expiration: Wed Nov  9 2022
```

disable (default): enable web-filter globally
enable: disable web-filter globally

- Connectivity problems to FortiGuard and conserve mode can cause web filtering intermittent issues

FORTINET

© Fortinet Inc. All Rights Reserved.

20

Additional tips:

- Check that web filtering isn't disabled globally.
- If users are having intermittent issues, check that the communication with FortiGuard is stable (check the web filtering statistics). Check also that the device is not entering conserve mode.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand order of inspection
- ✓ Configure HTTPS inspection
- ✓ Test web filtering
- ✓ Examine web filtering statistics
- ✓ Troubleshoot web filtering problems

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

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

DO NOT REPRINT
© FORTINET

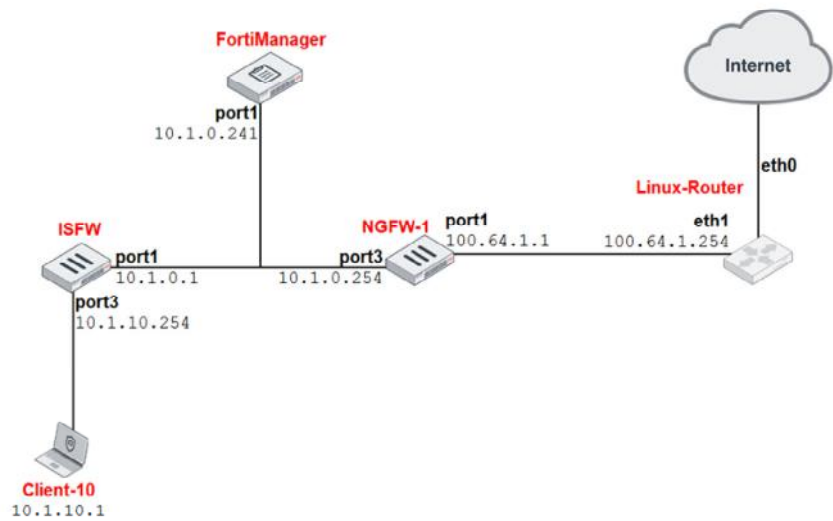
Lab 10—Web Filtering and Antivirus

Now, you will work on *Lab 9—Web Filtering and Antivirus*.

DO NOT REPRINT
© FORTINET

Lab 10—Web Filtering and Antivirus

- On ISFW:
 - Create web filter profile
 - Create antivirus profile
 - Create firewall policy
- Troubleshooting:
 - Web filtering problem
 - Antivirus problem



FORTINET

© Fortinet Inc. All Rights Reserved.

23

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

DO NOT REPRINT
© FORTINET



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

DO NOT REPRINT
© FORTINET

Objectives

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

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

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

DO NOT REPRINT
© FORTINET

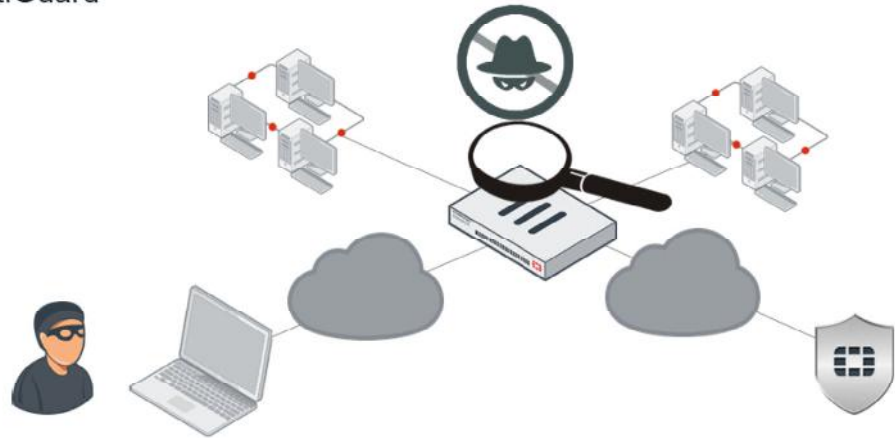
IPS Deployment and Tuning

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

DO NOT REPRINT
© FORTINET

IPS Review

- Detects and blocks:
 - Known exploits that match signatures
 - Network errors and protocol anomalies
- Updated through FortiGuard
- Flow-based only



FORTINET

© Fortinet Inc. All Rights Reserved.

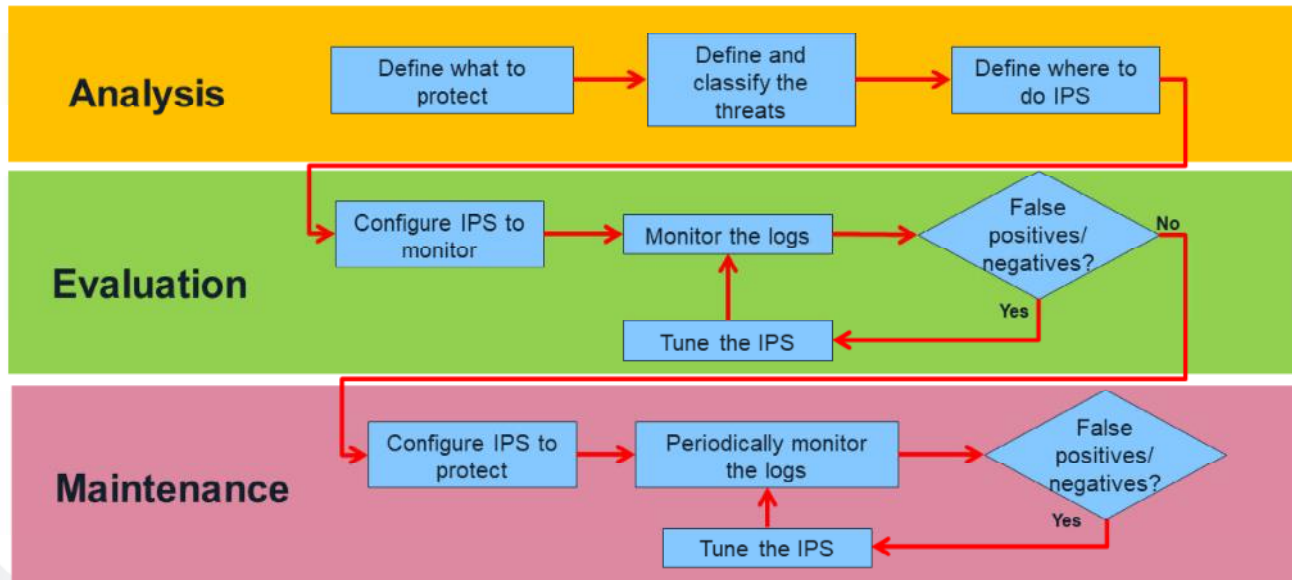
4

IPS uses signature databases to detect known attacks. You can also use IPS signatures to detect network errors and anomalies.

Like the antivirus signature databases, the IPS signature databases are also updated through FortiGuard.

DO NOT REPRINT
© FORTINET

Steps for Deploying IPS



FORTINET

© Fortinet Inc. All Rights Reserved.

5

There is no single correct way to deploy an IPS solution. It depends greatly on the network and application requirements. However, in most cases, you will follow the steps shown on this slide.

There are usually three stages in the deployment of an IPS solution:

- **Analysis:** The administrator defines what to protect and where.
- **Evaluation:** After an initial IPS configuration, the administrator makes further adjustments based on the IPS logs. During this stage, you configure the IPS only to monitor traffic, not block it.
- **Maintenance:** After the IPS configuration is working correctly, the administrator sets IPS to protect. The administrator must continue to monitor the logs, and make further adjustments if any false positives or negatives occur.

You will learn more about each stage in this lesson.

DO NOT REPRINT
© FORTINET

Identify What to Protect

- Don't set unrealistic expectations about protecting everything from the beginning
- Set priorities:
 - Start with the most business-critical services
- After you know the services to protect, you can define the threats and where to implement IPS:
 - Understand your deployment requirements
 - Classify the threats into groups

FORTINET

© Fortinet Inc. All Rights Reserved.

6

During the analysis stage, you must identify:

- What services to protect
- The threats to those services
- Where to enable IPS inspection

Set realistic expectations. Focus on protecting the services that need protection. Start with the most critical services, and classify the threats into groups.

DO NOT REPRINT
© FORTINET

Configure IPS to Monitor

- One approach is to enable just one group of signatures at a time:
 - Start with the signatures that have more priority
 - Analyze the logs and either tune the IPS or enable another group
- Repeat until it's clear that the IPS is correctly tuned:
 - Monitor the network for one to two weeks
- You will learn about your network during this process!

FORTINET

© Fortinet Inc. All Rights Reserved.

7

During the evaluation stage, enable just one group of signatures at a time, starting with the more critical ones. Wait and analyze the logs. If the logs indicate any problems, fine tune the IPS configuration. After you feel comfortable with one signature group, enable IPS protection for the next group. This process can take from one to two weeks.

DO NOT REPRINT
© FORTINET

Configure the IPS to Protect

- Make the list of signatures that you set to block small and precise:
 - Minimizes false positives
 - Include the attacks that are most dangerous to critical services
- Continue to monitor IPS events:
 - IPS implementations are not *configure once and forget*
 - Tuning is an ongoing process

FORTINET

© Fortinet Inc. All Rights Reserved.

8

To minimize the number of false positives, make the list of signatures that you set to block small and precise. The list should include the attacks that are most dangerous to critical services.

After you deploy the IPS solution, you must continue to monitor IPS events.

DO NOT REPRINT
© FORTINET

IPS Tuning

- Check the events that:
 - Have been generated most
 - Have high priority
- Analyze the event:
 - Who is that source IP address?
 - Who is that destination IP address?
 - What is the service being attacked?
 - What type of attack is it?

FORTINET

© Fortinet Inc. All Rights Reserved.

9

When you check IPS events, start with the events that have been generated the most, or have high priority.

For each event type, analyze the IP addresses, services, and type of attack. The analysis should help you identify whether the event is a genuine attack or a false positive.

DO NOT REPRINT
© FORTINET

IPS Tuning

- Eliminate as many false positives as possible
- For each false positive, do one of the following to fix the problem:
 - Make changes to the source or destination
 - Create exemptions
 - Adjust the thresholds (for the case of rate-based signatures)

Security Profiles > Intrusion Prevention

Add Signatures

Type: Filter **Signature**

Action: **Default**

Packet logging: **Enable** **Disable**

Status: **Enable** **Disable** **Default**

Rate-based settings: **Default** Specify

Exempt IPs: 0 **Edit IP Exemptions**

Remove Selected Search Selected All

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1					
A325.Botnet	*****	Server	All	Block	

Edit IP Exemptions

+ Create New Delete

Source IP/Netmask	Destination IP/Netmask
10.1.4.10/32	0.0.0.0/0

FORTINET

© Fortinet Inc. All Rights Reserved.

10

Eliminate as many false positives as possible. For each false positive, try to fix the problem by making changes in either the source or destination of the traffic first. You can also use IPS exemptions.

DO NOT REPRINT
© FORTINET

Advanced IPS Configuration

In this section, you will learn about advanced IPS configuration settings.

DO NOT REPRINT
© FORTINET

Global IPS Configuration

- Affects IPS engine operations for the whole FortiGate device
- The default values work well in most cases
- The most commonly used options are:

```
# config ips global
    set fail-open {enable | disable}
    set intelligent-mode {enable | disable}
    set socket-size <ips_buffer_size>
    set traffic-submit {enable | disable}
    ...
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

12

The global IPS configuration settings affect the IPS engine operations for the whole FortiGate device. Most of the time, you don't need to modify these values because the default ones work well in most scenarios. However, under certain circumstances, changes to these settings may be beneficial.

DO NOT REPRINT
© FORTINET

IPS Intelligent Mode

```
set intelligent-mode {enable | disable}
```

- Controls the IPS engine's adaptive scanning behavior:
 - `enabled` (default)
 - Using heuristics, IPS engine determines when it is secure enough to stop scanning session traffic
 - It's a balanced method that covers all known exploits
 - `disable`
 - IPS engine scans every byte in every session



© Fortinet Inc. All Rights Reserved.

13

The `intelligent-mode` command controls the adaptive scanning behavior of the IPS.

When you enable adaptive scanning, IPS determines when it is secure enough to stop scanning the traffic in each session. When disabled, IPS scans every byte in every session.

DO NOT REPRINT
© FORTINET

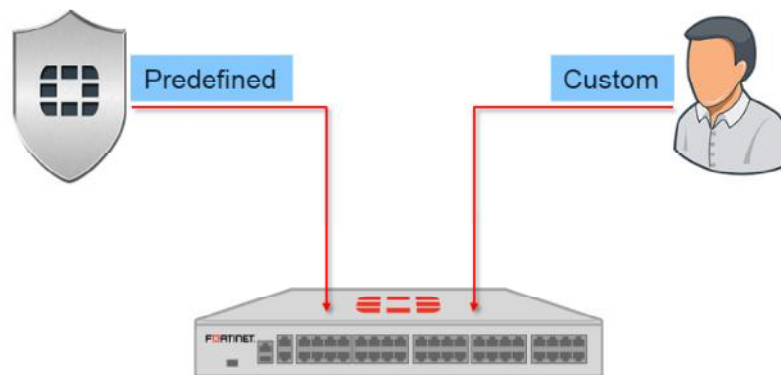
Custom Signatures

In this section, you will learn how to create custom signatures.

DO NOT REPRINT
© FORTINET

Types of IPS signatures

- There are two categories of Fortinet IPS signatures:
 - Predefined signatures are developed by FortiGuard analysts, which are distributed as a part of regular FortiGuard update packages
 - Custom signatures are created by users for specialized applications



© Fortinet Inc. All Rights Reserved.

15

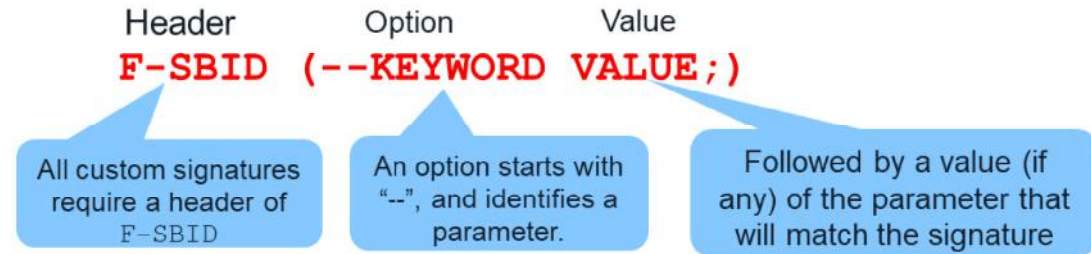
There are two categories of Fortinet IPS signatures:

- Predefined signatures are developed by FortiGuard analysts, which are distributed as a part of regular FortiGuard update packages
- Custom signatures are created by users for specialized applications

DO NOT REPRINT
© FORTINET

Syntax

- A custom signature is made up of a type header and a series of option and value pairs



- You must enclose the string of option and value pairs in parentheses
- Keywords are case insensitive
- Values are case sensitive

FORTINET

© Fortinet Inc. All Rights Reserved.

16

A custom signature is made up of a type header, and a series of option and value pairs.

All custom signatures require a header of F-SBID. An option starts with "--", followed by the option name, and, sometimes, a value. Some options don't require a value.

You must enclose the string of option and value pairs in parentheses. Also, keywords are case insensitive and values are case sensitive.

DO NOT REPRINT
© FORTINET

Syntax

- You can include multiple options in the rule by separating the options with a semicolon followed by a space

**F-SBID(--KEYWORD1 VALUE1; --KEYWORD2
VALUE2; --KEYWORDn VALUEn)**

- The maximum length for user-created rules is 1024 bytes

You can include multiple options in the rule by separating them with a semicolon. The maximum length is 1024 bytes for custom signatures and 4096 bytes for predefined signatures.

DO NOT REPRINT
© FORTINET

Option Types

`F-SBID (--KEYWORD VALUE ;)`

- The options used in the IPS signatures are divided into four categories based on their purpose
- There are many different options available within these categories
- You can reference a complete list of options in the *Custom IPS and Application Control Signature Syntax Guide*

Now you'll learn about supported option types. The options are divided into four categories based on their purpose.

DO NOT REPRINT
© FORTINET

Required Options

`F-SBID (--KEYWORD VALUE ;)`

- All signatures must include:
 - `--name`: Signature name that is displayed in the GUI and the CLI
 - `--service`: It specifies the session type associated with a packet
 - `--flow`: It specifies the direction of the detection packet

- Example:

```
F-SBID(--name "Block.HTTP.POST"; --protocol tcp; --service HTTP;
--flow from_client; --pattern "POST"; --context uri; --within
5,context; )
```

FORTINET

© Fortinet Inc. All Rights Reserved.

19

When creating a custom signature, you must define required options which are name, service, and flow.

The signature name must be unique for each custom signature. The maximum length of a signature name is 64 characters.

The service option specifies the session type, such as HTTP, FTP. *You can only use the service keyword once in a signature.* If a signature has neither a *service* keyword nor a *port* keyword, it will be added to all service trees including the *unknown_service* tree.

Similar to service option, the flow option can appear only once in the signature because it defines flow direction of the detection packet.

DO NOT REPRINT
© FORTINET

Protocol Options

`F-SBID (--KEYWORD VALUE ;)`

- Protocol-related options:
 - Used to match different protocol headers
- Example:

```
F-SBID(--name "Block.HTTP.POST"; --protocol tcp; --service HTTP;  
--flow from_client; --pattern "POST"; --context uri; --within  
5,context; )
```



© Fortinet Inc. All Rights Reserved.

20

Use protocol-related options to match protocol headers.

DO NOT REPRINT
© FORTINET

Payload Options

`F-SBID (--KEYWORD VALUE ;)`

- Payload-related options:
 - Used to match the packet payload
- Example:

```
F-SBID(--name "Block.HTTP.POST"; --protocol tcp; --service HTTP;  
--flow from_client; --pattern "POST"; --context uri; --within  
5,context; )
```

FORTINET

© Fortinet Inc. All Rights Reserved.

21

Use payload-related options to match portions of the packet payload.

DO NOT REPRINT
© FORTINET

Special Options

`F-SBID (--KEYWORD VALUE ;)`

- Special options:
 - Used for all other purposes
- Example:

```
F-SBID( --name "Ultraviewer.Custom"; --protocol tcp; --service  
ssl; --flow from_client; --pattern "ultraviewer"; --context  
host; --app_cat 7;)
```

Use special options for various purposes for more granular filtering.

In this example, specifying application category will result in this signature appearing under application control instead of IPS configuration.

DO NOT REPRINT
© FORTINET

Tips for Creating Custom Signatures

- Before creating a custom signature, gather as many samples of the traffic as possible:
 - It will help identify patterns, for example, source ports, destination ports, specific strings in the body, and so on
- Most of the time, the protocol-related patterns are obvious
- Try to identify payload-related patterns in the captures
- Use payload-related and special options to ensure the least number of false positive or negative matches

FORTINET

© Fortinet Inc. All Rights Reserved.

23

If you are planning to create a custom signature, gather as many samples of the traffic as possible. Good samples help you to identify patterns, for example, source ports, destination ports, specific string patterns in the packet payload, and so on.

Try to match payload patterns in addition to protocol patterns, because payload patterns tend to be unique to the specific traffic that you want to match. In this way, you might be able to reduce the number of false positives for the custom signature.

DO NOT REPRINT
© FORTINET

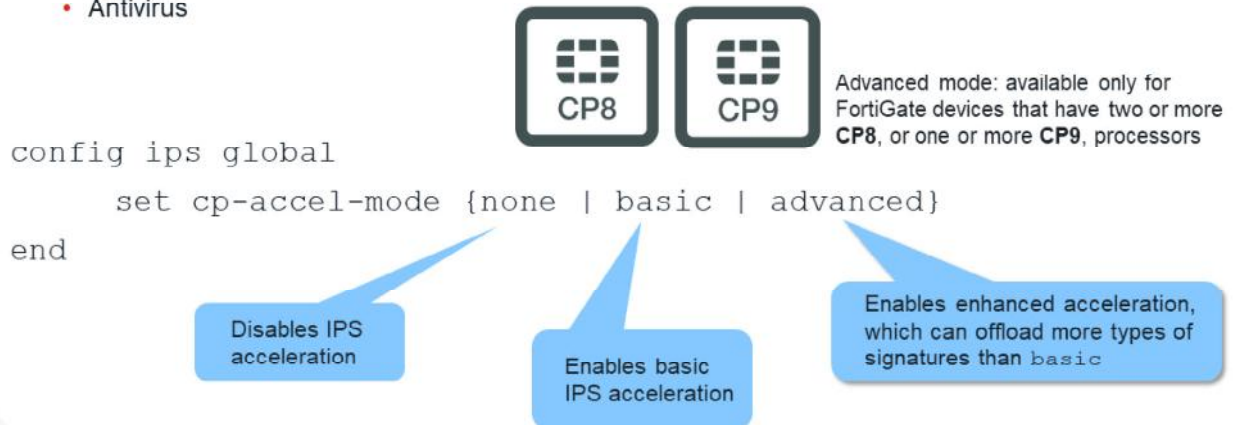
IPS Hardware Acceleration

In this section, you will learn about hardware acceleration options for IPS inspection.

DO NOT REPRINT
© FORTINET

Content Processor and IPS

- CP8 and CP9 provide a fast path for traffic inspected by IPS, including sessions with flow-based inspection
- Content processors (CPs) also accelerate intensive proxy-based tasks:
 - Encryption and decryption (SSL)
 - Antivirus



FORTINET

© Fortinet Inc. All Rights Reserved.

25

The CP is a co-processor for the CPU. It accelerates many common resource-intensive, security-related processes.

Since the very first FortiGate model, Fortinet has included a CP in the design. The CP works at the system level.

CP8 and CP9 provide a fast path for traffic inspected by IPS, including sessions with flow-based inspection.

CP processors also accelerate intensive proxy-based tasks:

- Encryption and decryption (SSL)
- Antivirus

DO NOT REPRINT
© FORTINET

Network Processor and IPS

- Pre-IPS anomaly filtering and logging
- NP6 provides NTurbo:
 - Increases the IPS processing performance by distributing the cost of processing to different CPU cores
 - Fast path for traffic inspected by IPS, including sessions with flow-based inspection
- Network processors (NPs) also offload:
 - Packet transmission
 - Link aggregation
 - IPsec phase 2 and hashing

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

Disables IPS
offloading

Enables IPS
offloading

FORTINET

© Fortinet Inc. All Rights Reserved.

26

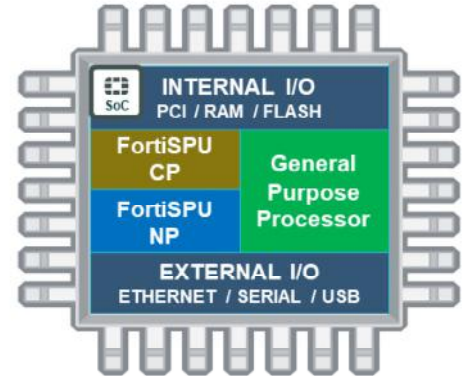
Network processors (NPs) provide the following features:

- Pre-IPS anomaly filtering and logging
- Packet offloading
- Link aggregation
- IPsec encryption and decryption

DO NOT REPRINT
© FORTINET

System on a Chip and IPS

- SPU that includes entire microprocessors, memory blocks, flash memory, and other large building blocks
- Fortinet's system on a chip (SoC) unifies:
 - FortiSPU-NP and FortiSPU-CP
 - General purpose CPU
 - Memories
 - Network interfaces
- SoC4 and SoC3 platforms include NTurbo:
 - Provides a fast path for traffic inspected by IPS



FORTINET

© Fortinet Inc. All Rights Reserved.

27

SoC combines a general-purpose CPU, NPs, and CPs, into a single chip. It accelerates IPS-inspected traffic.

SoC is found in desktop or small office models.

DO NOT REPRINT
© FORTINET

IPS Troubleshooting

In this section, you will learn about IPS troubleshooting.

DO NOT REPRINT
© FORTINET

IPS Engine

- There are two IPS-related daemons:
 - `ipsengine` handles inspection and detection tasks
 - `ipshelper` handles actions whose results can be shared by different daemons, to reduce load

```
# diagnose sys top
Run Time: 5 days, 5 hours and 58 minutes
IU, ON, OS, 99I; OWA, OHI, OST, 1768T, 1044F
  httpd      1313  S    0.3    1.3
  ipsengine  1350  S <  0.0    3.8
  pyfcgid    954   S    0.0    1.5
  ipshelper   71   S <  0.0    1.2
...
```

FORTINET

© Fortinet Inc. All Rights Reserved.

29

There are two important types of daemons that handle IPS-related tasks:

- `ipsengine` is the main type of daemon that handles all inspection and detection tasks
- `ipshelper` handles actions whose results can be shared by different `ipsengine` daemons

In some FortiGate models, it is normal to see multiple instances of the `ipsengine` daemon running.

DO NOT REPRINT
© FORTINET

IPS Fail Open

- Fail open is triggered when one of these two events happen:
 - The IPS socket buffer is full and new packets can't be added for inspection
 - The FortiGate is in conserve mode
- The action the IPS takes depends on the configuration:

```
# config ips global
  set fail-open <enable|disable>
  set database extended
  set traffic-submit disable
  ...
end
```

- enable: new packets might pass through without inspection
- disable: new packets might be dropped

FORTINET

© Fortinet Inc. All Rights Reserved.

30

IPS goes into fail open mode when there is not enough available memory in the IPS socket buffer for new packets. The IPS also goes into fail open mode when the FortiGate is in conserve mode. What happens during that state depends on the IPS configuration. If the `fail-open` setting is enabled, some new packets (depending on the system load) might pass through without being inspected. If it is disabled, new packets might be dropped.

DO NOT REPRINT
© FORTINET

Monitoring IPS Fail Open Events

- IPS fail open event details can be seen in the crash log:

```
# diagnose debug crashlog read
...
7: 2019-06-06 11:44:54 <05688> IPS enter fail open mode: engines=4 socketsize=1048576
8: 2019-09-06 11:44:54 packet_action-drop
...
20: 2019-06-06 11:45:53 <05688> IPS exit fail open mode
```

- The `packet_action` value indicates whether new packets are dropped or passed through
- The crash log also indicates when IPS has exited fail open mode

The IPS fail open event generates a log in the crashlog. The log indicates if new packets are dropped or passed through.

DO NOT REPRINT
© FORTINET

Monitoring IPS Fail Open Events

- IPS fail open entry log

```
date=2019-06-06 time=14:14:29 logid="0100022700" type="event"  
subtype="system" level="critical" vd="root" eventtime=1540790069  
logdesc="IPS session scan paused" action="drop" msg="IPS session scan,  
enter fail open mode"
```

- IPS fail open exit log

```
date=2019-06-06 time=14:18:54 logid="0100022701" type="event"  
subtype="system" level="critical" vd="root" eventtime=1540790334  
logdesc="IPS session scan resumed" msg="IPS session scan resumed,  
exit fail open mode."
```

FORTINET

© Fortinet Inc. All Rights Reserved.

32

IPS fail open entry and exit events also generate event logs.

DO NOT REPRINT
© FORTINET

Frequent IPS Fail Open Events

- Try to identify a pattern:
 - Traffic volume increases?
- Create IPS profiles specifically for the traffic type:
 - Profile to protect Windows servers doesn't need Linux or Solaris signatures
 - Disable IPS on internal to internal policies

FORTINET

© Fortinet Inc. All Rights Reserved.

33

Frequent IPS fail open events usually indicate that the IPS is not able to keep up with the traffic demands. So, try to identify patterns. Has the traffic volume increased recently? Have throughput demands increased?

Tune and optimize your IPS configuration: create IPS profiles specific for the type of traffic being inspected, and disable IPS profiles on policies that don't need them.

DO NOT REPRINT
© FORTINET

IPS and High CPU Use

- Temporary spikes in CPU use are normal:
 - Usually caused by a configuration change
 - `diagnose sys top` will show all `ipsengine` instances spike to 99% temporarily
- Continuous high CPU use by IPS engines might be caused by an infinite loop in packet parsing:
 - Symptom might not affect all of the `ipsengine` instances

FORTINET

© Fortinet Inc. All Rights Reserved.

34

Short spikes in the CPU usage by IPS processes could be caused by firewall policy or profile changes. These spikes are usually normal. Spikes might happen when FortiGate has hundreds of policies and profiles, or many virtual domains. Continuous high CPU usage by the IPS engines is not normal, and you should investigate it.

DO NOT REPRINT
© FORTINET

IPS and High CPU Use

```
# diagnose test application ipsmonitor ?
```

```
1: Display IPS engine information
```

```
2: Toggle IPS engine enable/disable status
```

```
3: Display restart log
```

```
4: Clear restart log
```

```
5: Toggle bypass status
```

```
6: Submit attack characteristics now
```

```
10: IPS queue length
```

```
11: Clear IPS queue length
```

```
12: IPS L7 socket statistics
```

```
13: IPS session list
```

```
14: IPS NTurbo statistics
```

```
15: IPSA statistics
```

```
97: Start all IPS engines
```

```
98: Stop all IPS engines
```

```
99: Restart all IPS engines and monitor
```

Traffic does not go to the IPS

Traffic goes to the IPS, but IPS does not do any inspection

FORTINET

© Fortinet Inc. All Rights Reserved.

35

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 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 particular FortiGate model. If the CPU use remains high after enabling IPS bypass mode, it usually indicates a problem in the IPS engine that you must report to Fortinet's support.

If you enable IPS bypass mode, remember to disable it, after you finish troubleshooting, using option 5.

Another recommendation to keep in mind: if you need to restart the IPS, don't use the `diagnose sys top kill` command. Instead, use option 99, as shown on this slide. This guarantees that all the IPS-related processes will restart properly.

DO NOT REPRINT
© FORTINET

False Positives

- Check that the IPS signature database is up-to-date
- Determine which signature is triggering the false positive
- Use IP exemptions on the signature as a temporary bypass for the affected endpoints
- If all factors are verified (that is, correct policy match, correct IPS profile match), then collect multiple sniffer samples of the traffic
- Provide the sniffer samples and the matching logs to the FortiGuard team for further investigation

support.fortinet.com

Anti Virus Ticket/FortiGuard Service
To submit Anti Virus ticket for your product or report false detection.

Submit Anti Virus Ticket

FortiGuard Service Ticket
To report false detection, uncaught spam or virus, misrated URL, etc. Select this option to contact the FortiGuard Center Threat Research & Response team for assistance.

FORTINET

© Fortinet Inc. All Rights Reserved.

36

If the IPS is generating false positives, first determine which signature is generating them. You can use IP exemptions as a solution. Additionally, you can provide sniffer samples and the matching logs to the FortiGuard team for further investigation.

DO NOT REPRINT
© FORTINET

False Negatives

- False negatives are more difficult to discover
- Verify:
 - Is the IPS signature database up-to-date?
 - Is traffic hitting the correct policy or IPS profile? Use sniffer and debug flow if necessary
 - Is IPS using high CPU and or memory? Is it crashing?
 - Is the signature action correctly set?
- Collect multiple sniffer samples, along with details of the application traffic, and provide them to the Fortinet IPS team for investigation

FORTINET

© Fortinet Inc. All Rights Reserved.

37

False negatives are more difficult to discover and troubleshoot. Check the following:

- Is traffic hitting the correct policy or IPS profile? Use sniffer and debug flow if necessary.
- CPU and memory use is normal
- IPS engines aren't crashing
- IPS configuration is correct

Again, after you verify all of those factors, you can collect sniffer samples and, along with details of the application traffic, provide all the information to the Fortinet IPS team for investigation.

DO NOT REPRINT
© FORTINET

Review

- ✓ Tune IPS configuration
- ✓ Perform advanced IPS configuration
- ✓ Configure custom signatures
- ✓ Configure IPS inspection acceleration
- ✓ Troubleshoot IPS

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

DO NOT REPRINT
© FORTINET

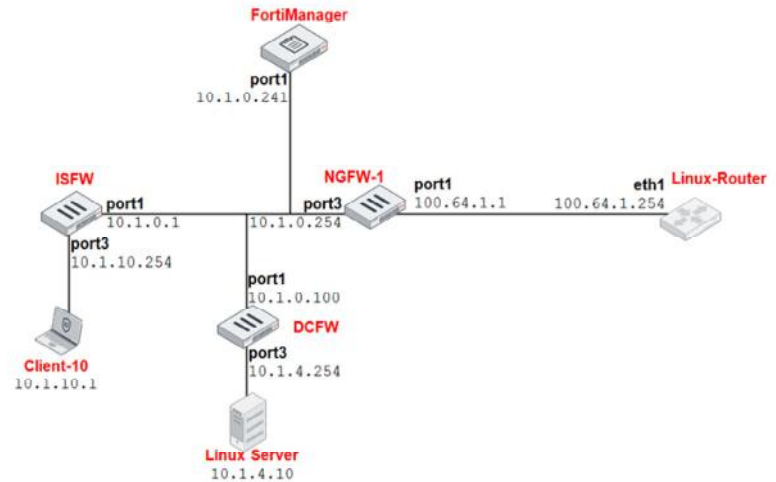
Lab 11—IPS

Now, you will work on *Lab 11—IPS*.

DO NOT REPRINT
© FORTINET

Lab 11—IPS

- IPS configuration:
 - On DCFW:
 - Add an IPS profile
 - Apply the IPS to the inbound firewall policy
 - On NGFW-1:
 - Add a VIP
 - Add an inbound firewall policy
- IPS custom signature



FORTINET

© Fortinet Inc. All Rights Reserved.

40

In this lab, you will configure FortiGate to protect a web server using IPS inspection. Then, you will test the configuration by generating suspicious traffic from outside to the server. Additionally, you will use the information gathered by the built-in sniffer to write a custom IPS signature.

DO NOT REPRINT
© FORTINET



FORTINET
NSE Training Institute

Enterprise Firewall

IPsec

FortiOS 6.4

© Copyright Fortinet Inc. All rights reserved.

Last Modified: 26 June 2020

In this lesson, you will learn about IPsec.

Objectives

- Route IPsec traffic
- Configure remote IPsec sites with overlapping IP subnets
- Troubleshoot the most common IPsec problems
- Check whether IPsec encryption and decryption is offloaded to hardware
- Use the debug flow to isolate IPsec traffic issues
- Capture IPsec traffic
- Monitor the status of an IPsec VPN

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

By demonstrating competence in IPsec, you will be able to configure IPsec using the FortiManager VPN manager, troubleshoot IPsec problems using debug flow, check IPsec encryption and decryption behavior, capture IPsec traffic, and monitor the IPsec VPN status.

DO NOT REPRINT
© FORTINET

IPsec Review

In this section, you will review some IPsec concepts from the *NSE 4* course.

DO NOT REPRINT
© FORTINET

IPsec Review

- Suite of protocols for securing IP communications
- Authenticates and/or encrypts packets:
 - Internet Key Exchange (IKE)
 - Encapsulating Security Payload (ESP)
 - Provides both data integrity and encryption
- For NAT traversal, ESP is UDP-encapsulated

IPsec is a suite of protocols for authenticating and encrypting traffic between two peers. The two most-used protocols in the suite are:

- IKE, which does the handshake, tunnel maintenance, and disconnection
- ESP, which ensures data integrity and encryption

DO NOT REPRINT
© FORTINET

IKE Review

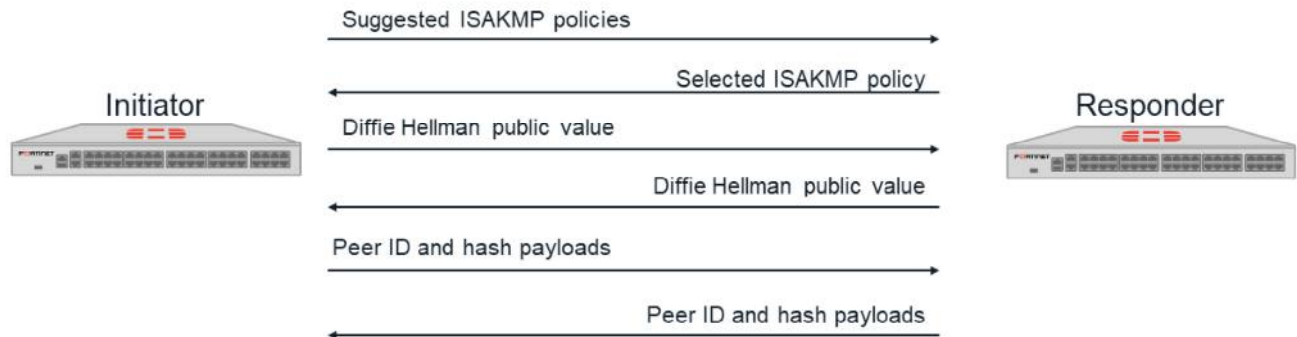
- Negotiates tunnel's private keys, authentication, and encryption
- Allows parties involved in a transaction to set up their security associations (SAs)
 - SAs are the basis for building security functions into IPsec
 - In normal two-way traffic, the exchange is secured by a pair of IKE SAs
- IKE uses two distinct phases:
 - Phase 1: main or aggressive mode
 - Phase 2: quick mode

IKE negotiates the private keys, authentications, and encryption that FortiGate uses to create an IPsec tunnel. Security associations (SAs) provide the basis for building security functions into IPsec. There are two distinct phases that IKE uses: phase 1 uses a single bi-directional SA, and phase 2 uses two IPsec SAs, one for each traffic direction.

DO NOT REPRINT
© FORTINET

Phase 1 Main Mode With Key

- Initiating packet does not yet have a peer ID



FORTINET

© Fortinet Inc. All Rights Reserved.

6

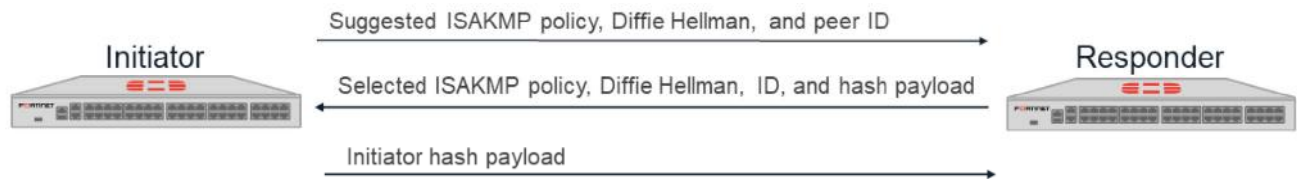
Next, you will review the differences between aggressive mode and main mode. This slide shows main mode, where six packets are exchanged:

1. The client initiates by proposing the security policies.
2. The responder selects which security policy it will agree to use, and replies.
3. The initiator sends its Diffie Hellman public value.
4. The responder replies with its own Diffie Hellman public value.
5. The initiator sends its peer ID and hash payload.
6. The responder replies with its peer ID and hash payload.

DO NOT REPRINT
© FORTINET

Phase 1 Aggressive Mode With Key

- Peer ID is included in the initiating packet and can be used to identify the VPN phase 1 configuration to use



FORTINET

© Fortinet Inc. All Rights Reserved.

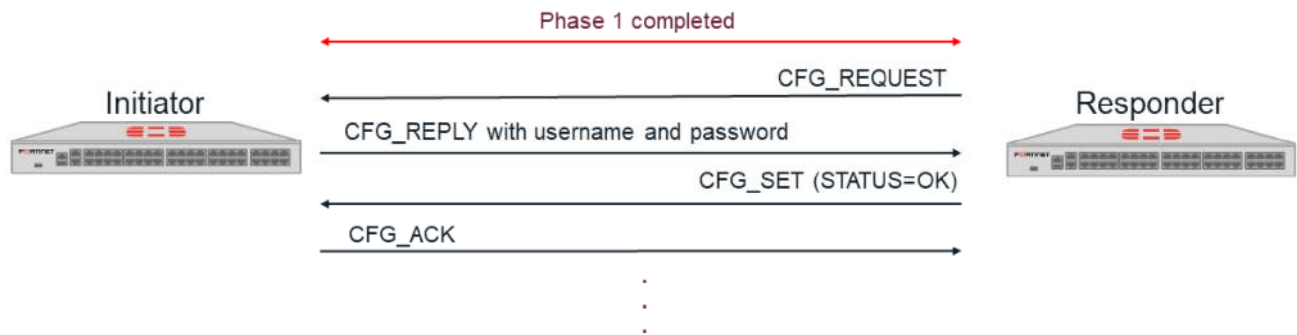
7

In comparison, this slide shows the aggressive mode negotiation in which only three packets are exchanged:

1. The client initiates by suggesting the security policies, and providing its Diffie Hellman public value and peer ID.
2. The responder replies with the same information, plus a hash.
3. The initiator sends its hash payload.

DO NOT REPRINT
© FORTINET

eXtended Authentication (XAuth)



FORTINET

© Fortinet Inc. All Rights Reserved.

8

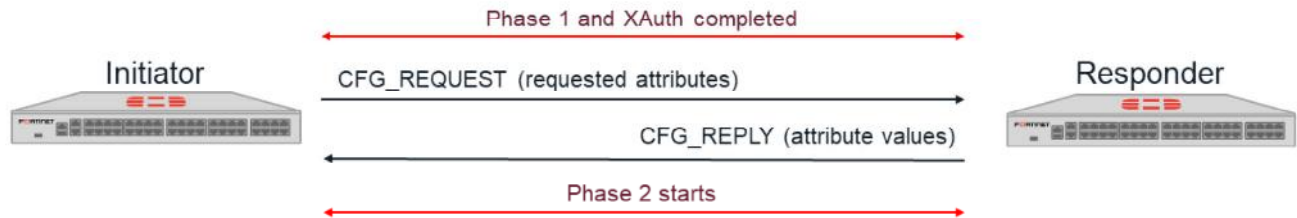
Extended authentication (XAuth) can be used as an additional level of authentication. When XAuth is used, one side must provide credentials (username and password) in order to successfully authenticate.

XAuth happens after the phase 1 is up and before any phase 2 negotiation. That is why XAuth is sometimes referred to as phase 1.5.

In any XAuth communication, there is always one client and one server. The server sends a **CFG_REQUEST** packet, which must be replied by the client with a **CFG_REPLY** packet. The **CFG_REPLY** packet includes the user credentials. If the authentication is ok, the server sends **CFG_SET** and the client replies with **CFG-ACK**.

DO NOT REPRINT
© FORTINET

IKE Mode Configuration



FORTINET

© Fortinet Inc. All Rights Reserved.

9

A FortiGate supports three different methods for automatically configuring the IP settings of IPsec clients: IKE mode configuration, DHCP over IPsec, and L2TP over IPsec.

This slide shows the IKE mode configuration.

After phase 1 is up, and before the phase 2, the client sends a `CFG_REQUEST` message listing the required IP settings (or attributes). The server replies with a `CFG_REPLY`, which contains the assigned values for each of the attributes requested.

Responder Dialup Selection Criteria

- For any incoming connection, FortiGate selects the first VPN (in alphabetical order) that matches the following:
 - Local gateway
 - Mode (aggressive or main)
 - Peer ID (if aggressive)
 - Authentication method (pre-shared key or certificate)
 - Certificate information (if certificate)
 - Proposal
 - DH group
- Important:
 - Pre-shared key itself is *not* part of the matching criteria

FORTINET

© Fortinet Inc. All Rights Reserved.

10

When the first phase 1 IPsec packet arrives, the FortiGate acting as the responder uses the first phase 1 configuration (in alphabetical order) that matches the following:

- Local gateway IP
- Mode (aggressive or main)
- Peer ID, if aggressive mode is used. As explained, only aggressive mode includes the peer ID in the first packet.
- Authentication method (for pre-shared key and certificates)
- Digital certificate information, if certificates are used as the authentication method
- Proposal
- DH group

However, in some circumstances, FortiOS can switch to a different phase 1, if it finds that it initially selected the wrong phase 1. This is called gateway revalidation and applies only to the following:

- IKEv1 with certificate authentication
- IKEv2 with pre-shared key authentication
- IKEv2 with certificate authentication

DO NOT REPRINT
© FORTINET

Responder Dialup Selection Criteria (Contd)

- Multiple dialup VPNs with pre-shared keys, the same local gateway, and the same SA settings, should use aggressive mode and different peer IDs

```
config vpn ipsec phase1-interface
edit "Student-1"
set type dynamic
set interface "port1"
set mode main
set xauthtype auto
set authusrgrp "Students-1"
set peertype any
set dhgrp 14 15 19
set proposal aes128-sha256 aes256-sha384
set psksecret <encrypted_password>
next
```

```
edit "Student-2"
set type dynamic
set interface "port1"
set mode main
set xauthtype auto
set authusrgrp "Students-2"
set peertype any
set dhgrp 14 15 19
set proposal aes128-sha256 aes256-sha384
set psksecret <encrypted_password>
next
```

This VPN will
never be
matched

FORTINET

© Fortinet Inc. All Rights Reserved.

11

If a FortiGate has multiple dialup VPNs using pre-shared keys and sharing the same local gateway, proposal, and DH group, you must use aggressive mode and different peer IDs. Using this method, the FortiGate identifies the right VPN configuration for each incoming IPsec proposal.

DO NOT REPRINT
© FORTINET

Routing IPsec Traffic



In this section, you will learn how FortiGate routes IP traffic.

DO NOT REPRINT
© FORTINET

Routing to Dialup Connections

- In interface mode, by default, static routes are automatically added to each IPsec dialup client

```
config vpn ipsec phase1-interface
edit <phase-1-name>
set type dynamic
set add-route [ enable* | disable ]
set distance <distance>
set priority <priority>
end
```

Disable `add-route` if you are using a dynamic routing protocol over IPsec and do not want FortiGate to automatically add static routes

Distance and priority assigned to the static routes added automatically

FORTINET

© Fortinet Inc. All Rights Reserved.

13

If the IPsec VPN has been configured in interface mode, statics routes are automatically added to clients each time a dialup IPsec connects. The destination subnets of the static routes are the ones received in the phase 2 quick mode selectors. When IKE mode configuration, or DHCP over IPsec is used, those subnets (with a /32 mask) matched the IP addresses assigned to dialup users.

If you are running a dynamic routing protocol over IPsec, disable `add-route`. This will prevent FortiGate from dynamically adding the route, as that is not required because the dynamic routing protocol updates the routing table once the tunnel is up.

By default, the distance assigned to those dynamic routes is 15, and the priority is 0. You can change those values in the phase 1 configuration.

DO NOT REPRINT
© FORTINET

Routing to Dialup Connections (Contd)

- If `net-device` is enabled, FortiGate creates separate virtual interfaces for each dialup client

- FortiGate uses the destination subnets in the quick-mode selectors
- Tunnel name = `phase1Name_index`

```
# config vpn ipsec phase1-interface
  edit Hub
    set add-route enable
    set net-device enable
  # end
```

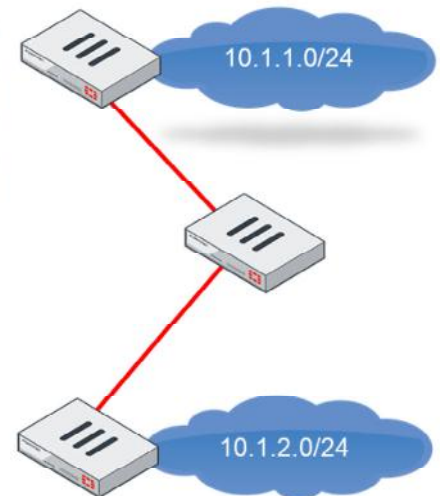
Default value

Default value
is disable

```
# get router info routing-table all
S 10.1.1.0/24 [15/0] via 100.64.3.1, Hub_1
S 10.1.2.0/24 [15/0] via 100.64.5.1, Hub_0
```

Subnets learned through
quick-mode selectors

One virtual interface
for each tunnel



FORTINET

© Fortinet Inc. All Rights Reserved.

14

When the phase 1 setting `net-device` is enabled, FortiGate creates separate virtual interfaces for each dialup client. The names of those interfaces comprise the phase 1 name and an index number.

When you use this configuration, FortiGate uses the information in the destination subnets of the quick-mode selectors to learned the networks behind each remote IPsec client. Each virtual IPsec interface is associated with one client (or one IKE SA).

DO NOT REPRINT
© FORTINET

Routing to Dialup Connections (Contd)

- By disabling `net-device`, FortiGate creates a single interface for all dialup clients

```
# config vpn ipsec phase1-interface
  edit Hub
    set add-route enable
    set net-device disable
    set tunnel-search selectors
  # end
```

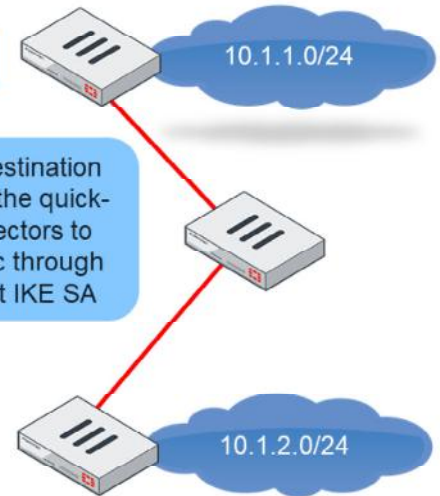
```
# get router info routing-table all
S 10.1.1.0/24 [15/0] via 100.64.3.1, Hub
S 10.1.2.0/24 [15/0] via 100.64.5.1, Hub
```

Default values

Use the destination subnets in the quick-mode selectors to route traffic through the correct IKE SA

Subnets learned through quick-mode selectors

One single interface



FORTINET

© Fortinet Inc. All Rights Reserved.

15

If `net-device` is disabled, FortiGate creates a single IPsec virtual interface that is shared by all IPsec clients connecting to the same dialup VPN.

In this case, the `tunnel-search` setting determines how FortiGate learns the networks behind each remote client. If `tunnel-search` is set to `selectors`, FortiGate uses, as in the previous case, the destination subnets of the quick-mode selectors to populate the routing table with information about the remote networks.

However, in this scenario there can be multiple clients (or IKE SA) associated with a single interface. FortiGate needs more information (specifically, the tunnel index to each remote network) to route traffic to the clients properly.

DO NOT REPRINT
© FORTINET

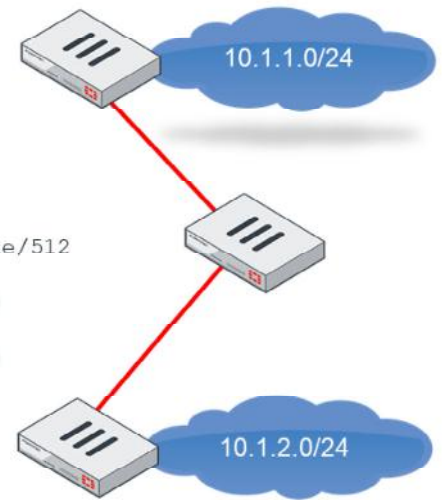
Routing to Dialup Connections (Contd)

```
# config vpn ipsec phase1-interface
  edit Hub
    set add-route enable
    set net-device disable
    set tunnel-search selectors

# end

# diagnose vpn tunnel list name Hub
list ipsec tunnel by names in vd 0
-----
name=Hub ver=1 serial=1 100.64.1.1:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/512
options[0200]=frag_rfc accept_traffic=1
proxyid_num=0 child_num=2 refcnt=15 ilast=56 olast=56 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run tally=2
ipv4 route tree:
10.1.1.0->10.1.1.255 0
10.1.2.0->10.1.1.255 1
```

Quick-mode selectors
and tunnel index



FORTINET

© Fortinet Inc. All Rights Reserved.

16

You can use the command `diagnose vpn tunnel list.` to display extra routing information.

The output from this command shows the mapping between each remote subnet (learned through quick-mode selectors) and the phase 1 index that must be used to properly route the traffic to the correct destinations.

DO NOT REPRINT
© FORTINET

Routing to Dialup Connections (Contd)

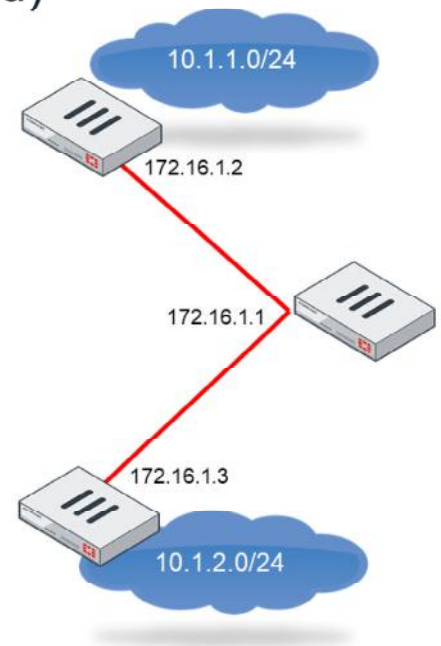
```
# config vpn ipsec phase1-interface
  edit Hub
    set net-device disable
    set tunnel-search nexthop
  # end

# get router info routing-table all
B 10.1.1.0/24 [200/0] via 172.16.1.2, Hub, 00:08:34
B 10.1.2.0/24 [200/0] via 172.16.1.3, Hub, 00:08:21
```

Use the remote IP address learned through IKE to route traffic through the correct IKE SA

You additionally require a dynamic routing protocol for FortiGate to learn the remote subnets

One single interface



FORTINET

© Fortinet Inc. All Rights Reserved.

17

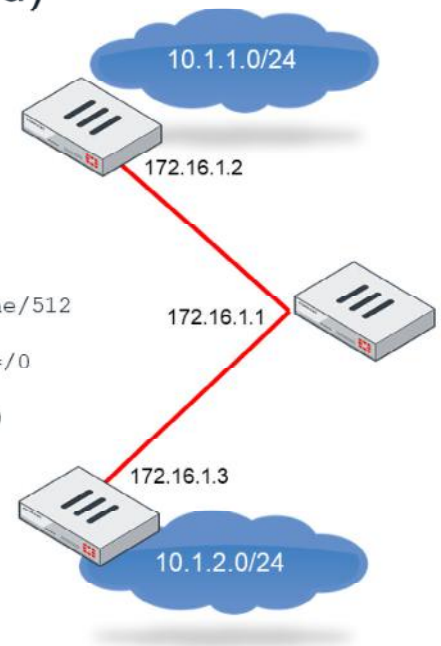
If `net-device` is set to `disable`, and `tunnel-search` is set to `nexthop`, FortiGate does not use the quick-mode selectors to learn about remote networks. FortiGate will learn those routes with the assistance of a dynamic routing protocol, which must be configured to run over the IPsec tunnels.

DO NOT REPRINT
© FORTINET

Routing to Dialup Connections (Contd)

```
# config vpn ipsec phase1-interface
  edit Hub
    set net-device disable
    set tunnel-search nexthop
  # end
# diagnose vpn tunnel list name Hub
list ipsec tunnel by names in vd 0
-----
name=Hub ver=1 serial=1 100.64.1.1:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/512
options[0200]=search-nexthop frag-rfc accept_traffic=1
proxyid_num=0 child_num=2 refcnt=20 ilast=176 olast=176 ad=/0
stat: rxp=22 txp=18 rxb=2992 txb=1752
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=2
ipv4 route tree:
100.64.3.1 1
100.64.5.1 0
172.16.1.2 1
172.16.1.3 0
```

Remote IP and interface index.
By default, it is the IP address of
the IPsec interface in the remote
FortiGate



FORTINET

© Fortinet Inc. All Rights Reserved.

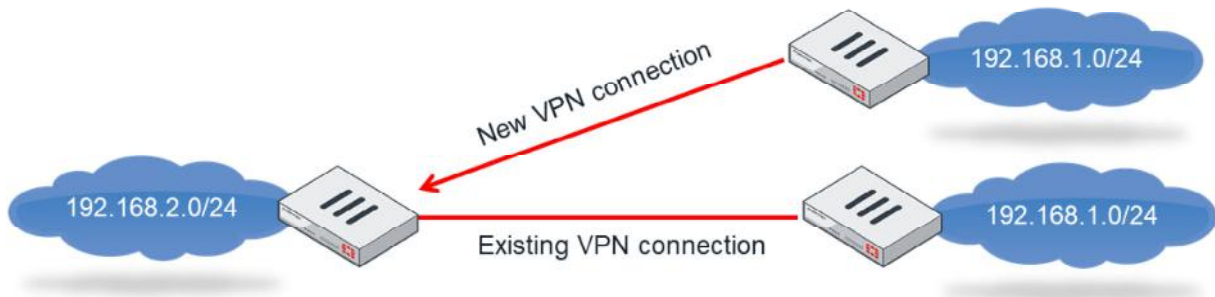
18

As with `tunnel-search` set to `nexthop`, FortiGate creates one single IPsec virtual interface that is shared by all IPsec clients. FortiGate needs more information about how to route the IPsec traffic through the correct IKE SA. With this configuration, FortiGate learns the remote IPs for each client through IKE messages. By default, these remote IPs belong to the IPsec virtual interfaces of the clients. FortiGate combines this information, with the routes learned through a routing protocol, to properly route the IPsec traffic, selecting the correct outbound IPsec virtual interface and IKE SA.

The output of the `diagnose vpn tunnel list` command shows the list of remote IPs and the associated tunnel indexes.

DO NOT REPRINT
© FORTINET

Overlapping Routes



- The `route-overlap` setting in the phase 2 defines the action to take if there is a new incoming dialup connection with overlapping IP subnets
 - `use-new` (default): Disconnect the existing dialup VPN and accept the new VPN
 - `use-old`: Keep the existing dialup VPN up and reject the new one
 - `allow`: Keep the existing dialup VPN up and accept the new one.

FORTINET

© Fortinet Inc. All Rights Reserved.

19

If two remote sites have the same subnets, they might create overlapping static routes in the central FortiGate. The setting `route-overlap`, found in phase 2, defines what action FortiGate will take when a new remote site is connecting and there is a remote site already connected with an overlapping subnet. The possible actions include:

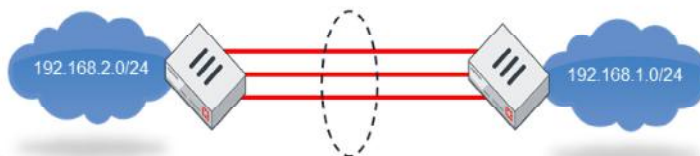
- `use-new` (default): Disconnect the existing dialup VPN and accept the new VPN.
- `use-old`: Keep the existing dialup VPN up and reject the new one.
- `allow`: Keep the existing dialup VPN up and accept the new one. Traffic for sessions that start from the central FortiGate will be load balanced (ECMP) between both VPNs.

DO NOT REPRINT
© FORTINET

IPsec Tunnel Aggregation

- Two or more IPsec tunnels between two sites can be combined to create an aggregated tunnel
 - Similar to LACP port aggregation
 - One single aggregated IPsec interface for routing and firewall policing

L3 – Layer 3 load balancing
L4 – Layer 4 load balancing
redundant – Use first tunnel that comes up
weighted-round-robin – round-robin routing using link weight



FORTINET

VPN > IPsec Tunnels > Create New > IPsec Aggregate

New IPsec Aggregate

Name

Algorithm Weighted Round Robin

Aggregate Member

L3	Weighted Round Robin
L4	
Redundant	

```
config vpn ipsec phase1-interface
edit < >
set aggregate member enable
set aggregate-weight < >
next
end
```

Set weight to use per-packet load balancing
using weighted-round-robin

© Fortinet Inc. All Rights Reserved.

20

Two or more IPsec tunnels between two sites can be combined to create an aggregated tunnel. This is similar to LACP port aggregation. One single aggregated IPsec interface is created and used for routing and firewall policing.

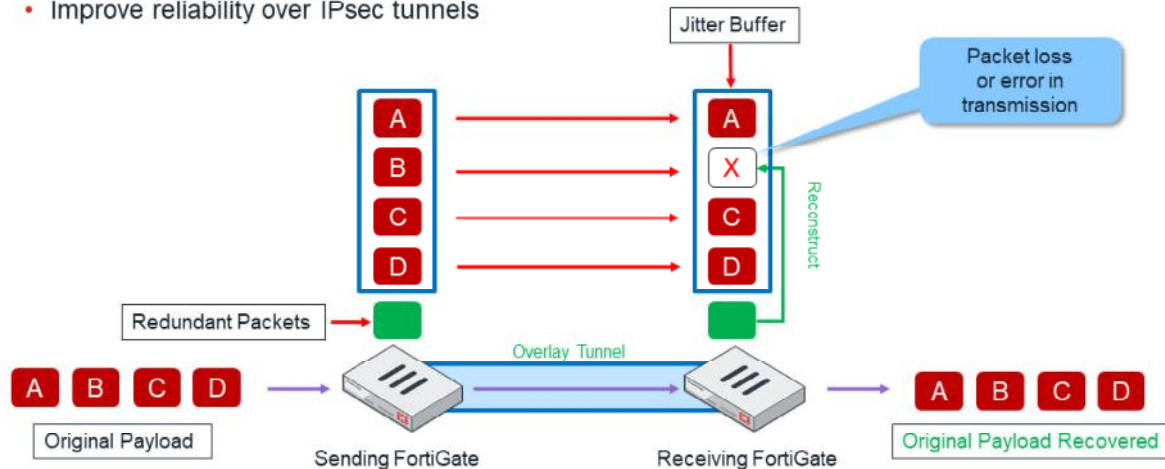
Aggregated IPsec tunnels support five load-balancing methods:

- `round-robin`: Traffic is balanced per-packet.
- `L3`: Traffic is balanced based on the Layer 3 header information.
- `L4`: Traffic is balanced based on the Layer 4 header information.
- `redundant`: All traffic is sent through the tunnel that came up first. The other tunnels are used for backup.
- `weighted-round-robin`: Traffic is load balanced in a round-robin manner based on link weights configured for each tunnel.

DO NOT REPRINT
© FORTINET

Forward Error Correction (FEC)

- Add additional packets with redundant data
- The recipient can use the redundant data to reconstruct any lost packet
 - Improve reliability over IPsec tunnels



FORTINET

© Fortinet Inc. All Rights Reserved.

21

Forward Error Correction (FEC) is a phase 1 setting that, when enabled, adds additional packets with redundant data. The recipient can use this redundant information to reconstruct any lost packet, or any packet that arrived with errors. Although this feature increases the bandwidth usage, it improves reliability that can overcome adverse WAN conditions such as lossy or noisy links. FEC can be critical for delivering a better user experience for business-critical applications like voice and video services.

DO NOT REPRINT
© FORTINET

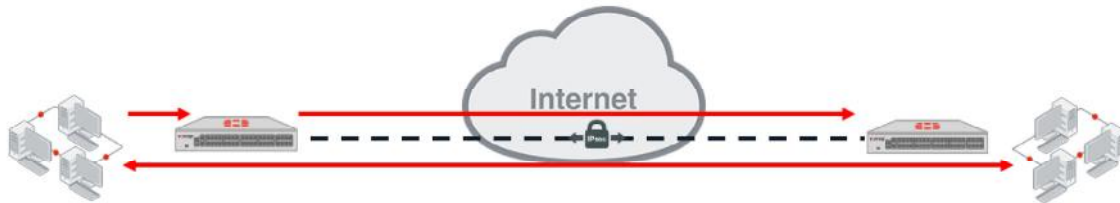
IPsec Troubleshooting

In this section, you will learn the basics of IPsec troubleshooting.

DO NOT REPRINT
© FORTINET

IPsec Connection Steps

1. Interesting traffic triggers the VPN negotiation
2. Phase 1 goes up
 - Single bidirectional IKE security association (SA)
3. Extended authentication (if required)
4. IKE mode configuration (if required)
5. Phase 2 goes up
 - Two IPsec SAs (one for each traffic direction) for each phase 2
6. Tunnel is established and traffic can traverse tunnel



FORTINET

© Fortinet Inc. All Rights Reserved.

23

When isolating IPsec problems, it is useful to understand that an IPsec connection can be described as a multistep process:

1. Interesting traffic triggers the VPN negotiation. Traffic is called *interesting* when it must travel through an IPsec tunnel (encrypted and encapsulated) to reach a remote network.
2. Phase 1 goes up.
3. If extended authentication is required, one side authenticates.
4. If one side requires IP settings, the other side sends the required settings through IKE mode configuration.
5. One or more phase 2s go up. Two IPsec SAs are negotiated for each phase 2.
6. Traffic crosses the tunnel.

So, if you have an IPsec issue, you should identify in which of these steps the problem has occurred.

DO NOT REPRINT
© FORTINET

IKE Filter Options

```
# diagnose vpn ike log filter
list          Display the current filter.
clear         Erase the current filter.
name          Phase1 name to filter by.
src-addr4     IPv4 source address range to filter by.
msrc-addr4    multiple IPv4 source address to filter by.
dst-addr4     IPv4 destination address range to filter by.
mdst-addr4    multiple IPv4 destination address to filter by.
src-addr6     IPv6 source address range to filter by.
msrc-addr6    multiple IPv6 source address to filter by.
dst-addr6     IPv6 destination address range to filter by.
mdst-addr6    multiple IPv6 destination addresses to filter by.
src-port      Source port range to filter by.
dst-port      Destination port range to filter by.
vd            Index of virtual domain. -1 matches all.
interface     Interface that IKE connection is negotiated over.
negate        Negate the specified filter parameter.

# diagnose vpn ike log filter clear
# diagnose vpn ike log filter dst-addr4 <remote peer ip>
```

FORTINET

© Fortinet Inc. All Rights Reserved.

24

The IKE daemon handles all IPsec connections on FortiGate. It's important to familiarize yourself with the available filter options. You use these options to filter the output of the IKE real-time debug, so that only information that is relevant to you is displayed.

The most common filter option is `dst-addr4`, which you use to filter the output by the IP address of the remote peer. Also, multiple addresses are supported. Filtering by name is helpful when the remote peer IP address is unknown.

DO NOT REPRINT
© FORTINET

IKE Real-Time Debug

```
# diagnose debug application ike <bit-mask>
```

```
# diagnose debug enable
```

- Bit-mask value: -1 is recommended
- You should enable timestamp when troubleshooting IKE issues:

```
# diagnose debug console timestamp enable
```

Bit-mask	Description
1	Major errors
2	Configuration changes
4	Connections attempts
8	Phase 1 and 2 negotiation messages
16	NAT-T messages
32	Dead peer detection messages
64	Encryption and decryption keys
128	Encrypted traffic Payload

After setting the filter, enable the IKE real-time debug using the commands shown on this slide.

The table shown on this slide includes the type of output that is enabled by each bit in the bit-mask. The most common value for the bit-mask is -1 (all outputs enabled). It shows the DPD packets and all the information required for troubleshooting IPsec negotiation problems.

DO NOT REPRINT
© FORTINET

Debugging Main Mode

```
# diagnose debug application ike -1
# diagnose debug enable
```

```
ike 0: comes 10.10.2.2:500->10.10.1.1:500,ifindex=6....
ike 0: IKEv1 exchange=Identity Protection id=76a2fb2b18d6fee7/0000000000000000 len=716
ike 0:....92: responder: main mode get 1st message...
ike 0:....92: VID RFC 3947 4A131C81070358455C5728F20E95452F
```

```
ike 0:....92: negotiation result
ike 0:....92: proposal id = 1:
ike 0:....92:   protocol id = ISAKMP:
ike 0:....92:   trans_id = KEY_IKE.
ike 0:....92:   encapsulation = IKE/none
ike 0:....92:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:....92:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....92:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....92:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:....92: ISAKMP SA lifetime=86400
```

```
ike 0:....92: SA proposal chosen, matched gateway Hub2Spoke1
ike 0: found Hub2Spoke1 10.10.1.1 6 -> 10.10.2.2:500
```

First main mode message

Phase 1 proposal

Proposal chosen and matched tunnel Hub2Spoke1

FORTINET

© Fortinet Inc. All Rights Reserved.

26

Now, you will look at the output of the IKE real-time debug during a main-mode negotiation. As explained earlier, main mode requires the interchange of six packets. The real-time debug shows when the first packet (first main mode message) arrives. Then the debug shows the negotiated settings for the phase 1. A message is generated once FortiGate identifies the VPN configuration to use (with the name of the VPN).

Debugging Main Mode (Contd)

```
ike 0:Hub2Spoke1:92: peer is FortiGate/FortiOS (v6 b1579)
```

Remote peer device
information

```
...
ike 0:Hub2Spoke1:92: sent IKE msg (ident_r1send): 10.10.1.1:500->10.10.2.2:500, len=192,
id=76a2fb2b18d6fee7/399d6ddd6e830672
```

```
ike 0: comes 10.10.2.2:500->10.10.1.1:500, ifindex=6....
```

```
ike 0: IKEv1 exchange=Identity Protection id=76a2fb2b18d6fee7/399d6ddd6e830672 len=380
```

```
ike 0:Hub2Spoke1:92: responder:main mode get 2nd message...
```

Second main mode
message

```
ike 0:Hub2Spoke1:92: NAT not detected
```

```
ike 0:Hub2Spoke1:92: sent IKE msg (ident_r2send): 10.10.1.1:500->10.10.2.2:500, len=380,
id=76a2fb2b18d6fee7/399d6ddd6e830672
```

```
ike 0: comes 10.10.2.2:500->10.10.1.1:500, ifindex=6....
```

```
ike 0: IKEv1 exchange=Identity Protection id=76a2fb2b18d6fee7/399d6ddd6e830672 len=108
```

```
ike 0:Hub2Spoke1:92: responder: main mode get 3rd message...
```

Third main mode
message

```
...
ike 0:Hub2Spoke1:92: received pl notify type INITIAL-CONTACT
```

```
ike 0:Hub2Spoke1:92: peer identifier IPV4_ADDR 10.10.2.2
```

```
ike 0:Hub2Spoke1:92: PSK authentication succeeded
```

Authentication
successful

```
ike 0:Hub2Spoke1:92: authentication OK
```

```
ike 0:Hub2Spoke1:92: sent IKE msg (ident_r3send): 10.10.1.1:500->10.10.2.2:500, len=92,
id=76a2fb2b18d6fee7/399d6ddd6e830672
```

```
...
ike 0:Hub2Spoke1:92: established IKE SA 76a2fb2b18d6fee7/399d6ddd6e830672
ike 0:Hub2Spoke1:92: processing INITIAL-CONTACT
```

Phase 1 is up

FORTINET

© Fortinet Inc. All Rights Reserved.

27

Next, the output shows the remote peers information. The second and third main mode messages arrive. After the authentication is successful and the preshared key matches, a final message is generated to indicate that the phase 1 is up.

Debugging Aggressive Mode

```

ike 0: comes 10.10.2.2:500->10.10.1.1:500,ifindex=6....
ike 0: IKEv1 exchange=Aggressive id=3c6c62a443611a29/0000000000000000 len=776
ike 0:...:96: responder: aggressive mode get 1st message.....
ike 0:...:96: VID FORTIGATE 8299031/57A36082C6A621DE00050428
ike 0::96: peer identifier IPV4_ADDR 10.10.2.2
ike 0:...:96: negotiation result
ike 0:...:96: proposal id = 1:
ike 0:...:96:   protocol id = ISAKMP:
ike 0:...:96:     trans_id = KEY_IKE.
ike 0:...:96:     encapsulation = IKE/none
ike 0:...:96:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:...:96:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:...:96:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:...:96:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:...:96: ISAKMP SA lifetime=86400
ike 0:...:96: SA proposal chosen, matched gateway Hub2Spoke1
ike 0: found Hub2Spoke1 10.10.1.1 6 -> 10.10.2.2:500...
ike 0:Hub2Spoke1:96: responder: aggressive mode get 2nd response...
...
ike 0:Hub2Spoke1:96: PSK authentication succeeded
ike 0:Hub2Spoke1:96: authentication OK
ike 0:Hub2Spoke1:96: NAT not detected
ike 0:Hub2Spoke1:96: established IKE SA 3c6c62a443611a29/dccee519f2e8b9b9
ike 0:Hub2Spoke1: carrier up

```

First aggressive mode message

IKE proposal

Proposal chosen for Hub2Spoke1

Authentication successful

Phase 1 is up

This slide shows the output of the real-time debug for phase 1 aggressive mode. It displays the three aggressive-mode packets interchanged, and the proposals.

DO NOT REPRINT
© FORTINET

Debugging XAuth

ike 0:DialUP_0:13: initiating XAUTH.

ike 0:DialUP_0:13: sending XAUTH request

CFG_REQUEST sent

ike 0:DialUP_0:13: sent IKE msg (cfg_send): 10.200.1.1:500->10.200.3.1:500, len=76, id=2d5d8e9aa17045c4/e93fbb0a30d4b217:bd294d3e

ike 0:DialUP_0:13: peer has not completed XAUTH exchange

CFG_REPLY received

ike 0: comes 10.200.3.1:500->10.200.1.1:500, ifindex=2....

ike 0: IKEv1 exchange=Mode config id=2d5d8e9aa17045c4/e93fbb0a30d4b217:bd294d3e len=92

ike 0:DialUP_0:13: received XAUTH_USER_NAME 'fortinet' length 8

ike 0:DialUP_0:13: received XAUTH_USER_PASSWORD length 8

ike 0:DialUP_0: XAUTH user "fortinet"

ike 0:DialUP: auth group VPN

CFG_SET sent

ike 0:DialUP_0: XAUTH succeeded for user "fortinet" group "VPN"

ike 0:DialUP_0:13: sent IKE msg (cfg_send): 10.200.1.1:500->10.200.3.1:500, len=68, id=2d5d8e9aa17045c4/e93fbb0a30d4b217:3639b66f

CFG_ACK received

ike 0: comes 10.200.3.1:500->10.200.1.1:500, ifindex=2....

ike 0: IKEv1 exchange=Mode config id=2d5d8e9aa17045c4/e93fbb0a30d4b217:3639b66f len=68

FORTINET

© Fortinet Inc. All Rights Reserved.

29

The IKE real-time debug shows, after phase 1, the exchange of XAuth packets. On this slide, you can see the CFG_REQUEST packet. You can also see the CFG_REPLY, showing the XAuth user and group name.

After that, the IKE real-time debug shows the CFG_SET and CFG_ACK.

DO NOT REPRINT
© FORTINET

Debugging IKE Mode Configuration

...

ike 0: comes 172.31.18.81:500->172.31.224.125:500,ifindex=5....

CFG_REQUEST received

ike 0: IKEv1 exchange=Mode config id=bc69d3c493f5/9137d875a2c420c6:c4ad

ike 0:vpn_0:4: mode-cfg type 1 request 0:''

ike 0:vpn_0:4: mode-cfg using allocated IPv4 10.255.255.100

ike 0:vpn_0:4: mode-cfg assigned (1) IPv4 address 10.255.255.100

ike 0:vpn_0:4: mode-cfg type 2 request 0:''

ike 0:vpn_0:4: mode-cfg assigned (2) IPv4 netmask 255.255.255.0

ike 0:vpn_0:4: mode-cfg type 3 request 0:''

ike 0:vpn_0:4: mode-cfg send (3) IPv4 DNS(1) 10.185.0.200

CFG_REPLY sent

ike 0:vpn_0:4: sent IKE msg (cfg send): 172.31.224.125:500->172.31.18.81:500,

ike 0: comes 172.31.18.81:500->172.31.224.125:500,ifindex=5....

...

FORTINET

© Fortinet Inc. All Rights Reserved.

30

After the extended authentication, the remote site proceeds to request and receive the IP settings through IKE mode configuration.

The output shows the CFG_REQUEST and CFG_REPLY packets.

Debugging Phase 2

```
ike 0:comes 10.10.2.2:500->10.10.1.1:500,ifindex=6....
ike 0:IKEv1 exchange=Quick id=3c6c62a443611a29/dccee519f2e8b9b9:8f32bfcc len=588
ike 0:Hub2Spoke1:96:551: responder received first quick-mode message
```

```
...
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: my proposal:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: proposal id = 1:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   protocol id = IPSEC_ESP:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   PFS DH group = 14
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   trans_id = ESP_AES_CBC (key_len = 128)
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   type = AUTH_ALG, val=SHA1
```

Local gateway proposal(s)

```
...
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: incoming proposal:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: proposal id = 1:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   protocol id = IPSEC_ESP:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   PFS DH group = 14
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   trans_id = ESP_AES_CBC (key_len = 128)
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   type = AUTH_ALG, val=SHA1
```

Remote gateway proposal(s)

This slide shows the phase 2 negotiation.

The debug shows the phase 2 proposal from the local gateway, and the phase 2 proposal coming to the remote gateway. In this case, both proposals (local and remote) match.

Debugging Phase 2 (Contd)

```
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: negotiation result
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: proposal id = 1:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   protocol id = IPSEC_ESP:
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   PFS DH group = 14
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   trans_id = ESP_AES_CBC (key_len = 128)
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:Hub2Spoke1:96:Hub2Spoke1:551:   type = AUTH_ALG, val=SHA1
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: set pfs=MODP2048
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: using tunnel mode.
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: replay protection enabled
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: SA life soft seconds=43153.
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: SA life hard seconds=43200.
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: IPsec SA selectors #src=1 #dst=1
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: src 0 7 0:192.168.1.0-192.168.1.255:0
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: dst 0 7 0:10.10.20.0-10.10.20.255:0
***
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: add IPsec SA: SPIs=01e54b23/3dd3546b
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: added IPsec SA: SPIs=01e54b23/3dd3546b
ike 0:Hub2Spoke1:96:Hub2Spoke1:551: sending SNMP tunnel UP trap
```

Negotiated phase 2
proposal

Phase 2 is up

Next, the output shows the negotiated phase 2 settings. The last messages confirm that the phase 2 is up.

DO NOT REPRINT
© FORTINET

Debug Flow of Tunnel Traffic

```
Hub # id=20085 trace_id=5 func=print_pkt_detail line=4742 msg="vd-root received a
packet(proto=1, 192.168.1.111:1->10.10.20.111:2048) from lan. type=8, code=0, id=1, seq=165."
id=20085 trace_id=5 func=init_ip_session_common line=4893 msg="allocate a new session-001efeca"
```

Must match quick-mode selectors

```
id=20085 trace_id=5 func=vf_ip4_route_input line=1597 msg="find a route: flags=00000000 gw=10.10.20.111 via
Hub2Spoke1"
```

```
id=20085 trace_id=5 func=fw_forward_handler line=691 msg="Allowed by Policy-10:"
```

Traffic allowed by
VPN firewall policy

```
id=20085 trace_id=5 func=... line=122 msg="enter IPsec interface-Hub2Spoke1"
```

```
id=20085 trace_id=5 func=esp_output4 line=1149 msg="IPsec encrypt/auth"
```

```
id=20085 trace_id=5 func=ipsec_output_finish line=519 msg="send to 10.10.1 2 via intf-wan2"
```

Reply from remote host

Traffic entering the tunnel

```
id=20085 trace_id=6 func=print_pkt_detail line=4742 msg="vd-root received a packet(proto=1, 10.10.20.111:1-
192.168.1.111:0) from Hub2Spoke1. type=0, code=0, id=1, seq=165."
```

```
id=20085 trace_id=6 func=resolve_ip_tuple_fast line=4806 msg="Find an existing session, id-001efeca, reply
direction"
```

Traffic allowed using existing
session

FORTINET

© Fortinet Inc. All Rights Reserved.

33

If the VPN is up but the traffic can't cross the tunnel, you should use the debug flow. This slide shows an example output of the debug flow for traffic that is crossing an IPsec tunnel. The output shows the following:

- Packet arriving
- Packet being allowed by a firewall policy
- Packet entering the tunnel
- Packets being encrypted and sent

If the traffic is not crossing the tunnel because of a routing misconfiguration, the output of the debug flow shows it. The debug flow also displays if the traffic drops and why (for example, when packets don't match the quick mode selector).

Capturing IKE Traffic

Protocol	NAT and NAT-T	No NAT
IKE	Initially UDP port 500 UDP port 4500 after NAT is detected	UDP port 500
ESP	Encapsulated in UDP port 4500	IP protocol 50

- No NAT:
 - IKE traffic:


```
# diagnose sniffer packet <port> 'host <remote-gw> and udp port 500'
```
 - ESP traffic


```
# diagnose sniffer packet any 'host <remote-gw> and esp'
```
- With NAT and NAT-T:
 - IKE and ESP traffic:


```
# diagnose sniffer packet any 'host <remote-gw> and (udp port 500 or udp port 4500)'
```

If you need to capture the IPsec traffic, remember that the IP protocol and UDP port numbers depend on NAT-T and the use of NAT.

If there is no FortiGate located in the middle that is running NAT, IKE traffic uses UDP port 500 and ESP traffic uses IP protocol 50. This slide shows the two sniffer filters that the sniffer command must use to capture each of those traffic protocols.

If NAT-T is enabled, and there is a FortiGate located in the middle that is running NAT, the sniffer command must use a different filter. In this case, IKE traffic uses port UDP 500, but switches to UDP port 4500 during the tunnel negotiation. Additionally, ESP traffic is encapsulated inside the UDP-4500 channel.

DO NOT REPRINT

© FORTINET

IPsec SA

```
# diagnose vpn tunnel list name Hub2Spoke1
list ipsec tunnel by names in vd 0
-----
name=Hub2Spoke1 ver=1 serial=2 10.10.1.1:0->10.10.2.2:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=8 ilast=11 olast=3 auto-discovery=0
stat: rxp=513 txp=129 rxb=459050 txb=93
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=36
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=Hub2Spoke1 proto=0 sa=1 ref=2 serial=1
src: 0:192.168.1.0/255.255.255.0:0
dst: 0:10.10.20.0/255.255.255.0:0
SA: ref=7 options=2e type=00 soft=0 mtu=1438 expire=41195/0B replaywin=1024 seqno=9d esn=0
replaywin_lastseq=00000200
life: type=01 bytes=0/0 timeout=43150/43200
dec: spi=01e54b14 esp=aes key=16 914dc5d092667ed436ea7f6efb867976
    ah=sha1 key=20 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
enc: spi=3dd3545f esp=aes key=16 017b8ff6c4ba21eac99b22380b7de74d
    ah=sha1 key=20 edd8141f4956140eef703d9042621d3dbf5cd961
dec:pkts/bytes=513/458986, enc:pkts/bytes=250/26848
npu_flag=03 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu_selid=1
```

Lists specified tunnel
information only

DPD information

Anti-replay is enabled

SA information

Hardware offload
information

FORTINET

© Fortinet Inc. All Rights Reserved.

35

The command `diagnose vpn tunnel list` displays the current IPsec SA information for all active tunnels.

The command `diagnose vpn tunnel list name <tunnel name>` provides SA information about a specific tunnel.

DO NOT REPRINT
© FORTINET

IPsec Tunnel Details

```
Hub # get vpn ipsec tunnel details
gateway
```

```
name: 'Hub2Spoke1'
type: route-based
local-gateway: 10.10.1.1:0 (static)
remote-gateway: 10.10.2.2:0 (static)
mode: ike-v1
interface: 'wan2' (6)
rx packets: 1025 bytes: 524402 errors: 0
tx packets: 641 bytes: 93 errors: 0
dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
selectors
```

Phase 1 details

```
name: 'Hub2Spoke1'
auto-negotiate: disable
mode: tunnel
src: 0:192.168.1.0/0.0.0.0:0
dst: 0:10.10.20.0/0.0.0.0:0
SA
```

Quick mode selectors

```
lifetime/rekey: 43200/32137
mtu: 1438
```

Tunnel MTU

```
tx-esp-seq: 2ce
replay: enabled
```

```
inbound
spi: 01e54b14
enc: aes-cb 914dc5d092667ed436ea7f6efb867976
auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
outbound
spi: 3dd3545f
enc: aes-cb 017b0ff6c4ba21eac59b22380b7dc74d
```

Phase 2 SAs for each direction

```
auth: sha1 edd8141f4956140eeef703d5042621d3dbf5cd961
```

Hardware acceleration

```
NEU acceleration: encryption(outbound) decryption(inbound)
```

FORTINET

© Fortinet Inc. All Rights Reserved.

36

`get vpn ipsec tunnel details` provides detailed information for the active IPsec tunnels.

DO NOT REPRINT
© FORTINET

IKE Gateway List

```
Hub # diagnose vpn ike gateway list name Hub2Spoke1
vd: root/0
name: Hub2Spoke1
version: 1
interface: wan2 6
addr: 10.10.1.1:500 -> 10.10.2.2:500
created: 3196s ago
auto-discovery: 0
IKE SA: created 1/1 established 1/1 time 6020/6020/6020 ms
IPsec SA: created 1/1 established 1/1 time 40/40/40 ms
```

When was the phase 1
created

```
id/spi: 87 16b474clae9de3ca/67e428c8c7118617
```

```
direction: initiator
```

Is this gateway initiator
or responder?

```
status: established 3196-3190s ago = 6020ms
```

```
proposal: aes128-sha256
```

```
key: 34641b135ceeb2cd-c44a41d15dec439c
```

```
lifetime/rekey: 86400/82909
```

```
DPD sent/rcv: 00000040/0000002e
```

```
Hub # diagnose vpn ike gateway clear <name>
```

Clear phase 1

FORTINET

© Fortinet Inc. All Rights Reserved.

37

The command `diagnose vpn ike gateway list` also provides some details about a tunnel.

The command `diagnose vpn ike gateway clear` closes a phase 1. Be careful when using this command as it has a global effect, meaning that running it without specifying the phase 1 name will result in all phase 1s of all VDOMs being cleared.

DO NOT REPRINT
© FORTINET

Additional IPsec Debug Commands

```
Hub # get vpn ipsec stats tunnel
```

```
tunnels
total: 1
static/ddns: 1
dynamic: 0
manual: 0
errors: 0
selectors
total: 1
up: 1
```

Number of tunnels
currently active

```
Hub # get vpn ipsec tunnel summary
```

```
'Hub2Spoke1' 10.10.2.2:0 selectors(total,up): 1/1 rx(pkt,err): 1025/0 tx(pkt,err): 769/0
```

```
Hub # get ipsec tunnel list
```

NAME	REMOTE-GW	PROXY-ID-SOURCE	PROXY-ID-DESTINATION	STATUS	TIMEOUT
Hub2Spoke1	10.10.2.2:0	192.168.1.0/255.255.255.0	10.10.20.0/255.255.255.0	up	42844

Tunnel
name

Peer IP

Quick mode selectors

Status

Timeout value for each
active tunnel

FORTINET

© Fortinet Inc. All Rights Reserved.

38

The command `get vpn ipsec stats tunnel` provides some global overall counters related to all the VPNs currently active.

The other two commands shown on this slide provide summarized information about the VPNs.

DO NOT REPRINT
© FORTINET

Hardware Offloading Requirements

- You can offload IPsec encryption and decryption to hardware on some FortiGate models
- Hardware offloading capabilities and supported algorithms vary by processor type and model
- By default, offloading is enabled for supported algorithms
 - You can manually disable offloading:

```
config vpn ipsec phase1-interface
    edit <tunnel_name>
        set npu-offload enable | disable
    next
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

39

On some FortiGate models, you can offload the encryption and decryption of IPsec traffic to hardware. The supported algorithms depend on the model and type of processor on the unit that is offloading the encryption and decryption.

By default, hardware offloading is enabled for the supported algorithms. This slide shows the commands you can use to disable hardware offloading per tunnel, if necessary.

Session NPU-Flag Field

- IPsec SAs have an NPU-flag field

```
# diagnose vpn tunnel list name Hub2Spoke1
list ipsec tunnel by names in vd 0
...
npu_flag=03 npu_rgw=10.10.2.2 npu_lgw=10.10.1.1
npu_selid=1
```

NPU-flag Value	Description
npu_flag=00	Both IPsec SAs loaded to the kernel
npu_flag=01	Outbound IPsec SA copied to NPU
npu_flag=02	Inbound IPsec SA copied to NPU
npu_flag=03	Both outbound and inbound IPsec SA copied to NPU
npu_flag=20	Unsupported cipher or HMAC, IPsec SA cannot be offloaded

FORTINET

© Fortinet Inc. All Rights Reserved.

40

All IPsec SAs have an `npu_flag` field indicating offloading status. In the case of IPsec traffic, the FortiGate session table also includes that field.

First, when phase 2 goes up, the IPsec SAs are created and loaded to the kernel. As long as there is no traffic crossing the tunnel, the SAs are not copied to the NPU, and the `npu_flag` shows 00. The value of that field also remains 00 when IPsec offloading is disabled.

Second, if the first IPsec packet that arrives is an outbound packet that can be offloaded, the outbound SA is copied to the NPU and the `npu_flag` changes to 01. However, if the first IPsec packet is inbound and can be offloaded, the inbound SA is copied to the NPU and the `npu_flag` changes to 02.

After both SAs are copied to the NPU, the `npu_flag` changes to 03.

The value 20 in the `npu_flag` field indicates that hardware offloading is unavailable because of an unsupported cipher or HMAC algorithm.

Common IPsec Problems

Problem	Output of IKE debug	Common Causes	Common Solutions
Tunnel is not coming up	Error: negotiation failure	IPsec configuration mismatch	Verify phase 1 and phase 2 configurations between both peers
	Error: no SA proposal chosen	IPsec configuration mismatch	Verify phase 1 and phase 2 configurations between both peers
Tunnel unstable	DPD packet lost	ISP issue	Check internet connection
Tunnel is up but traffic doesn't pass through it	Error in debug flow: no matching IPsec Selector, drop	Quick mode selectors mismatch	Verify quick mode selectors are correct
		NAT is enabled	Disable NAT on the VPN firewall policy
	Routing issue	Route missing or pointing to wrong device	Verify route is correctly defined

FORTINET

© Fortinet Inc. All Rights Reserved.

41

This slide shows a summary of the most common IPsec problems and solutions.

If the tunnel doesn't come up, use the IKE real-time debug. In such cases, an error message usually appears.

When the tunnel is unstable, you usually see that DPD packets are being lost, which indicates that the problem might be on the ISP side.

If the tunnel is up but traffic isn't passing through it, use the debug flow. One of the peers might be dropping packets or routing traffic incorrectly. Another possibility is that the packets don't match the quick mode selectors, so FortiGate drops the packets.

Review

- ✓ IPsec review
- ✓ Responder dialup selection criteria
- ✓ IPsec routing
- ✓ IPsec VPNs with overlapping routes
- ✓ Troubleshoot IPsec
- ✓ Offload hardware for encryption and decryption
- ✓ Identify common IPsec problems
- ✓ Capture IKE and IPsec traffic

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

DO NOT REPRINT
© FORTINET

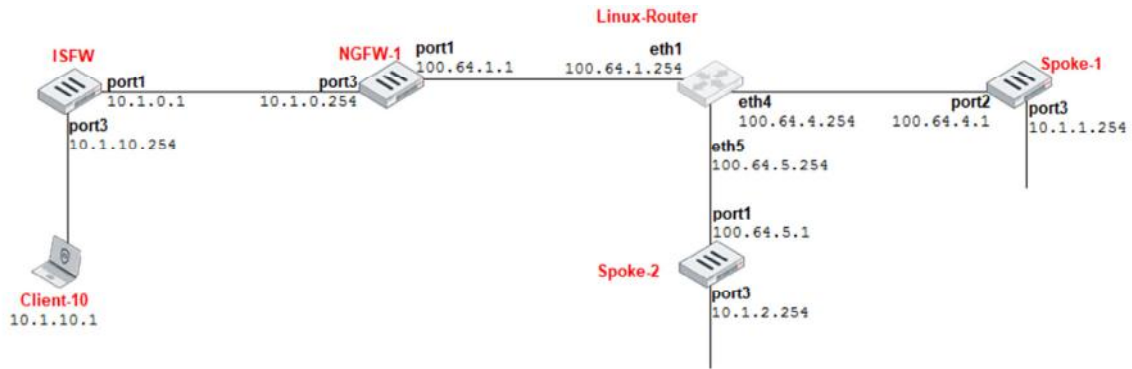
Lab 12—IPsec

Now, you will now work on *Lab 12—IPsec*.

DO NOT REPRINT
© FORTINET

Lab 12—IPsec

- Troubleshooting:
 - IPsec between Spoke-1 and Spoke-2 is not coming up



FORTINET

© Fortinet Inc. All Rights Reserved.

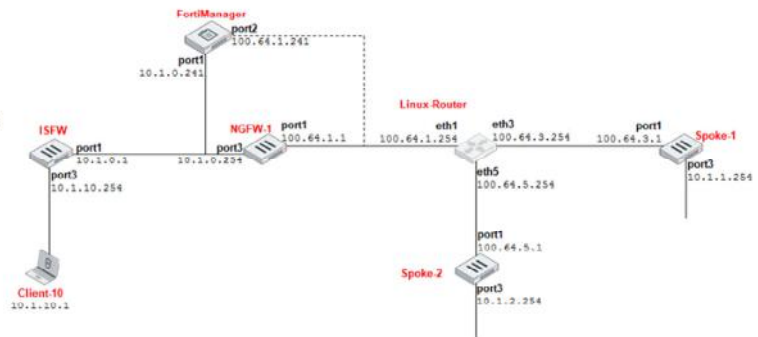
44

In this lab, you will troubleshoot an IPsec problem between Spoke-1 and Spoke-2.

DO NOT REPRINT
© FORTINET

Lab 12—IPsec

- VPN Manager:
 - Create a VPN community
 - NGFW-1 is the hub
 - Spoke-1 and Spoke-2 are spokes
 - Install the VPN configuration
 - Add IPsec firewall policies
 - Install the policies



- Do not send traffic; routing is not ready yet

Then, you will configure a hub-and-spoke VPN network using the FortiManager VPN manager.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about autodiscovery VPN (ADVPN).

DO NOT REPRINT
© FORTINET

Objectives

- Configure and test autodiscovery VPN with Internal Border Gateway Protocol (IBGP)
- Use the Internet Key Exchange (IKE) real-time debug to troubleshoot ADVPN problems

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

By demonstrating competence in the Fortinet ADVPN, you will be able to configure and test ADVPN with IBGP, as well as use the IKE real-time debug to troubleshoot ADVPN problems.

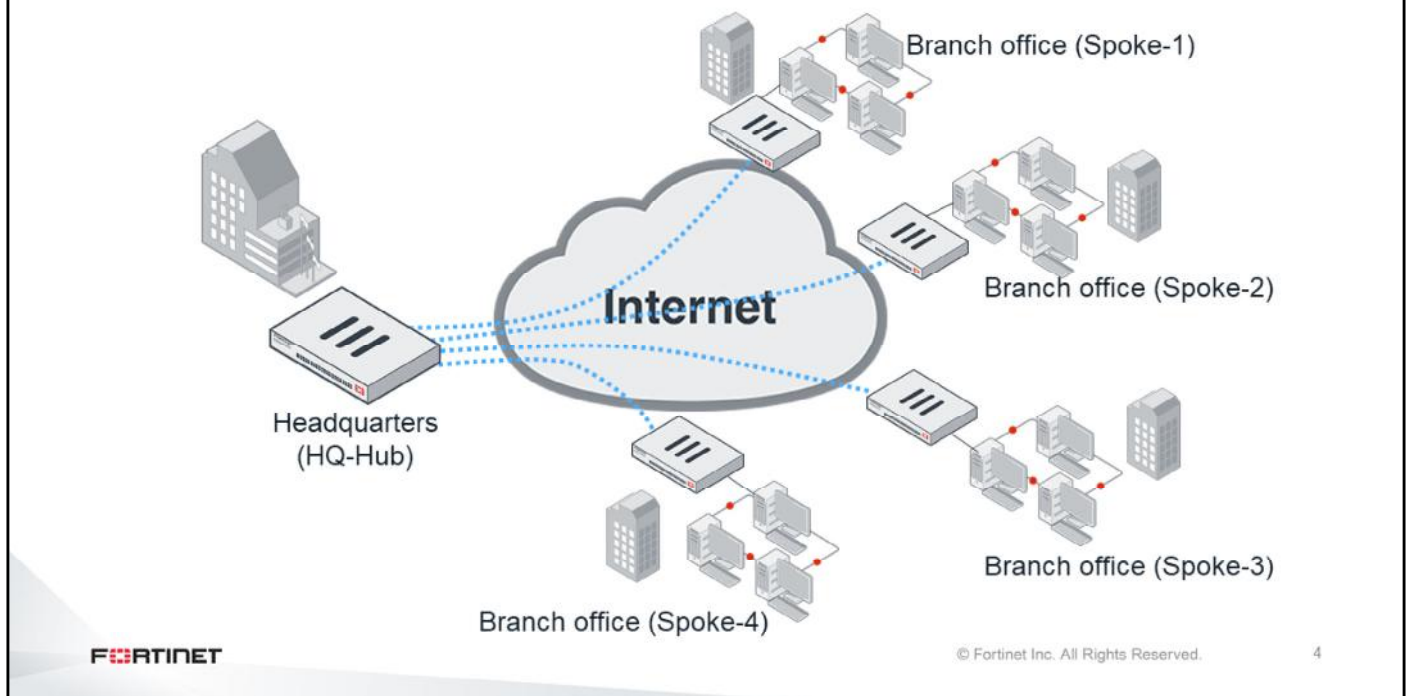
DO NOT REPRINT
© FORTINET



In this section, you will learn how to deploy and manage ADVPN.

DO NOT REPRINT
© FORTINET

Hub-and-Spoke Topology



Why should you use ADVPN? To find the answer, you will review the most common VPN topologies.

One point-to-multipoint topology variation is called *hub-and-spoke*. As its name describes, all clients connect through a central *hub*, similar to the way spokes connect to hubs on wheels.

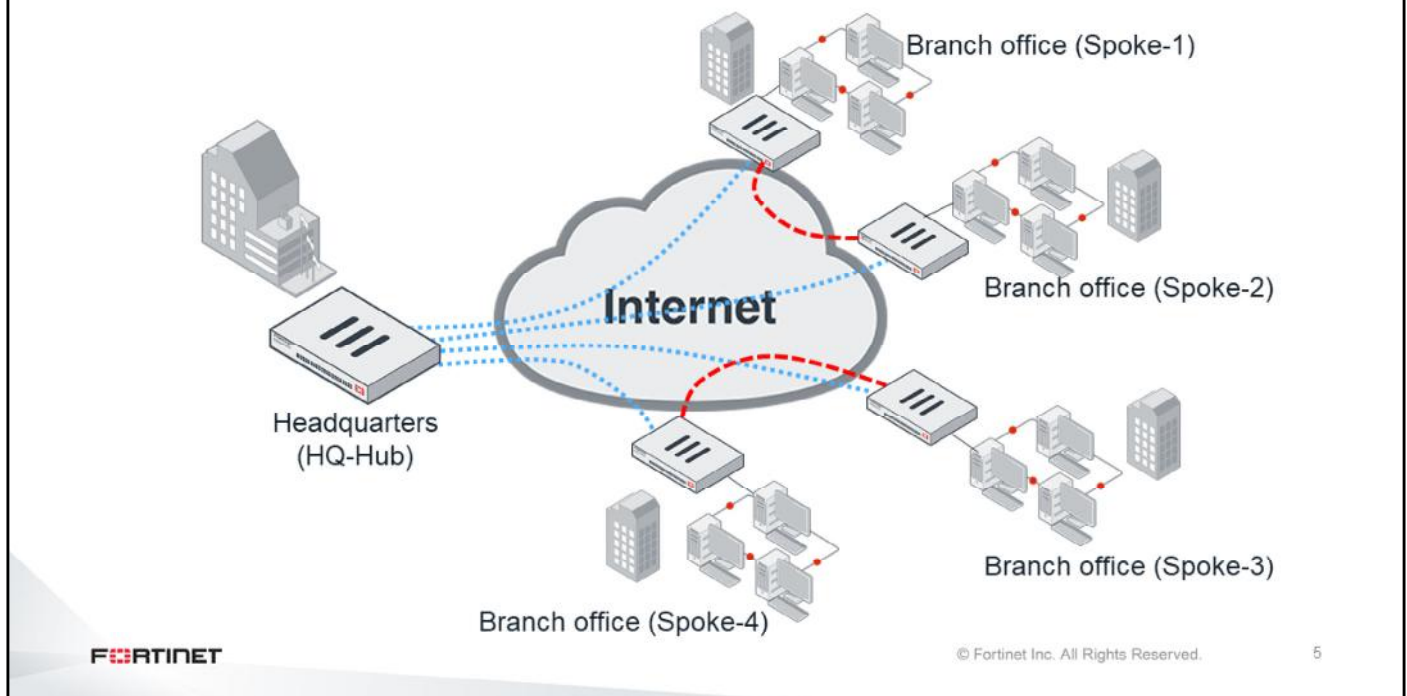
In the example shown on this slide, each client—*spoke*—is a branch-office FortiGate. For any branch office to reach another branch office, its traffic must pass through the hub.

One advantage of using this topology is that you can easily manage the VPN configuration and firewall policies. Also, system requirements are minimal for the FortiGate devices that function as branch offices, because each FortiGate must maintain only one tunnel, or two SAs. In this example, four tunnels, or eight security associations (SAs), are necessary in the hub.

A disadvantage of using this topology is that communication between branch offices through headquarters (HQ) is slower than it would be using a direct connection, especially if HQ is physically distant, as it can be for global companies. For example, if your company's HQ is in Brazil, and your company also has offices in Japan and Germany, latency can be significant. Another disadvantage is lack of redundancy. For example, if FortiGate at HQ fails, the VPN fails company-wide. Also, FortiGate at HQ must be more powerful, because it handles four tunnels simultaneously, or eight SAs.

DO NOT REPRINT
© FORTINET

Partial Mesh Topology

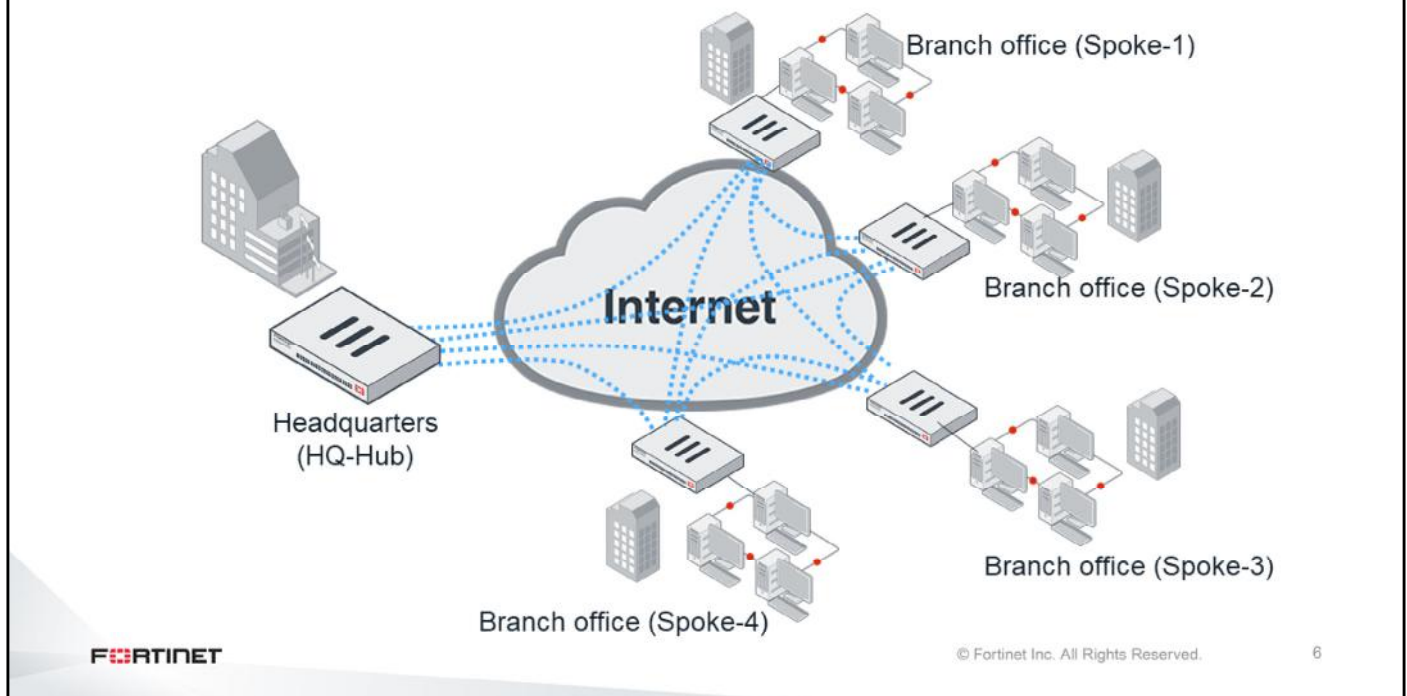


This slide shows a VPN that has a partial mesh topology. There are two types of mesh topologies, partial mesh and full mesh.

Partial mesh attempts to compromise, minimizing required resources as well as latency. Partial mesh can be appropriate if communication is not required between every location. This slide shows additional connections between Spoke-1 and Spoke-2 and, Spoke-3 and Spoke-4 connections. However, each FortiGate's configuration is still more complex than hub-and-spoke. Routing, especially, may require extensive planning.

DO NOT REPRINT
© FORTINET

Full Mesh Topology



This slide shows a VPN that has a full mesh topology.

Full mesh connects every location to every other location. Like the previous hub-and-spoke example, the example on this slide shows only five locations. In order to fully interconnect, each FortiGate needs four VPN tunnels, or eight SAs, to the other FortiGate devices. This equals three more tunnels for each spoke FortiGate. In total, 10 tunnels are needed. If your company were to expand to six locations, it would require 15 tunnels. Seven locations would need 21 tunnels, and so on. You can use the formula $N \text{ sites} = N (N-1) / 2$ to calculate the number of tunnels. This topology causes less latency and requires much less HQ bandwidth than hub-and-spoke. Its disadvantages? Every spoke FortiGate must be more powerful. Additionally, both administration and troubleshooting get more complicated.

So, in general, if your company has many locations, hub-and-spoke will be cheaper, but slower, than a mesh topology. Mesh topologies place less strain on the central location and can be more fault-tolerant, but are also more expensive.

DO NOT REPRINT
© FORTINET

Fortinet ADVPN

- ADVPN is a proprietary solution based on IKE and IPsec
- Provides direct connectivity between all sites by creating on-demand tunnels between spokes
 - Benefit of full-mesh topology while providing scalability with minimum configuration
- Spoke-to-spoke traffic no longer needs to flow through the hub

FORTINET

© Fortinet Inc. All Rights Reserved.

7

ADVPN was introduced in FortiOS 5.4. It combines the benefits of hub-and-spoke and full-mesh topologies because all the spoke-to-spoke tunnels are dynamically created on demand. After a shortcut tunnel is established between two spokes and routing has converged, spoke-to-spoke traffic no longer needs to flow through the hub. ADVPN provides direct connectivity.

DO NOT REPRINT
© FORTINET

ADVPN

- Supports multiple hub-and-spoke architecture
- Supports NAT for on-demand tunnels
- Requires use of dynamic routing
 - BGP, OSPF, and RIPv2/RIPng are supported
 - PIM/multicast is supported
- Supports both IPv4 and IPv6

FORTINET

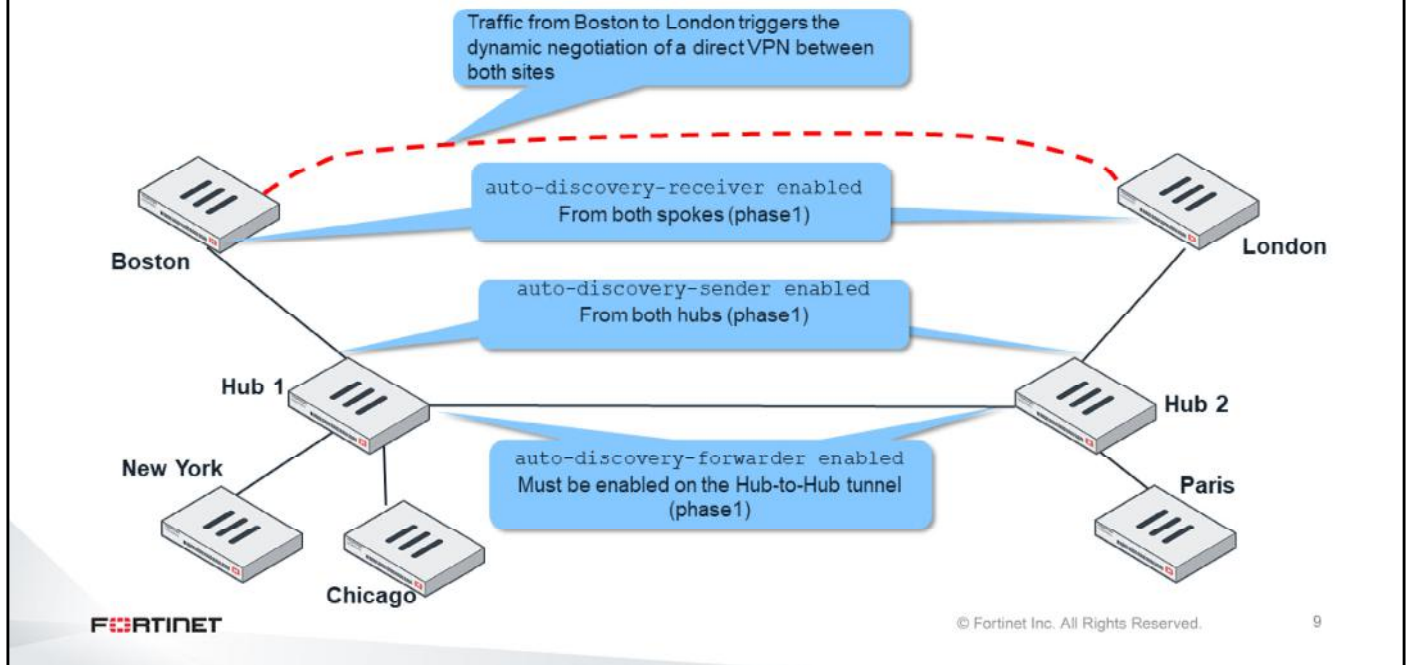
© Fortinet Inc. All Rights Reserved.

8

- ADVPN supports single or multiple hub architectures
- NAT is supported for the on-demand tunnels
- ADVPN requires the use of a routing protocol. Currently, it supports BGP, OSPF and RIPv2/RIPng. It also supports PIM and multicast.
- Both IPv4 and IPv6 are supported

DO NOT REPRINT
© FORTINET

ADVPN Configuration and Example (Dual Regions)



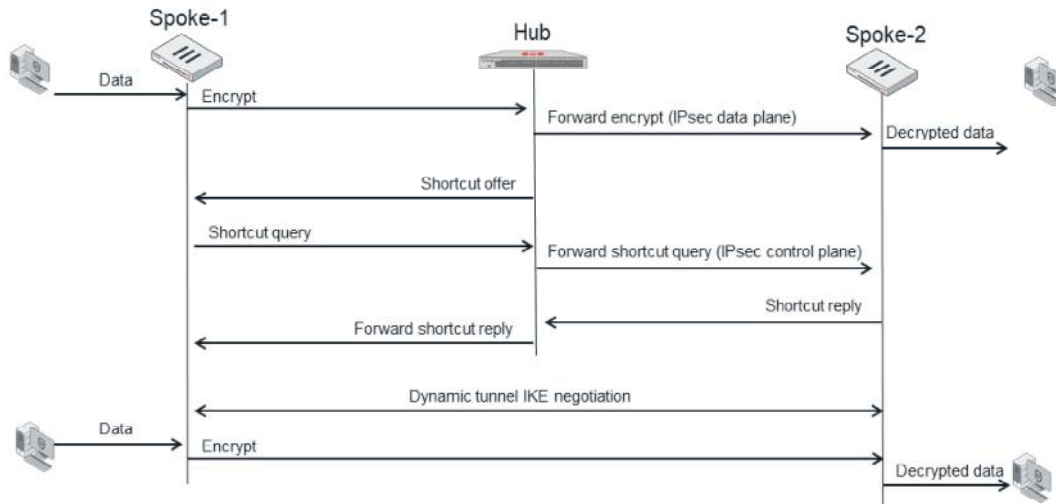
This slide shows an example of how ADVPN works.

An administrator configures IPsec VPNs in multiple FortiGate devices to form VPN hub-and-spoke topologies. In this example, there are two hubs. Hub 1 has three spokes. Hub 2 has two spokes. There is also a VPN connecting both hubs.

The dynamic tunnels between spokes are created on demand. Say that a user in Boston sends traffic to London. Initially, the direct tunnel between Boston and London has not been negotiated. So, the first packets from Boston to London are routed through Hub 1 and Hub 2. When Hub 1 receives those packets, it knows that ADVPN is enabled in all the VPNs all the way to London because of `auto-discovery-sender enable` settings. So, Hub 1 sends an IKE message to Boston informing it that it can try to negotiate a direct connection to London. On receipt of this IKE message, Boston creates a FortiOS-specific IKE information message that contains its public IP address, its local subnet, the desired destination subnet (London's subnet), and an auto-generated PSK (alternatively can also use digital certificate authentication). This IKE message is sent to London through Hub 1 and Hub 2. When London receives the IKE message from Boston, it stores the PSK and replies with another IKE information message that contains London's public IP address. After the reply arrives in Boston, the dynamic tunnel is negotiated between both peers. The negotiation succeeds because London is expecting a connection attempt from Boston's public IP address. You will explore this in greater detail in the next few slides.

DO NOT REPRINT
© FORTINET

ADVPN Message Exchange



FORTINET

© Fortinet Inc. All Rights Reserved.

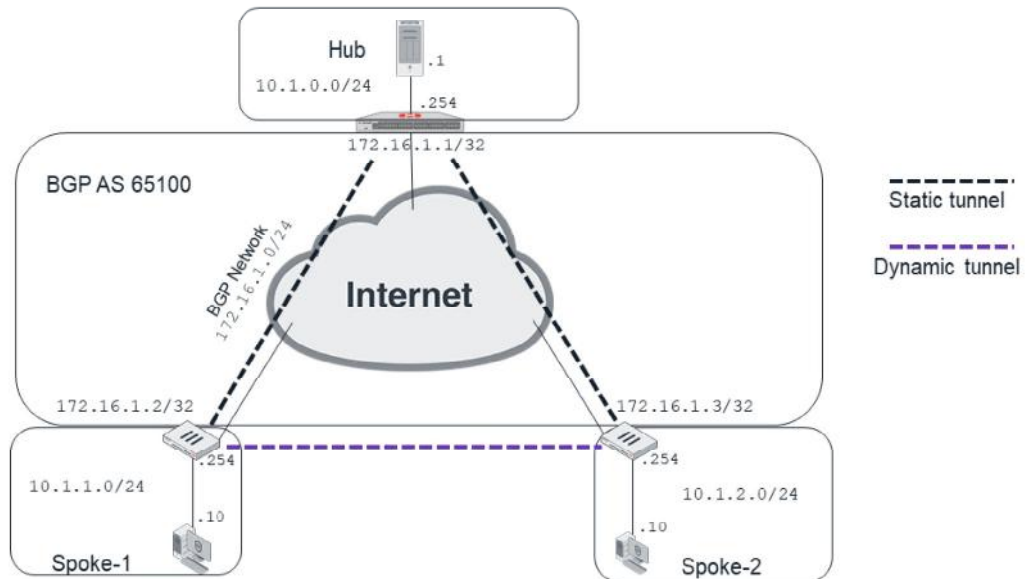
10

Now, you will examine the IKE messages that are exchanged when an on-demand tunnel is being negotiated:

1. The client behind Spoke-1 generates traffic for devices located on Spoke-2's network.
2. Spoke-1 receives the packet, encrypts it, and sends it to the Hub.
3. The Hub receives the packet from Spoke-1 and forwards it to Spoke-2.
4. Spoke-2 receives the packet, decrypts it, and forwards it to the destination device.
5. The Hub knows that a more direct tunnel option might be available from Spoke-1 to Spoke-2. The Hub sends a shortcut offer message to Spoke-1.
6. Spoke-1 acknowledges the shortcut offer by sending a shortcut query to the Hub.
7. The Hub forwards the shortcut query message to Spoke-2.
8. Spoke-2 acknowledges the shortcut query and sends a shortcut reply to the Hub.
9. The Hub forwards the shortcut reply to Spoke-1.
10. Spoke-1 and Spoke-2 initiate the tunnel IKE negotiation.

DO NOT REPRINT
© FORTINET

Example of an IBGP Topology for ADVPN



FORTINET

© Fortinet Inc. All Rights Reserved.

11

As mentioned earlier, ADVPN requires the use of a dynamic routing protocol. In the next slides, you will learn how to configure ADVPN with IBGP.

As an example, you will use an IBGP topology made up of one hub with two spokes. All the devices are in the AS 65100.

DO NOT REPRINT
© FORTINET

Hub ADVPN Configuration

```
Hub # config vpn ipsec phase1-interface
```

```
edit "H2S_0"
```

```
set type dynamic
```

```
set interface "port1"
```

```
set proposal aes128-sha1
```

```
set net-device disable
```

```
set add-route disable
```

```
set tunnel-search nexthop
```

```
...
```

```
set auto-discovery-sender enable
```

```
set psksecret ENC ...
```

```
next
```

```
end
```

```
config vpn ipsec phase2-interface
```

```
edit "H2S_0"
```

```
set phase1name "H2S_0"
```

```
set proposal aes128-sha1
```

```
next
```

```
end
```

Dynamic routing is used for learning the spokes' protected subnets

Decides which tunnel the packet must be sent on

Enables ADVPN

The mask for the local IP can only be /32 so, the mask for the overlay subnet must be specified in remote-ip

```
Hub # show sys interface | grep -f H2S_0
```

```
config system interface
```

```
edit "H2S_0" <---
```

```
set vdom "root"
```

```
set ip 172.16.1.1 255.255.255.255
```

```
set allowaccess ping
```

```
set type tunnel
```

```
set remote-ip 172.16.1.254/24
```

```
set snmp-index 34
```

```
set interface "port1"
```

```
next
```

```
end
```

Assign a remote dummy IP (overlay IP and subnet)

FORTINET

© Fortinet Inc. All Rights Reserved.

12

This slide shows the following ADVPN configuration in the hub:

- Disable `set add-route` to ensure that dynamic routing is used for learning the spokes' protected subnets.
- Set `tunnel-search` to `nexthop`, to ensure the next-hop IP of the route matched by a packet is used to decide into which tunnel the packet must be sent.
- Disable `set net-device` to ensure FortiGate does not create dynamic interface.
- You must enable `set auto-discovery-sender` if you want ADVPN. This setting indicates that when IPsec traffic transits the hub, it should send a shortcut offer to the initiator of the traffic to indicate that it could perhaps establish a more direct connection (shortcut).
- Assign an overlay IP address to the IPsec virtual interface. This is a requirement for having a dynamic routing protocol over IPsec.
- The overlay IPs of all hub-and-spoke participants are in the same subnet.
- For the `remote-ip`, you can use an unused IP from the overlay subnet. You will need to add the appropriate subnet based on the number of hub and spokes.
- For the phase 2 configuration, ensure that quick modes are set to all `(0.0.0.0/0.0.0.0)`.
- Set a firewall policy to allow the traffic from the spokes to the hub, from the hub to the spokes, and between spokes through the hub.

DO NOT REPRINT
© FORTINET

Spoke ADVPN Configuration

```
Spoke-1 # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
  edit "H2S_0"
    set interface "port1"
    set proposal aes128-shal
    set auto-discovery-receiver enable
    set net-device enable
    set psksecret ENC ...
  next
end
```

Enables ADVPN

```
config vpn ipsec phase2-interface
  edit "H2S_0"
    set phase1name "H2S_0"
    set proposal aes128-shal
  next
end
```

```
Spoke-1 # show sys interface
config system interface
...
  edit "H2S_0"
    set vdom "root"
    set ip 172.16.1.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 172.16.1.1/24
    set snmp-index 33
    set interface "port1"
  next
end
```

Hub overlay IP with
/24

FORTINET

© Fortinet Inc. All Rights Reserved.

13

This slide shows the following ADVPN configuration in a spoke:

- Enable ADVPN with the command `auto-discovery-receiver`. Use this command to indicate that this IPsec tunnel wants to participate in an autodiscovery VPN (that is, receive a SHORTCUT-OFFER).
- Assign an interface IP, remote IP, and subnet to the IPsec virtual interface.

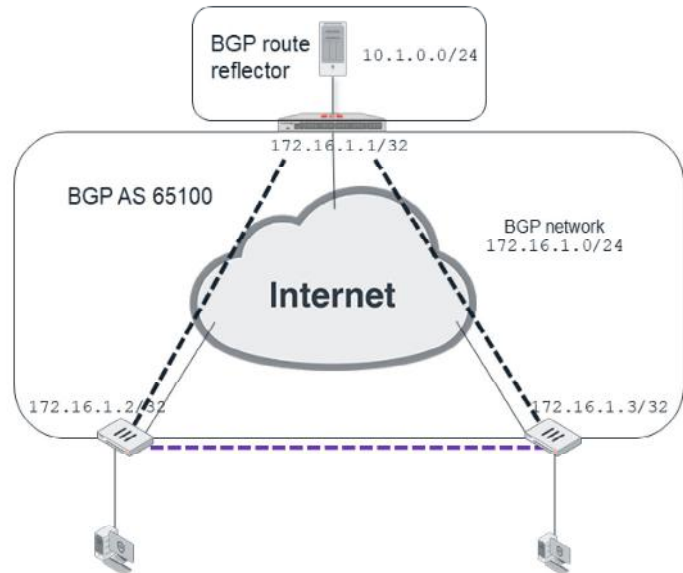
DO NOT REPRINT
© FORTINET

Hub IBGP Configuration

```

Hub # show router bgp
config router bgp
  set as 65100
  set router-id 172.16.1.1
  config neighbor-group
    edit "advpn"
      set remote-as 65100
      set route-reflector-client enable
    next
  end
  config neighbor-range
    edit 1
      set prefix 172.16.1.0 255.255.255.0
      set neighbor-group "advpn"
    next
  end
  config network
    edit 1
      set prefix 10.1.0.0 255.255.255.0
    next
  end
...
end

```



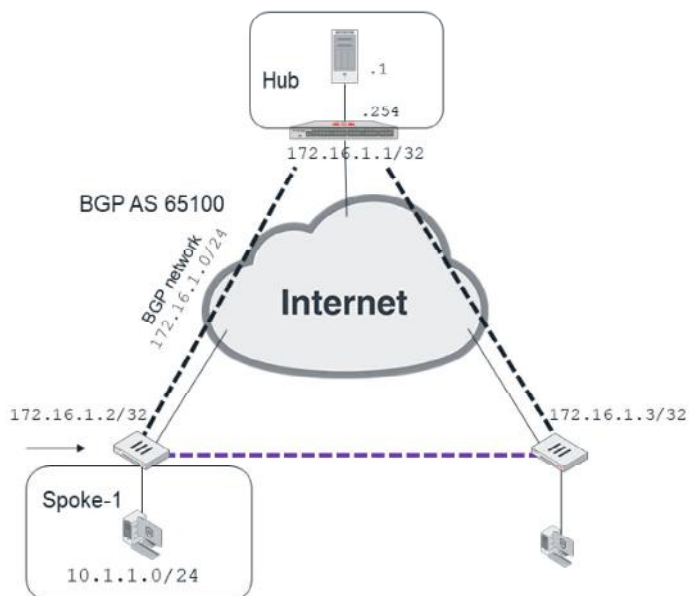
This slide shows the following IBGP configuration in the hub:

- Configure a BGP neighbor group. All the spokes are part of it.
- Create a neighbor range with a prefix that includes all the spokes. In this way, you don't need to define each spoke individually as a neighbor.
- If you are using IBGP for ADVPN, you must configure the hub as a route reflector. So, routes learned from one spoke are forwarded to the other spokes.
- Add the local network(s) behind the hub to be advertised over BGP.

DO NOT REPRINT
© FORTINET

Spoke IBGP Configuration

```
Spoke-1 # show router bgp
config router bgp
  set as 65100
  set router-id 172.16.1.2
  config neighbor
    edit "172.16.1.1"
      set remote-as 65100
    next
  end
  config network
    edit 1
      set prefix 10.1.1.0 255.255.255.0
    next
  end
...
end
```



FORTINET

© Fortinet Inc. All Rights Reserved.

15

This slide shows the following IBGP configuration in one of the spokes:

- Configure the hub as a BGP neighbor
- Define the internal network that will be advertised over the BGP

DO NOT REPRINT
© FORTINET

ADVPN and FortiManager VPN Manager

- Some settings need to be changed from their default values:
 - Set protected networks to **all**
 - Enable ADVPN in the IPsec phase 1
 - Use a script
 - Ensure that the **Add Route** option is disabled on the hub
 - Enable `net-device` on spokes
 - Use a script
 - Configure IP addresses on the IPsec virtual interfaces
 - Configure dynamic routing
 - Use a script to enable route reflector if using IBGP
 - Phase1 name_0
 - FortiManager creates phase1 name_0 interface when using VPN console

FORTINET

© Fortinet Inc. All Rights Reserved.

16

If you are configuring ADVPN on FortiManager using the VPN manager, remember the following:

- Set the protected networks to **all**
- Use scripts to enable ADVPN in phase 1
- Disable the option **Add Route** on the hub
- Use scripts to enable `net-device` on spokes
- Configure IP addresses on the IPsec virtual interfaces
- Configure dynamic routing. If you are using IBGP, use a script to enable route reflector on the hub.
- It is important to know that when creating phase-1 using a FortiManager VPN console, the phase-1 name is created with an underscore and a zero (phase1name_0). For example, a phase-1 named VPN will be created as VPN_0.

DO NOT REPRINT
© FORTINET

VPN Manager—ADVPN

- Change the address object for **Protected Subnet** to **all**:

The screenshot shows the Fortinet VPN Manager interface. The top navigation bar includes 'VPN Manager', 'IPsec VPN', 'Monitor', 'Map View', and 'SSL VPN'. The user is logged in as 'admin'. The left sidebar shows 'All VPN Communities' with 'H2S' selected. The main panel displays the configuration for the 'H2S' community, including a 'Dial up' icon and details for Name, Number of VPN, Authentication, and Security Properties. Below this is a table with columns: Name, Role, Default VPN Interface, and Protected Subnet. The 'Protected Subnet' column is highlighted with a red box, showing the value 'all' for all three entries: NGFW-1[root], Spoke-1[root], and Spoke-2[root].

Name	Role	Default VPN Interface	Protected Subnet
NGFW-1[root]	Hub	external	all
Spoke-1[root]	Spoke	external	all
Spoke-2[root]	Spoke	external	all

The configuration of the **Protected Subnet** is under **All VPN Communities**.

DO NOT REPRINT
© FORTINET

VPN Manager—ADVPN (Contd)

- Turn off the **Add Route** switch on the hub device:

The screenshot shows the VPN Manager configuration interface for ADVPN. The 'Add Route' switch is highlighted with a red box and is set to 'OFF'. Other visible settings include:

- XAUTH Type:** ☒ Disable, ☐ PAP Server, ☐ CHAP Server, ☐ AUTO Server
- Enable IKE Configuration Method ("mode config"):** ☐ OFF
- DHCP Server:** ☐ OFF
- Default Gateway:** 0.0.0.0
- DNS Service:** ☒ Use System DNS Setting, ☐ Specify
- Netmask:** 255.255.255.255
- IPsec Lease Hold:** 60
- Auto-Configuration:** ☐ OFF
- DHCP Server IP Range:** Table with columns Seq#, Start IP, End IP. Below the table is a link: Click here to add a new entry.
- Add Route:** ☒ OFF (highlighted with a red box)
- Exclusive IP Range:** Table with columns Seq#, Start IP, End IP. Below the table is a link: Click here to add a new entry.
- Advanced Options >**

FORTINET

© Fortinet Inc. All Rights Reserved.

18

For ADVPN, turn off the **Add Route** switch under the VPN gateway configuration of the hub.

This prevents the hub from adding routes based on IKE negotiations. For that purpose, ADVPN uses a dynamic routing protocol instead.

DO NOT REPRINT
© FORTINET

Spoke Routing Table Before On-Demand Tunnel

```
Spoke-1 # get router info bgp network
BGP table version is 13, local router ID is 172.16.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i0.0.0.0/0	172.16.1.1	0	100	0	0 100 i
*>i10.1.0.0/24	172.16.1.1	0	100	0	0 i
*> 10.1.1.0/24	0.0.0.0	100	32768		0 i
*>i10.1.2.0/24	172.16.1.3	0	100	0	0 i

BGP next-hop must be accessible through tunnel

```
Spoke-1 # get router info routing-table all
S* 0.0.0.0/0 [10/0] via 100.64.3.254, port1
B 10.1.0.0/24 [200/0] via 172.16.1.1, H2S_0, 13:02:21
C 10.1.1.0/24 is directly connected, port3
B 10.1.2.0/24 [200/0] via 172.16.1.3, H2S_0, 00:00:30
C 100.64.3.0/24 is directly connected, port1
C 100.64.4.0/24 is directly connected, port2
C 172.16.1.0/24 is directly connected, H2S_0
C 172.16.1.2/32 is directly connected, H2S_0
```

Spoke-to-spoke traffic flows through the hub

FORTINET

© Fortinet Inc. All Rights Reserved.

19

After the tunnels between the hub and the spokes come up, you can run the commands, shown on this slide, on the spokes to verify that routing updates are taking place:

This slide shows that Spoke-1 learned the routes to the hubs and to the networks of Spoke-2, through BGP. Spoke-2 is currently accessible through the hub.

DO NOT REPRINT
© FORTINET

IKE Real-Time Debug of ADVPN

- Can specify multiple IP addresses to filter the IKE real-time debug
 - Useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations

```
diag debug console timestamp enable
diag vpn ike log filter clear
diag vpn ike log filter mdst-addr4 <ip.of.Hub> <ip.of.Spoke>
diag debug application ike -1
diag debug enable
```

You can specify multiple IP addresses when debugging IKE. This is very useful when debugging ADVPN shortcuts and spoke-to-spoke ADVPN negotiation issues.

DO NOT REPRINT
© FORTINET

ADVPN Debug

Spoke-1

```
ike 0:H2S_0:4: notify msg received: SHORTCUT-OFFER
ike 0:H2S_0: shortcut-offer 10.1.1.254->10.1.2.254 psk 64 ppk 0 ver 1 mode 0
ike 0 looking up shortcut by addr 10.1.2.254, name H2S_0
```

Spoke-1 receives an OFFER from the hub caused by data traffic from 10.1.1.254 to 10.1.2.254

```
ike 0:H2S_0: send shortcut-query 289635615481843711
ce3375c4c7fb498f/000000000000000000 100.64.3.1 10.1.1.254->10.1.2.254 psk
64 ttl 32 nat 0 ver 1 mode 0
```

Spoke-1 sends a QUERY

Hub

```
ike 0:H2S_0_0:2: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_0: recv shortcut-query 289635615481843711 ce3375c4c7fb498f/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 15 10.1.1.254->10.1.2.254 route lookup oif 15
ike 0:H2S_0_1: forward shortcut-query 289635615481843711 ce3375c4c7fb498f/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 ver 1 mode 0, ext-mapping
100.64.3.1:500
```

Hub receives this QUERY and forwards it to Spoke-2

FORTINET

© Fortinet Inc. All Rights Reserved.

21

If you run the IKE real-time debug during the negotiation of an ADVPN tunnel, you will see the exchange of all shortcuts. This slide shows an example of the output of the real-time debug. You can see the Spoke-1 receives a OFFER from the Hub because of the data traffic from Spoke-1 to Spoke-2.

Spoke-1 sends a shortcut-query to Spoke-2 and the Hub receives this shortcut-query and forwards it to Spoke-2.

DO NOT REPRINT
© FORTINET

ADVPN Debug (Contd)

Spoke-2

```
ike 0:H2S_0:4: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0: recv shortcut-query 289635615481843711 ce3375c4c7fb498f/0000000000000000 100.64.3.1
10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 nat 0 ver 1 mode 0

send shortcut-reply 289635615481843711 ce3375c4c7fb498f/c7b1befb2d4a30d4 100.64.5.1 to 10.1.1.254
psk 64 ppk 0 ver 1 mode 0
```

Hub

```
ike 0:H2S_0_1:3: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_1: recv shortcut-reply 289635615481843711 ce3375c4c7fb498f/c7b1befb2d4a30d4 100.64.5.1
to 10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.3.1:500
ike 0:H2S_0: iif 15 10.1.2.254->10.1.1.254 route lookup oif
ike 0:H2S_0_0: forward shortcut-reply 289635615481843711 ce3375c4c7fb498f/c7b1befb2d4a30d4
100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31 ver 1 mode 0 ext-mapping 100.64.5.1:500
```

Spoke-2 receives the QUERY and
REPLY to Spoke-1

Hub receives the REPLY and
forwards it to Spoke-1

FORTINET

© Fortinet Inc. All Rights Reserved.

22

In the example shown on this slide, Spoke-2 receives the `shortcut-query` and sends a `shortcut-reply` to Spoke-1.

Hub receives the `shortcut-reply` and forwards it to Spoke-1.

DO NOT REPRINT
© FORTINET

ADVPN Debug (Contd)

Spoke-1

```
ike 0:H2S_0:4: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0: rcv shortcut-reply 289635615481843711 ce3375c4c7fb498f/c7b1befb2d4a30d4 100.64.5.1 to
10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.5.1:500
ike 0:H2S_0: iif 15 10.1.2.254->10.1.1.254 route lookup oif 13
ike 0:H2S_0: shortcut-reply received from 100.64.5.1:500, local-nat=no, peer-nat=no
ike 0:H2S_0: created connection: 0xd7997b0 3 100.64.3.1->100.64.5.1:500.
ike 0:H2S_0: adding new dynamic tunnel for 100.64.5.1:500
ike 0:H2S_0: added new dynamic tunnel for 100.64.5.1:500
```

Spoke-1 receives the REPLY and initiates a shortcut negotiation directly with Spoke-2

Dynamic tunnel created between the spokes

FORTINET

© Fortinet Inc. All Rights Reserved.

23

Finally, Spoke-1 receives the reply message and initiates a shortcut negotiation directly with Spoke-2, and the dynamic tunnel interface is created.

DO NOT REPRINT
© FORTINET

ADVPN Tunnels

- IPsec tunnel list on Spoke-1

Spoke-1 # get ipsec tunnel list

NAME	REMOTE-GW	PROXY-ID-SOURCE	PROXY-ID-DESTINATION	STATUS	TIMEOUT
H2S_0	100.64.1.1:0	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	up	2860
H2S_0_0	100.64.5.1:0	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	up	33072

- IPsec tunnel list on Spoke-2

Spoke-2 # get ipsec tunnel list

NAME	REMOTE-GW	PROXY-ID-SOURCE	PROXY-ID-DESTINATION	STATUS	TIMEOUT
H2S_0	100.64.1.1:0	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	up	5807
H2S_0_0	100.64.3.1:0	0.0.0.0/255.255.255.255	0.0.0.0/255.255.255.255	up	32064

On-demand tunnel
H2S_0_0

FORTINET

© Fortinet Inc. All Rights Reserved.

24

Using the `get ipsec tunnel list` command, you can verify which on-demand tunnels are up. It is important to note that on-demand tunnels remain active until their SAs are manually flushed, or until they time out.

DO NOT REPRINT
© FORTINET

Spoke Routing Table After On-Demand Tunnel

```
Spoke-1 # get router info bgp network
BGP table version is 2, local router ID is 172.16.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop          Metric LocPrf Weight RouteTag Path
*>i0.0.0.0/0       172.16.1.1             0    100      0         0 100 i
*>i10.1.0.0/24     172.16.1.1             0    100      0         0 i
*> 10.1.1.0/24     0.0.0.0                100   32768      0         0 i
*>i10.1.2.0/24     172.16.1.3             0    100      0         0 i
```

Total number of prefixes 5

```
Spoke-1 # get router info routing-table all
```

```
.
S* 0.0.0.0/0 [10/0] via 100.64.3.254, port1
B 10.1.0.0/24 [200/0] via 172.16.1.1, H2S_0, 12:47:47
C 10.1.1.0/24 is directly connected, port3
B 10.1.2.0/24 [200/0] via 172.16.1.3, H2S_0_0, 12:41:56
B 10.1.4.0/24 [200/0] via 172.16.1.1, H2S_0, 12:24:43
C 100.64.3.0/24 is directly connected, port1
C 172.16.1.0/24 is directly connected, H2S_0
C 172.16.1.2/32 is directly connected, H2S_0
C 172.16.1.3/32 is directly connected, H2S_0_0
C 172.16.1.3/32 is directly connected, H2S_0_0
```

Spoke-2 network is now available
through on-demand tunnel

Spoke-2 is now directly connected

FORTINET

© Fortinet Inc. All Rights Reserved.

25

This slide shows the routing table after the on-demand tunnel is up.

You can confirm that the network of Spoke-2 is directly accessible using the on-demand tunnel: H2S_0_0.

DO NOT REPRINT
© FORTINET

Review

- ✓ Configure ADVPN
- ✓ Troubleshoot ADVPN

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

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

DO NOT REPRINT
© FORTINET

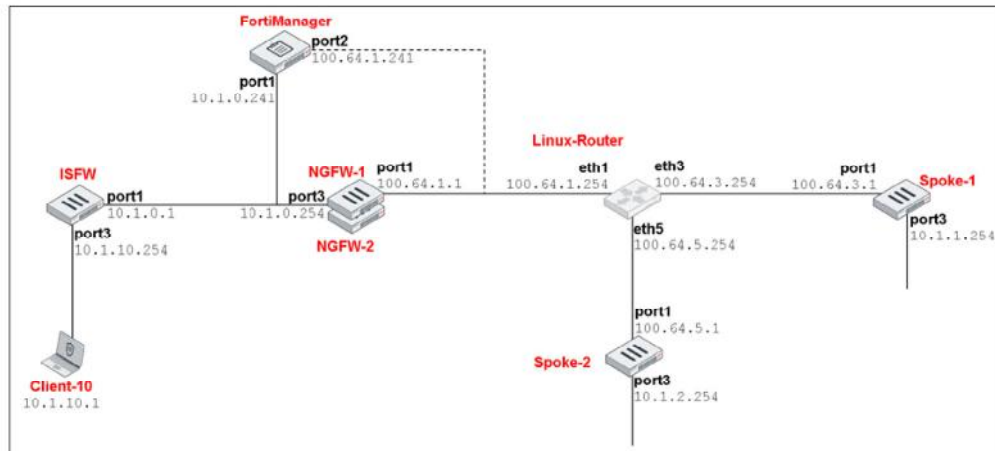
Lab 13—ADVPN

Now, you will work on *Lab 13—ADVPN*.

DO NOT REPRINT
© FORTINET

Lab 13—ADVPN

- On each FortiGate:
 - Enable ADVPN
 - Assign an IP address to the IPsec interface
 - Configure IBGP with route reflector



FORTINET

© Fortinet Inc. All Rights Reserved.

28

In this lab, you will run CLI and TCL scripts to configure ADVPN and IBGP on the three FortiGate devices.

© Fortinet Inc. All Rights Reserved.

This slide shows your IBGP network, including router IDs and the IP addresses used in the IPsec interfaces.

DO NOT REPRINT
© FORTINET

Lab 13—NGFW Script

```
config vpn ipsec phase1-interface
edit "H2S_0"
set net-device disable
set tunnel-search nexthop
set auto-discovery-sender enable
set add-route disable
next
end
```

```
config system interface
edit "H2S_0"
set vdom "root"
set ip 172.16.1.1 255.255.255.255
set remote-ip 172.16.1.254/24
next
end
```

```
config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor-group
edit "advpn"
set remote-as 65100
set next-hop-self enable
set route-reflector-client enable
next
end
config neighbor-range
edit 1
set prefix 172.16.1.0 255.255.255.0
set neighbor-group "advpn"
next
end
config network
edit 1
set prefix 10.1.0.0 255.255.255.0
next
```

FORTINET

© Fortinet Inc. All Rights Reserved.

30

This slide shows the CLI script that configures the NGFW with ADVPN and IBGP. The first part enables ADVPN. The second part configures the IP address in the IPsec interface. The last part configures IBGP with route-reflector-client enabled.

DO NOT REPRINT
© FORTINET

Lab 13—Spokes Script

```
# Procedure for executing CLI commands
proc do_cmd {cmd} {
  puts [exec "$cmd\n" "# " 15]
}
```

```
# Extract the hostname
set query [exec "get system status | grep Hostname\n" "# "]
set pos [lsearch $query "*Spoke*"]
set hostname [lindex $query $pos]
```

```
# Extract the spoke number from the hostname
set len [string length $hostname]
set pos2 [expr [string last - $hostname] + 1]
set spokenum [string range $hostname $pos2 $len]
set spokenumplusone [expr $spokenum + 1]
```

FORTINET

© Fortinet Inc. All Rights Reserved.

31

Configuration is slightly different from one spoke to another, so you will use TCL to create a single script that can run on all the spokes, and configure each spoke individually. What changes from one spoke to another is the router ID, the prefix to advertise, and the IP address in the IPsec interface. The script derives those items from the spoke hostname.

The first part of the CLI script shown on this slide defines a function that is called each time a CLI command needs to be run. This simplifies the TCL script.

The second part extracts the hostname from the output of the command `get system status`.

The third part extracts the spoke number from the hostname. For example, Spoke-1 is the spoke number 1, Spoke-10 is the spoke number 10, and so on.

Two variables are created:

- `$spokenum` is the spoke number. It is used to set the prefix to advertise.
- `$spokenumplusone` is the spoke number plus 1. It is used to set the router ID and IPsec interface IP address.

DO NOT REPRINT
© FORTINET

Lab 13—Spokes Script

```
# Enable ADVPN
do_cmd "config vpn ipsec phase1-interface"
do_cmd "edit H2S_0"
do_cmd "set auto-discovery-receiver enable"
do_cmd "next"
do_cmd "end"
```

```
# Configure IP address in the IPsec interface
do_cmd "config system interface"
do_cmd "edit H2S_0"
do_cmd "set ip 172.16.1.$spokenumberplusone 255.255.255.255"
do_cmd "set remote-ip 172.16.1.1/24"
do_cmd "next"
do_cmd "end"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

32

Next, the TCI script enables ADVPN. After that, it configures the IPsec interface IP address: for example, 172.16.1.2 for Spoke-1, 172.16.1.11 for Spoke-10, and so on. It uses the variable \$spokenumberplusone.

DO NOT REPRINT
© FORTINET

Lab 13—Spokes Script

```
# Configure BGP
do_cmd "config router bgp"
do_cmd "set as 65100"
do_cmd "set router-id 172.16.1.$spokenumberplusone"
do_cmd "config neighbor"
do_cmd "edit 172.16.1.1"
do_cmd "set remote-as 65100"
do_cmd "next"
do_cmd "end"
do_cmd "config network"
do_cmd "edit 1"
do_cmd "set prefix 10.1.$spokenumber.0 255.255.255.0"
do_cmd "next"
do_cmd "end"
do_cmd "end"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

33

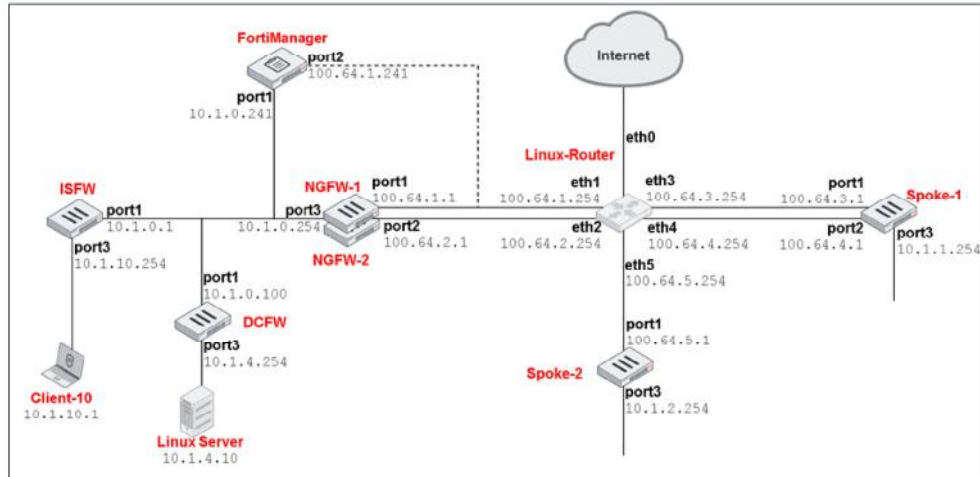
Finally, the TCL configures BGP. For example, the router ID for Spoke-1 is 172.16.1.2, for Spoke-7 is 172.16.1.8, and so on. The script uses the variable `$spokenumberplusone` again.

In the case of the BGP prefix, Spoke-1 advertises 10.1.1.0/24, Spoke-5 advertises 10.1.5.0/24, and so on. The script uses the variable `$spokenumber`.

DO NOT REPRINT
© FORTINET

Lab 13

- Troubleshooting:
 - Why can't a client behind Spoke-1 reach the Linux server?



FORTINET

© Fortinet Inc. All Rights Reserved.

34

Additionally, you will troubleshoot a routing problem with OSPF and BGP.

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the troubleshooting exercises.

DO NOT REPRINT
© FORTINET

Lab 3—Traffic and Session Monitoring

Now, we will look at the solutions for the troubleshooting exercise in the traffic and session monitoring lab.

DO NOT REPRINT
© FORTINET

Problems to Troubleshoot

- There were four problems:
 - Unable to telnet to ISFW (10.1.10.254)
 - Client-10 unable to access the web server on 10.1.4.10
 - No Internet access
 - Unable to telnet to Linux-Router (100.64.1.254)

FORTINET

© Fortinet Inc. All Rights Reserved.

3

There were four problems:

- Unable to telnet to ISFW (10.1.10.254)
- Client-10 was unable to access the web server at 10.1.4.10
- No Internet access
- Unable to telnet to Linux-Router (100.64.1.254)

DO NOT REPRINT
© FORTINET

Problem 1: Telnet Access to ISFW

```
ISFW # diagnose sniffer packet any "port 23 and host 10.1.10.1" 4  
interfaces=[any]  
filters=[port 23 and host 10.1.10.1]  
6.252157 port3 in 10.1.10.1.53567 -> 10.1.10.254.23: syn 3438661631  
9.255609 port3 in 10.1.10.1.53567 -> 10.1.10.254.23: syn 3438661631
```

FORTINET

© Fortinet Inc. All Rights Reserved.

4

In the first problem, packets were arriving to ISFW as verified with the sniffer command. However ISFW was not replying with the SYN/ACK packets.

DO NOT REPRINT
© FORTINET

Problem 1: Telnet Access to ISFW

```
ISFW # diagnose debug flow filter dport 23
ISFW # diagnose debug flow trace start 10
ISFW # diagnose debug enable

id=20085 trace_id=4 func=print_pkt_detail line=4784 msg="vd-root received a
packet(proto=6, 10.1.10.1:53539->10.1.10.254:23) from port3. flag [S], seq
4051836222, ack 0, win 8192"
id=20085 trace_id=4 func=init_ip_session_common line=4935 msg="allocate a new
session-0000d277"
id=20085 trace_id=4 func=vf_ip_route_input_common line=2584 msg="find a route:
flag=84000000 gw=10.1.10.254 via root"
id=20085 trace_id=4 func=fw_local_in_handler line=387 msg="iprope_in_check()
check failed on policy 1, drop"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

5

The next step was to use the debug flow, which showed the error `iprope_in_check()` check failed on policy 1, drop. As this is FortiGate management traffic, the problem could be one of the following:

- The telnet service was not enabled in port3
- The telnet service was using a different port
- The source IP address was not in the trusted host list
- There was a local-in firewall configured to block telnet traffic

DO NOT REPRINT
© FORTINET

Problem 1: Telnet Access to ISFW

- Solution:

- Delete the local-in policy configured to deny telnet requests to the unit.

```
ISFW (local-in-policy) # show firewall local-in-policy
config firewall local-in-policy
    edit 1
        set intf "port3"
        set srcaddr "10.1.10."
        set dstaddr "all"
        set service "TELNET"
        set schedule "always"
    ...
ISFW # config firewall local-in-policy
ISFW (local-in-policy) # delete 1
ISFW (local-in-policy) # end
```

Note: User created local-in policies are not displayed on the GUI. You can only view them on the CLI.

FORTINET

© Fortinet Inc. All Rights Reserved.

6

The problem was actually a local-in policy blocking the telnet traffic. Removing that policy fixed the problem.

If you tried to view the local-in policy on the GUI, you wouldn't have seen the user created policy. You can only view them on the CLI.

DO NOT REPRINT
© FORTINET

Problem 2: Unable to Access Linux Web Server

```
ISFW # diagnose sniffer packet any "host 10.1.4.10 and port 80" 4  
interfaces=[any]  
filters=[host 10.1.4.10 and port 80]
```

```
30.612212 port3 in 10.1.10.1.53949 -> 10.1.4.10.80: syn 3704715407  
30.864757 port3 in 10.1.10.1.53950 -> 10.1.4.10.80: syn 4120712996
```

FORTINET

© Fortinet Inc. All Rights Reserved.

7

For the second problem, the sniffer displayed only incoming SYN packets.

DO NOT REPRINT
© FORTINET

Problem 2: Unable to Access Linux Web Server

```
ISFW # diagnose debug reset
ISFW # diagnose debug flow filter dport 80
ISFW # diagnose debug flow filter saddr 10.1.10.1
ISFW # diagnose debug flow trace start 10
ISFW # diagnose debug enable

id=20085 trace_id=1 func=print_pkt_detail line=5370 msg="vd-root:0
received a packet(proto=6, 10.1.10.1:54350->10.1.4.10:80) from port3. flag
[S], seq 3700697961, ack 0, win 29200"
id=20085 trace_id=1 func=init_ip_session_common line=5530 msg="allocate a
new session-000003cb"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2590 msg="find a
route: flag=80000000 gw=10.1.4.10 via root"
id=20085 trace_id=1 func=fw_local_in_handler line=409
msg="iprope_in_check() check failed on policy 0, drop"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

8

The debug flow showed the same error as with the first problem: `iprope_in_check()` check failed on policy 0, drop. However, in this case, the cause was different because this traffic was not intended to terminate in the FortiGate. As explained in this lesson, the cause might be a wrong VIP or IP pool configuration.

DO NOT REPRINT
© FORTINET

Problem 2: Unable to Access Linux Web Server

- Solution:
 - Remove invalid IP pool entry in the ISFW

Policy & Objects > IP Pools

<div>+ Create New Edit Clone Delete <input type="text" value="Search"/> Q</div>				
Name	External IP Range	Type	ARP Reply	Ref.
IPPOOL	10.1.4.1 - 10.1.4.254	Overload	✓ Enabled	0

FORTINET

© Fortinet Inc. All Rights Reserved.

9

There was actually an IP pool on ISFW with the 10.1.4.0/24 subnet. As the web server's IP address is part of the IP pool, the FortiGate assumes that it *owns* this address. So, any traffic destined to 10.1.4.10 terminates in the FortiGate. The solution was removing the IP pool configuration.

DO NOT REPRINT
© FORTINET

Problem 3: Unable to Access Public Web Sites

```
ISFW # diagnose debug reset
ISFW # diagnose debug flow filter dport 53
ISFW # diagnose debug flow filter saddr 10.1.10.1
ISFW # diagnose debug flow trace start 10
ISFW # diagnose debug enable

ISFW # id=20085 trace_id=20 func=print_pkt_detail line=4784 msg="vd-root
received a packet(proto=17, 10.1.10.1:54126->4.2.2.1:53) from port3. "

id=20085 trace_id=20 func=init_ip_session_common line=4935 msg="allocate a
new session-00011f9e"

id=20085 trace_id=20 func=vf_ip_route_input_common line=2584 msg="find a
route: flag=04000000 gw=10.1.0.254 via port1"

id=20085 trace_id=20 func=fw_forward_handler line=558 msg="Denied by
forward policy check (policy 0)"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

1
0

For the third problem, users were unable to access public websites. Attempts to connect to yahoo.com were failing, however you could still ping 8.8.8.8. This means that Client-10 does have Internet connectivity but it is having issues resolving domain names. We could confirm this by running a debug flow of the traffic to port 53 (DNS).

DO NOT REPRINT
© FORTINET

Problem 3: Unable to Access Public Web Sites

- Solution:
 - Allow DNS traffic in the firewall policy:

Policy & Objects > Firewall Policy

10.1.10.	all	always	HTTP HTTPS TELNET PING	✓ ACCEPT	✗ Disabled	SSL no-inspection	All
----------	-----	--------	---------------------------------	----------	------------	-------------------	-----

Add DNS to the
allowed services

FORTINET

© Fortinet Inc. All Rights Reserved.

1
1

The problem was that DNS traffic was not allowed in the firewall policies. Adding the DNS service to the firewall policy solved the problem.

DO NOT REPRINT
© FORTINET

Problem 4: Telnet Access to the Linux Router

```
ISFW # diagnose sniffer packet any "port 23" 4
interfaces=[any]
filters=[port 23]
17.580187 port3 in 10.1.10.1.56730 -> 100.64.1.254.23: syn 1424159519
17.580252 port1 out 10.1.10.1.56730 -> 100.64.1.254.23: syn 1424159519
17.580818 port1 in 100.64.1.254.23 -> 10.1.10.1.56730: rst 0 ack 1424159520
17.580873 port3 out 100.64.1.254.23 -> 10.1.10.1.56730: rst 0 ack 1424159520
17.581060 port1 in 100.64.1.254.23 -> 10.1.10.1.56730: rst 0 ack 1424159520
```

ISFW is not doing anything wrong. Linux-Router is resetting the connection.

FORTINET

© Fortinet Inc. All Rights Reserved.

1
2

In the last problem, the sniffer of traffic to port 23 showed that the FortiGate was actually routing the SYN packets properly this time. However, the router was replying with RST packets. So, the problem was not on the FortiGate side, but on the server side.

DO NOT REPRINT
© FORTINET

Lab 4—Routing

Now, we will look at the solutions for the troubleshooting exercise in the routing lab.

DO NOT REPRINT
© FORTINET

Route Changes and Source NAT sessions

- `port1` goes down and traffic is automatically routed to secondary interface (`port2`)
- `port1` comes back on, however SNAT sessions continue to use `port2` because the route is still active in the routing table
- To change this behaviour, do one of the following:
 - Clear the existing entries in the session table
 - Enable `snat-route-change`:

```
config system global
    set snat-route-change enable
end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

1
4

When the primary Internet link went down, the routing table changed. So, all the routing information was flushed from the affected sessions and traffic was routed to `port2`. When `port1` came back up, all SNAT sessions continued using `port2`, because the `port2` route was still valid and the interface was still up. Existing SNAT sessions would continue using `port2` until they expire.

There is a global setting that instructs FortiGate to reroute existing SNAT sessions upon any routing change, even for the cases where the old route is still up. You can enable the `snat-route-change` setting as shown on this slide.

DO NOT REPRINT
© FORTINET

Problem 1: Default Routes

```
NGFW-1 # get router info routing-table database
```

```
Routing table for VRF=0
```

```
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
```

```
> - selected route, * - FIB route, p - stale info
```

```
S    *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1, [10/0]
```

```
S    0.0.0.0/0 [11/0] via 100.64.2.254, port2, [5/0]
```

```
C    *> 10.1.0.0/24 is directly connected, port3
```

```
S    *> 10.1.4.0/24 [10/0] via 10.1.0.100, port3
```

```
S    *> 10.1.10.0/24 [10/0] via 10.1.0.1, port3
```

```
C    *> 100.64.1.0/24 is directly connected, port1
```

```
C    *> 100.64.2.0/24 is directly connected, port2
```

FORTINET

© Fortinet Inc. All Rights Reserved.

1
5

The default route configuration was not working as desired. The default route using **port2** was inactive.

DO NOT REPRINT
© FORTINET

Problem 1: Default Routes

- Solution:

- Change the **Administrative Distance** to 10
- Change the **Priority** value to be higher than the **port1** route's priority (10).

Network > Static Routes

Destination ⓘ	<div>Subnet Internet Service</div>
	0.0.0.0/0.0.0.0
Gateway Address	100.64.2.254
Interface	port2
Administrative Distance ⓘ	11
Comments	<div>Write a comment... 0/255</div>
Status	<div>Enabled Disabled</div>
Advanced Options	
Priority ⓘ	5

FORTINET

© Fortinet Inc. All Rights Reserved.

1
6

The **port2** default route's distance was higher than the **port1** default route. In order for both default routes to be active, they must have the same distance. Also, the **port2** priority value was lower than **port1** route's priority value.

DO NOT REPRINT
© FORTINET

Problem 2: Traffic to 100.64.3.1

```
NGFW-1 # diagnose sniffer packet any "icmp and host 100.64.3.1" 4
interfaces=[any]
filters=[icmp and host 100.64.3.1]
10.204428 port3 in 10.1.10.1 -> 100.64.3.1: icmp: echo request
10.204628 port2 out 100.64.2.1 -> 100.64.3.1: icmp: echo request
10.205866 port2 in 100.64.3.1 -> 100.64.2.1: icmp: echo reply
10.205901 port3 out 100.64.3.1 -> 10.1.10.1: icmp: echo reply

id=20085 trace_id=1 func=print_pkt_detail line=5370 msg="vd-root:0 received a
packet(proto=1, 10.1.10.1:39616->100.64.3.1:2048) from port3. type=8, code=0,
id=39616, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5530 msg="allocate a new session-
0000024a"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2578 msg="Match policy routing:
to 100.64.2.254 via ifindex-6"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2590 msg="find a route:
flag=00000000 gw=100.64.2.254 via port2"
id=20085 trace_id=1 func=fw_forward_handler line=751 msg="Allowed by Policy-2: SNAT"
id=20085 trace_id=1 func=__ip_session_run_tuple line=3264 msg="SNAT 10.1.10.1-
>100.64.2.1:39616"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

1
7



Why was traffic to 100.64.3.1 taking **port2**? The debug flow showed the reason. There was a policy-based route overriding the static route configuration.

DO NOT REPRINT
© FORTINET

Problem 2: Traffic to Spoke-1

- Solution:
 - Remove the policy-based route

Network > Policy Routes

+ Create New Edit Delete <input type="text" value="Search"/> <input type="button" value="Q"/>					
Seq.#	Incoming Interface	Outgoing Interface	Source	Destination	Hit Count
1	 port3	 port2	10.1.10.0/255.255.255.0	100.64.3.0/255.255.255.0	18 

Removing the policy-based route fixed the problem.

DO NOT REPRINT
© FORTINET

Lab 5—FortiGuard

Now, we will look at the solutions for the troubleshooting exercises in the FortiGuard lab.

DO NOT REPRINT
© FORTINET

Problem 1: Local FDS

```
DCFW # diagnose debug application update -1
```

```
Debug messages will be on for 30 minutes
```

```
DCFW # dia debug enable
```

```
DCFW # exe update-now
```

```
upd_daemon[1354]-Received update now request
```

```
do_setup[296]-Starting SETUP
```

```
upd_comm_connect_fds[446]-Trying FMG 10.1.0.210:8890
```

```
tcp_connect_fds[259]-Failed connecting after sock writable
```

```
upd_comm_connect_fds[460]-Failed TCP connect
```

```
do_setup[308]-Failed setup
```

```
upd_daemon[1584]-Disabling remaining actions 12
```

FORTINET

© Fortinet Inc. All Rights Reserved.

2
0

The first problem was that DCFW was experiencing issues connecting to FortiManager for license information. The output of the FortiGuard real time debug showed that DCFW was trying to connect to the wrong IP address.

DO NOT REPRINT
© FORTINET

Problem 1: Local FDS

- Solution:

- Change server IP to 10.1.0.241

```
DCFW # config system central-management
DCFW (central-management) # config server-list
DCFW (server-list) # edit 1
DCFW (1) # set server-address 10.1.0.241
DCFW (1) # end
DCFW (central-management) # end
```



© Fortinet Inc. All Rights Reserved.

2
1

Correcting the IP address in the central management configuration solved the problem.

DO NOT REPRINT
© FORTINET

Problem 2: Rating Lookups

```
ISFW # diagnose debug application urlfilter -1
```

```
ISFW # diagnose debug enable
```

```
0(4086) msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:  
d=fortinet.com:80, id=751, cat=255, vfname='root', vfid=0,  
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
```

```
0(4086) msg="Policy denies URLs when a rating error occurs" user="N/A"  
src=10.1.10.1 sport=48072 dst=208.91.114.181 dport=80 service="http"  
hostname="fortinet.com" status=blocked error="all Fortiguard servers  
failed to respond" url="/"
```

FORTINET

© Fortinet Inc. All Rights Reserved.

2
2

The second issue involved web filtering rating on ISFW. The web filtering real time debug showed that ISFW was not able to find any available FortiGuard servers.

DO NOT REPRINT
© FORTINET

Problem 2: Rating Lookups

- Solution:
 - Change the server type to update and rating

```
ISFW # config system central-management
ISFW (central-management) # config server-list
ISFW (server-list) # edit 1
ISFW (1) # set server-type update rating
ISFW (1) # end
ISFW (central-management) # end
```


DO NOT REPRINT
© FORTINET

Lab 8—OSPF

We will see the solutions for the troubleshooting exercise in the OSPF lab.

DO NOT REPRINT
© FORTINET

Problem 1: Duplicate Router ID

```
OSPF: -----
OSPF: RECV[Hello]: From 0.0.0.2 via port3:10.1.4.254 (10.1.4.10 -> 224.0.0.5)
OSPF: -----
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 44
OSPF:   Router ID 0.0.0.2
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0xee91
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*| - | - | - | E | -)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 10.1.4.10
OSPF:   BDRouter 0.0.0.0
OSPF:   # Neighbors 0
OSPF: -----
OSPF: RECV[Hello]: duplicate router-id 0.0.0.2 detected on port3:10.1.4.254
OSPF: IFSM[port1:10.1.0.100]: Hello timer expire
OSPF: SEND[Hello]: To 224.0.0.5 via port1:10.1.0.100, length 52
OSPF: -----
```

FORTINET

© Fortinet Inc. All Rights Reserved.

2
5

The OSPF real time debug showed why the adjacency was not coming up. The Linux Server is using the router ID 0.0.0.2, which is also being used by DCFW.

DO NOT REPRINT
© FORTINET

Problem 1: Duplicate Router ID

- Solution:
 - Change the DCFW router ID to 0.0.0.4

DCFW System Router : OSPF Display Options

OSPF

Router ID 0.0.0.4

Advanced Options >

Areas

+ Create New Edit Delete Column Settings

Area	Type	Authentication
0.0.0.0	Regular	None

Networks

FORTINET

© Fortinet Inc. All Rights Reserved.

2
6

To solve this problem from the DCFW side, change the DCFW router ID from 0.0.0.2 to any other ID available.

DO NOT REPRINT
© FORTINET

Problem 1: Duplicate Router ID

```
DCFW # get router info ospf neighbor
```

```
OSPF process 0:
```

Neighbor ID Interface	Pri	State	Dead Time	Address
0.0.0.3	1	Full/Backup	00:00:32	10.1.0.1 port1
0.0.0.1	1	Full/DR	00:00:34	10.1.0.254 port1
0.0.0.2	1	Full/DR	00:00:31	10.1.4.10 port3

FORTINET

© Fortinet Inc. All Rights Reserved.

2
7

If you applied the fix on DCFW, you should see the Linux-Router (0.0.0.0.2) adjacency coming up.

DO NOT REPRINT
© FORTINET

Lab 9—BGP

Now, we will look at the solutions for the troubleshooting exercise in the BGP lab.

DO NOT REPRINT
© FORTINET

Problem 1: Wrong Remote AS

```
NGFW-1 # diagnose ip router bgp all enable
NGFW-1 # diagnose ip router bgp level info
NGFW-1 # diagnose debug en
```

```
BGP: [RIB] Scanning BGP Network Routes...
BGP: [NETWORK] Accept Thread: Incoming conn from host 100.64.2.254 (FD=21)
BGP: 100.64.2.254-Outgoing [FSM] State: Active Event: 14
BGP: 100.64.2.254-Outgoing [FSM] InConnReq: Accepting...
BGP: 100.64.2.254-Outgoing [NETWORK] FD=21, Sock Status: 0-Success
BGP: 100.64.2.254-Outgoing [FSM] State: Active Event: 17
BGP: 100.64.2.254-Outgoing [ENCODE] Msg-Hdr: Type 1
BGP: 100.64.2.254-Outgoing [ENCODE] Open: Ver 4 MyAS 65100 Holdtime 180
BGP: 100.64.2.254-Outgoing [ENCODE] Open: Msg-Size 61
BGP: 100.64.2.254-Outgoing [DECODE] Msg-Hdr: type 1 length 45
BGP: 100.64.2.254-Outgoing [DECODE] Open: Bad Remote-AS (100), expected 200
BGP: 100.64.2.254-Outgoing [FSM] State: OpenSent Event: 22
BGP: 100.64.2.254-Outgoing [ENCODE] Msg-Hdr: Type 3
BGP: %BGP-3-NOTIFICATION: sending to 100.64.2.254 2/2 (OPEN Message Error/Bad Peer AS.) 4
data-bytes [00 64 00 00]
BGP: [GRST] Timer Announce Defer: Check
...
```

FORTINET

© Fortinet Inc. All Rights Reserved.

2
9

The BGP neighbors were not coming up because NGFW-1 was configured with the remote AS 200, but the ISP AS is 100.

DO NOT REPRINT
© FORTINET

Problem 1: Wrong Remote AS

- Solution:
 - Change remote AS to 100

NGFW-1 System Router : BGP Display Options

BGP

Local AS 65100

Router ID 172.16.1.254

Neighbors

+ Create New Edit Delete Column Settings

Neighbor	Remote AS
<input type="checkbox"/> 100.64.1.254	100
<input type="checkbox"/> 100.64.2.254	100

FORTINET

© Fortinet Inc. All Rights Reserved.

3
0

Changing the remote AS number from 200 to 100 fixes the problem.

DO NOT REPRINT
© FORTINET

Problem 2: BGP Routing

```
NGFW-1 # get router info routing-table all
```

```
Routing table for VRF=0
```

```
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
```

```
* - candidate default
```

```
B* 0.0.0.0/0 [20/0] via 100.64.1.254, port1, 00:08:30
```

```
B 8.8.8.8/32 [20/0] via 100.64.2.254, port2, 00:08:28
```

```
C 10.1.0.0/24 is directly connected, port3
```

```
O 10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:51:34
```

```
C 100.64.1.0/24 is directly connected, port1
```

```
C 100.64.2.0/24 is directly connected, port2
```

FORTINET

© Fortinet Inc. All Rights Reserved.

3
1

The second problem is that NGFW-1 is receiving the prefix 8.8.8.8/32 through **port2**. This was causing all the traffic destined to 8.8.8.8 to be routed through **port2** instead of **port1**.

DO NOT REPRINT
© FORTINET

Problem 2: BGP Routing

- Solution:

- Create a prefix list blocking 8.8.8.8/32
- Apply the prefix list to the prefixes coming from the neighbour 100.64.2.254

```
config router prefix-list
  edit "public"
    config rule
      edit 1
        set prefix 0.0.0.0 0.0.0.0
      next
      edit 2
        set action deny
        set prefix 8.8.8.8 255.255.255.255
      next
    end
  next
end
```

```
config router bgp
  config neighbor
    edit "100.64.2.254"
      set prefix-list-in "public"
      set remote-as 100
    next
  end
```

FORTINET

© Fortinet Inc. All Rights Reserved.

3
2

For this issue, the fix is in the hands of the ISP router's administrator. However, while the ISP fixes the problem, we used a prefix list to block the incoming advertisement to the subnet 8.8.8.8/32.

DO NOT REPRINT
© FORTINET

Lab 10—Web Filtering and Antivirus

Now, we will look at the solutions for the troubleshooting exercises in the web filtering and antivirus lab.

DO NOT REPRINT © FORTINET

Problem 1: Web Filtering

- Why isn't ISFW blocking www.eicar.org?
- The web filtering real time debug explains why:

```
0(7288) action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=5733  
0 dst=213.211.198.62 dport=443 service="https" cat=50 url_cat=50 ip_cat=52 hostn  
ame="www.eicar.org" url="/"
```

```
# get webfilter categories | grep 50  
50 Information and Computer Security
```

- The URL is not categorized as Security Risk, but as Information and Computer Security

FORTINET

© Fortinet Inc. All Rights Reserved.

3

4

The first problem was that some users reported that www.eicar.org should be blocked because it belongs to the security risk category. However, the output of the web filtering real time debug showed that it belongs to a different category (Information Technology), which is allowed in the FortiGate configuration.

DO NOT REPRINT
© FORTINET

Problem 2: Antivirus

- Why doesn't ISFW detect the virus?
- The debug flow does not show this line:
`func=av_receive line=254 msg="send to application layer"`
- So, the FTP proxy is not inspecting the traffic
- Reason:
 - FTP traffic is using a non-standard port—222

FORTINET

© Fortinet Inc. All Rights Reserved.

3
5

The second problem was that ISFW was not blocking the FTP file transfer of an infected file. The debug flow was not showing the message sent to the application layer, which means that ISFW was actually not inspecting the traffic. The reason that this was not happening was because the FTP connection was using a non-standard port—222.

DO NOT REPRINT
© FORTINET

Lab 12—IPsec

Now, we will see the solutions for the troubleshooting exercise in the IPsec lab.

Problem 1: Encryption Mismatch

```

ike 0:755f07a141261b05/0000000000000000:45: responder: main mode get 1st message...
...
ike 0:755f07a141261b05/0000000000000000:45: incoming proposal
ike 0:755f07a141261b05/0000000000000000:45: proposal id = 0:
ike 0:755f07a141261b05/0000000000000000:45:   protocol id = ISAKMP:
ike 0:755f07a141261b05/0000000000000000:45:   trans_id = KEY_IKE.
ike 0:755f07a141261b05/0000000000000000:45:   encapsulation = IKE/noop
ike 0:755f07a141261b05/0000000000000000:45:   type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:755f07a141261b05/0000000000000000:45:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:755f07a141261b05/0000000000000000:45:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:755f07a141261b05/0000000000000000:45:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:755f07a141261b05/0000000000000000:45: ISAKMP SA lifetime=86400
...
ike 0:755f07a141261b05/0000000000000000:45: my proposal, gw VPN
ike 0:755f07a141261b05/0000000000000000:45: ISAKMP SA lifetime=86400
ike 0:755f07a141261b05/0000000000000000:45: proposal id = 1:
ike 0:755f07a141261b05/0000000000000000:45:   protocol id = ISAKMP:
ike 0:755f07a141261b05/0000000000000000:45:   trans_id = KEY_IKE.
ike 0:755f07a141261b05/0000000000000000:45:   encapsulation = IKE/noop
ike 0:755f07a141261b05/0000000000000000:45:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:755f07a141261b05/0000000000000000:45:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:755f07a141261b05/0000000000000000:45:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:755f07a141261b05/0000000000000000:45:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:755f07a141261b05/0000000000000000:45: ISAKMP SA lifetime=86400
...
ike 0:755f07a141261b05/0000000000000000:45: negotiation failure

```

The first problem was a misconfiguration in the phase 1. One side was configured with 3DES, the other side was configured with AES.

DO NOT REPRINT
© FORTINET

Problem 2: Pre-shared Key Mismatch

...

ike 0:VPN:130: responder: main mode get 3rd message...

ike 0:VPN:130: dec

E410DF2B73B8DF1C3ADBB8C4B7F264B2051002010000000000000006C9135F5F081B0E42CC8
D197A5CA4A8B5D24A88B30263F5BD1100003C17E06D5A125B43693308EA1732DEFFA7A9C58
891D2406B2F425674C4F2F93C919DB36F40849C0A793682E12673D91F7A60027CC58

ike 0:VPN:130: parse error

ike 0:VPN:130: probable pre-shared secret mismatch

FORTINET

© Fortinet Inc. All Rights Reserved.

3

8

The second problem was a mismatch in the pre-shared key.

DO NOT REPRINT
© FORTINET

Problem 3: ISP Blocking ESP Packets

```
Spoke-2 # diagnose sniffer packet any "esp or icmp" 4
interfaces=[any]
filters=[esp or icmp]
3.073926 VPN out 10.1.2.254 -> 10.1.1.254: icmp: echo request
3.073943 port1 out 100.64.5.1 -> 100.64.4.1: ESP(spi=0xcb35b188,seq=0x10)
4.078136 VPN out 10.1.2.254 -> 10.1.1.254: icmp: echo request
4.078164 port1 out 100.64.5.1 -> 100.64.4.1: ESP(spi=0xcb35b188,seq=0x11)
```

Spoke-2 is sending the packets out the correct interfaces

```
Spoke-1 # diagnose sniffer packet any "esp or icmp" 4
interfaces=[any]
filters=[esp]
```

But Spoke-1 is not receiving them.

FORTINET

© Fortinet Inc. All Rights Reserved.

3
9

The third problem is that the sniffer shows that the ESP packets from Spoke-2 are not arriving at Spoke-1. So the most likely reason for this is that the ESP packets are being blocked or dropped in transit (Linux-Router).

DO NOT REPRINT
© FORTINET

Lab 13—ADVPN

Now, we will look at the solutions for the troubleshooting exercise in the ADVPN lab.

DO NOT REPRINT
© FORTINET

Connectivity Problem

- Spokes cannot reach Linux Server
- Reason:
 - NGFW-1 is not advertising the prefix 10.1.4.0/24 to the spokes through BGP

```
NGFW-1 # get router info bgp neighbors 172.16.1.2 adver
BGP table version is 5, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*>i0.0.0.0/0 172.16.1.1 0 100 0 100 i
*>i10.1.0.0/24 172.16.1.1 100 32768 i
*>i10.1.2.0/24 172.16.1.3 100 0 i
Total number of prefixes 3
```

FORTINET

© Fortinet Inc. All Rights Reserved.

4
1

The cause of the routing problem was that the NGFW was not advertising the 10.1.4.0/24 prefix through BGP.

DO NOT REPRINT
© FORTINET

Connectivity Problem

- Solutions:
 - Add the `10.1.4.0/24` as a BGP network to advertise
 - Redistribute the OSPF routes to BGP

FORTINET

© Fortinet Inc. All Rights Reserved.

4
2

There are different ways to solve the problem. One of them is adding the `10.1.4.0/24` prefix to the BGP networks configuration. Another solution is redistributing the OSPF routes to BGP.

DO NOT REPRINT
© FORTINET



FORTINET®



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

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.