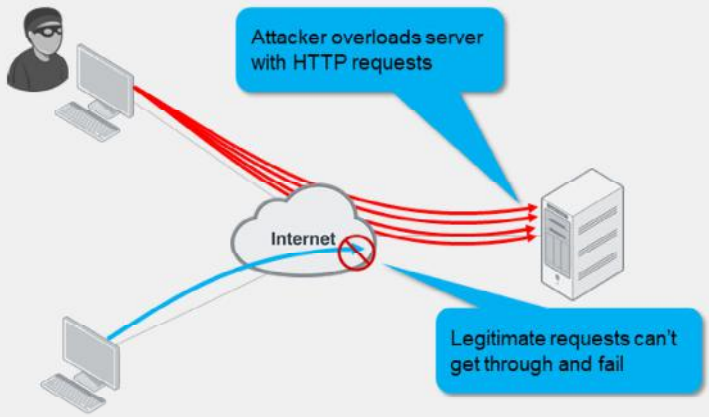
After completing this section, you should be able to achieve the objectives shown on this slide.

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

DoS Attacks

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



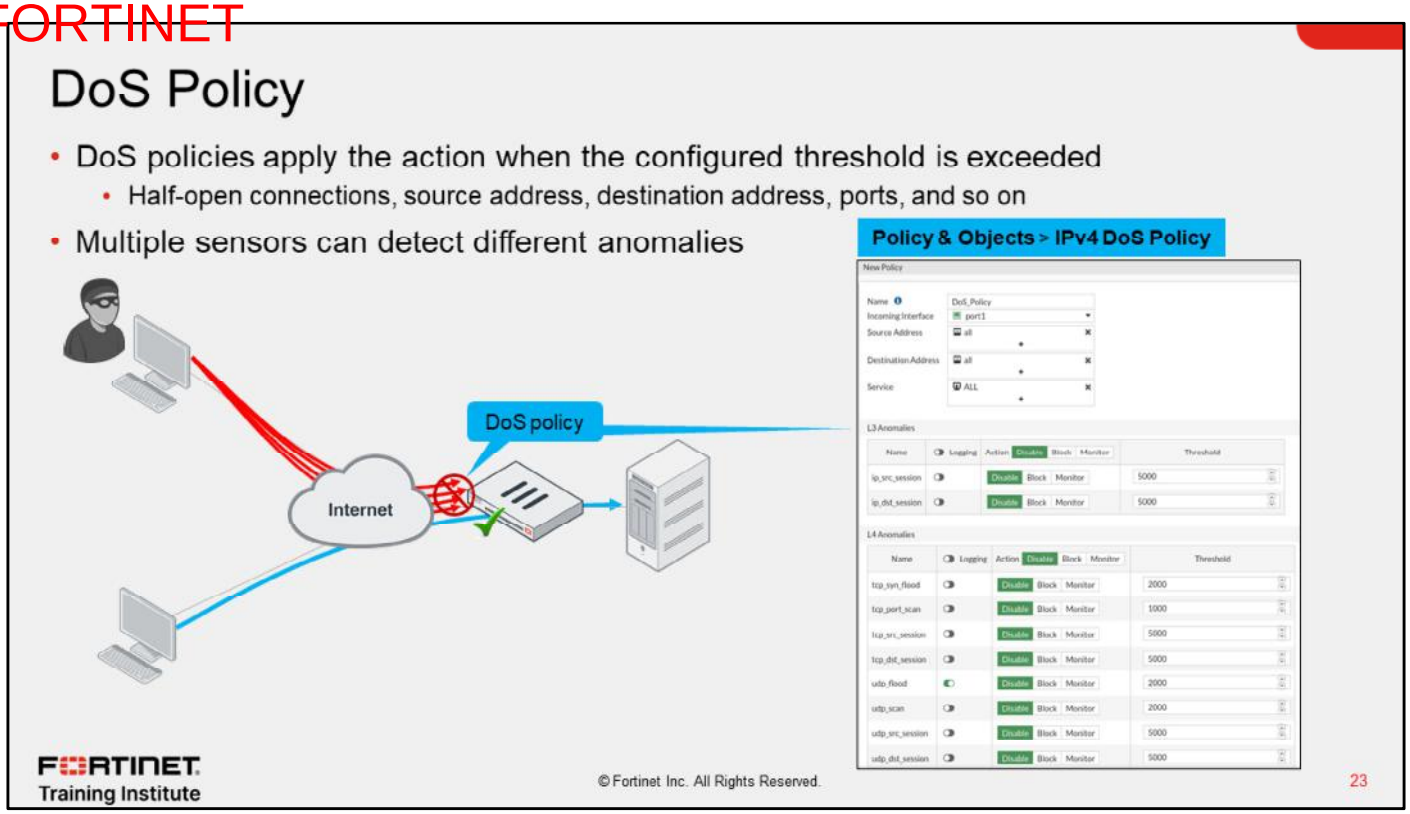
FORTINET Training Institute

22

So far, you have learned about signatures that match illegal commands and invalid protocol implementations. Those are easy to confirm as attacks.

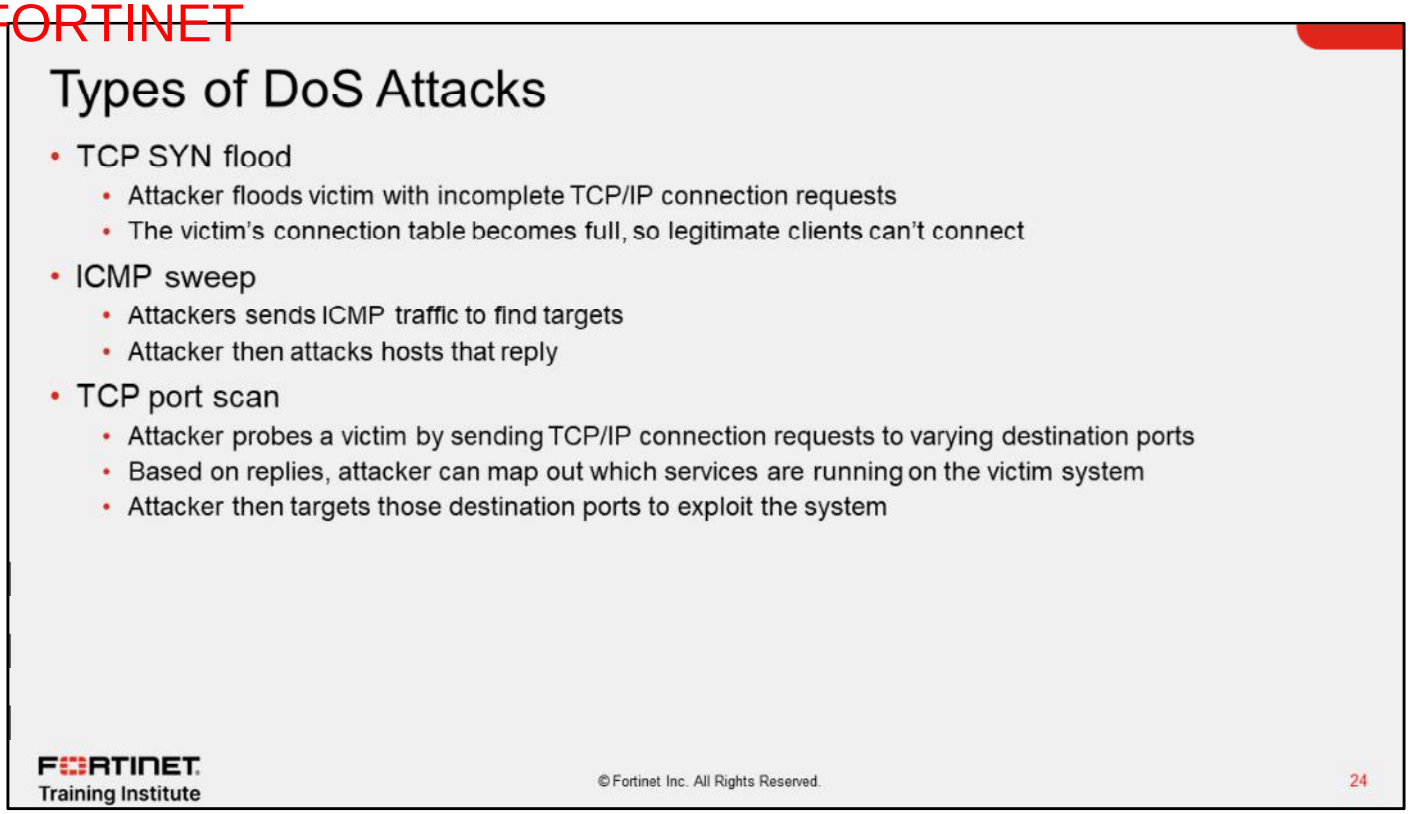
What about attacks that function by exploiting asymmetric processing or bandwidth between clients and servers?

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



To block DoS attacks, apply a DoS policy on a FortiGate that is located between attackers and all the resources that you want to protect.

DoS filtering is done early in the packet handling process, which is handled by the kernel.



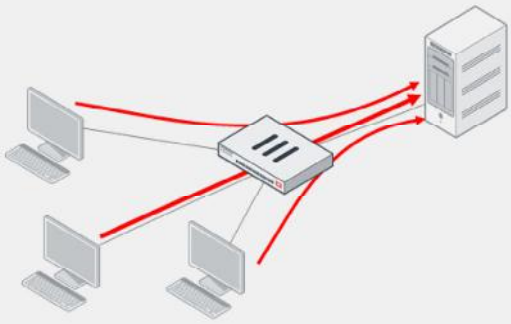
In TCP, the client sends a SYN packet to initiate a connection. The server must respond with a SYN/ACK packet, and save the connection information in RAM while it waits for the client to acknowledge with an ACK packet. Legitimate clients ACK quickly and begin to transmit data. But malicious clients continue to send more SYN packets, half-opening more connections, until the server's connection table is full. Once the server's table is full, it can't accept more connections and begins to ignore all new clients.

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

Attackers use port scanning to determine which ports are active on a system. The attacker sends TCP SYN requests to varying destination ports. Based on the replies, the attacker can map out which services are running on the system, and then proceed to exploit those services.

Types of DoS Attacks (Contd)

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



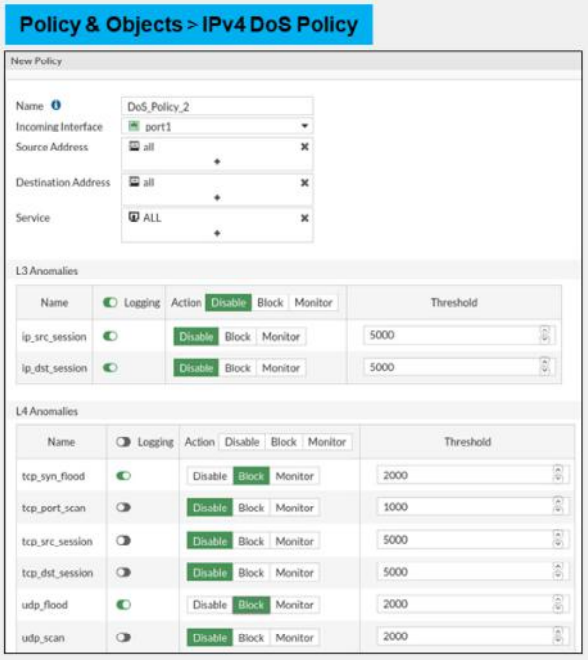
FORTINET Training Institute

25

An individual DoS attack is a flood of traffic coming from a single address. It can originate from the internet, or even from your internal network. Typically, a single device makes many connections or sessions, and possibly uses much bandwidth to connect to a single location. A variation of this is the distributed denial of service attack, or DDoS. It has many of the same characteristics as an individual DoS attack, but the main difference is that multiple devices are all attacking one destination at the same time.

DoS Policy Configuration

- Can apply multiple DoS policies to any physical or logical interface
- Types
  - Flood
    - Detects a large volume of the same type of traffic
  - Sweep/scan
    - Detects probing attempts
  - Source (SRC)
    - Detects a large volume of traffic from an individual IP
  - Destination (DST)
    - Detects a large volume of traffic destined for an individual IP



FORTINET Training Institute

26

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

- A flood sensor detects a high volume of that specific protocol, or signal in the protocol.
- A sweep/scan detects probing attempts to map which of the host ports respond and, therefore, might be vulnerable.
- Source signatures look for large volumes of traffic originating from a single IP address.
- Destination signatures look for large volumes of traffic destined for a single IP address.

When you implement DoS for the first time, if you don't have an accurate baseline for your network, be careful not to completely block network services. To prevent this from happening, configure the DoS policy initially to log, but not block. Using the logs, you can analyze and identify normal and peak levels for each protocol. Then, adjust the thresholds to allow normal peaks, while applying appropriate filtering.

The threshold for flood, sweep, and scan sensors are defined as the maximum number of sessions or packets per second. The thresholds for source and destination sensors are defined as concurrent sessions. Thresholds that are too high can exhaust your resources before the DoS policies trigger. Thresholds that are too low will cause FortiGate to drop normal traffic.

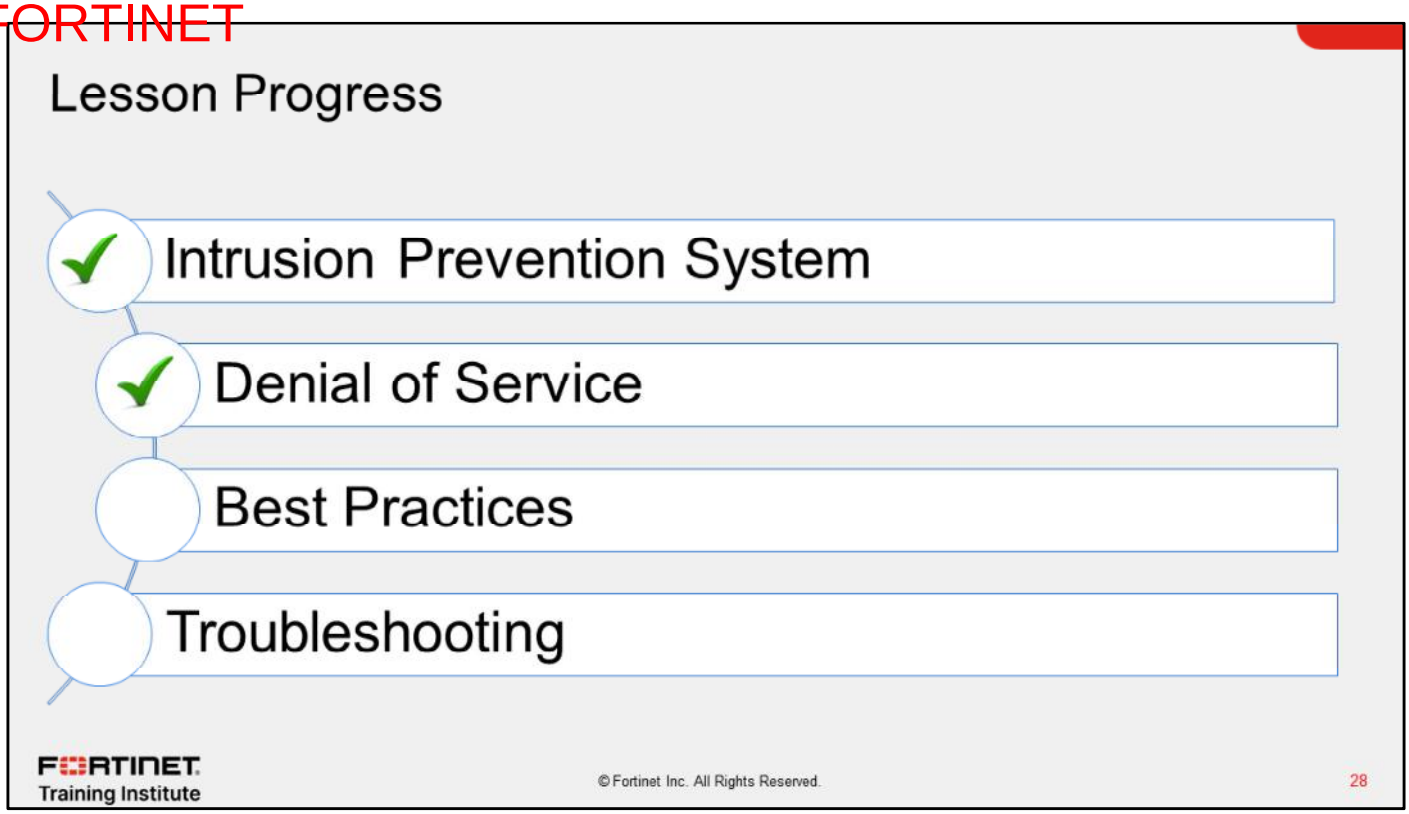
Knowledge Check

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

2. Which behavior is a characteristic of a DoS attack?
   - A. Attempts to exploit a known application vulnerability
   - ✓ B. Attempts to overload a server with TCP SYN packets

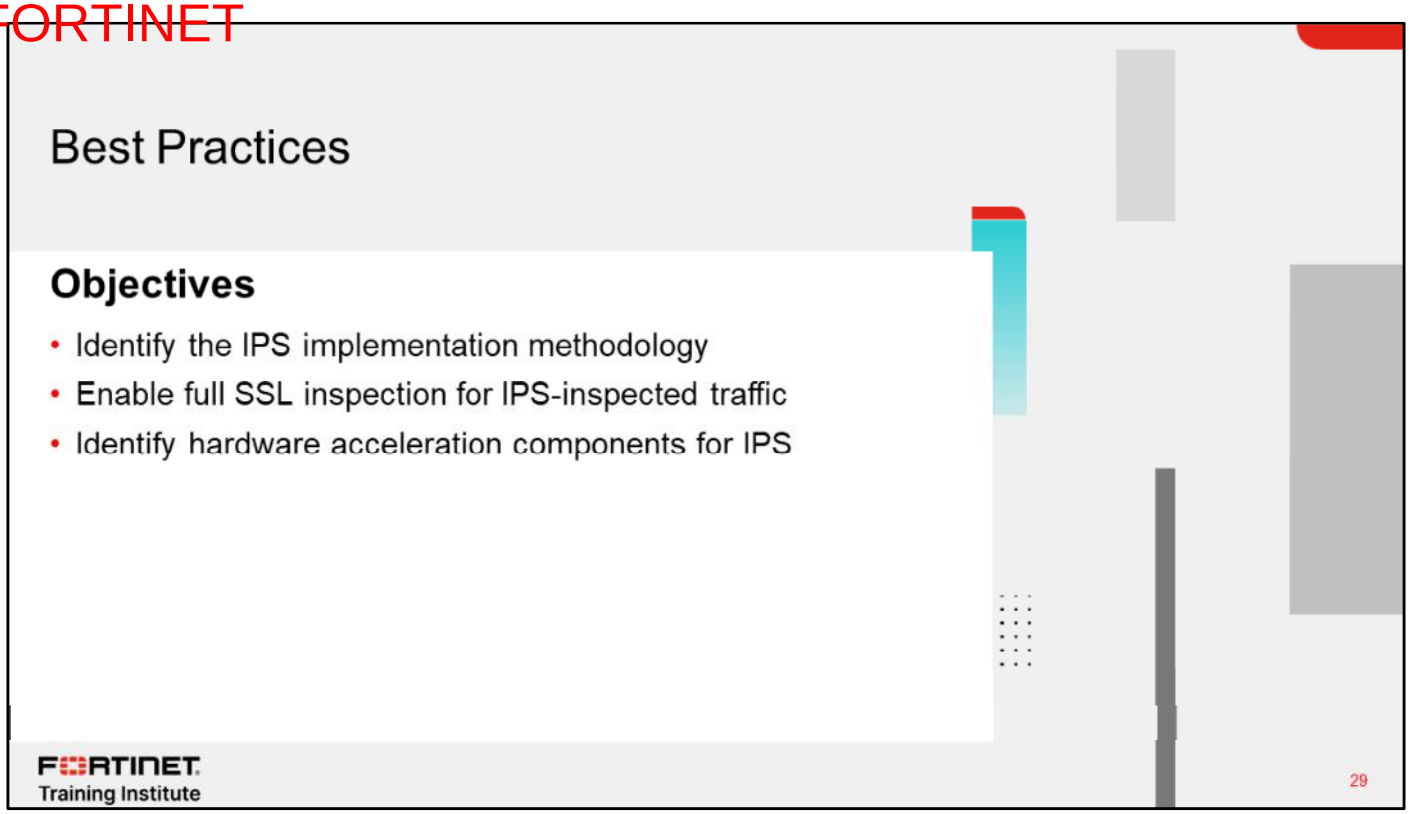
FORTINET Training Institute

27



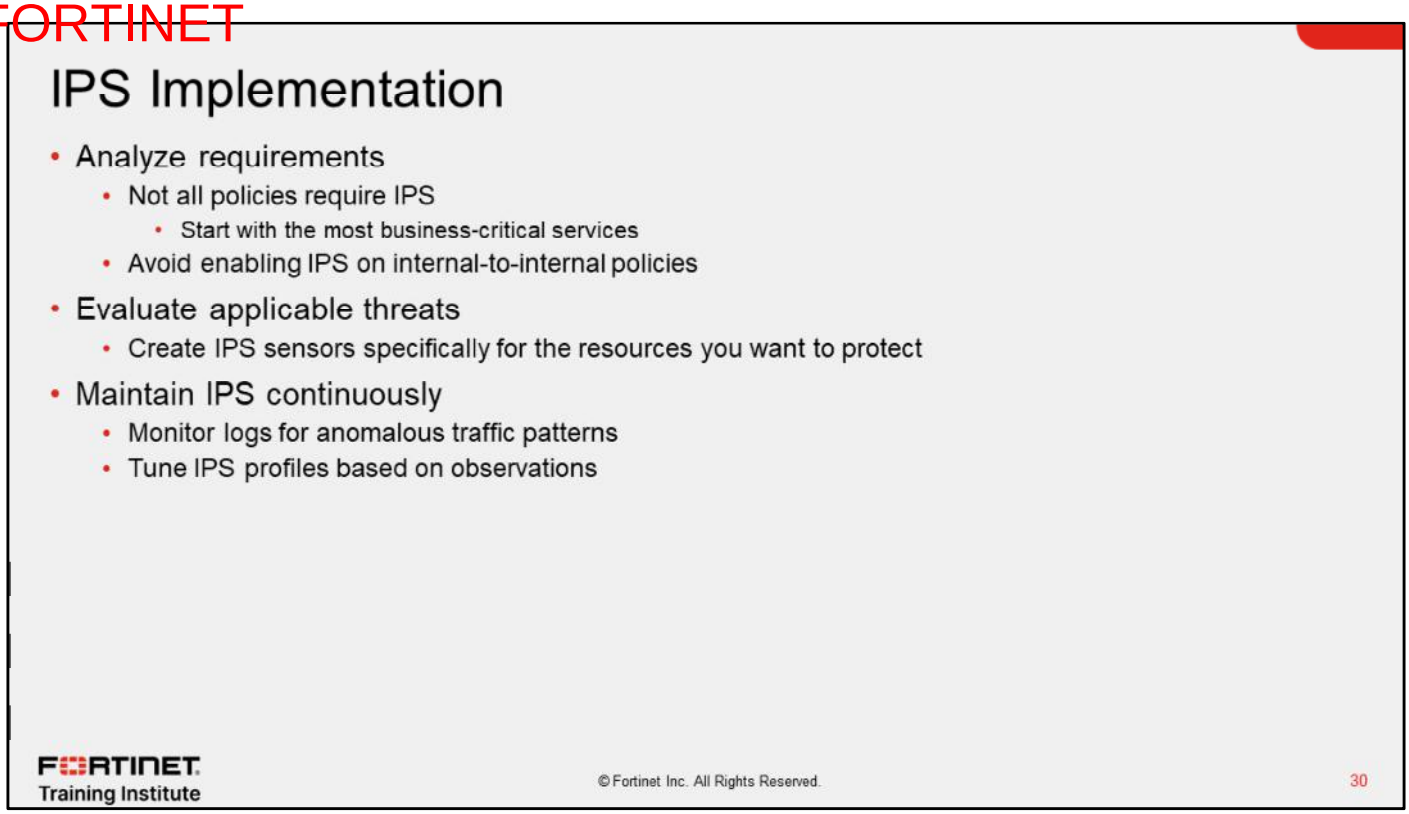
Good job! You now understand how to protect your network from DoS attacks on FortiGate.

Now, you will learn about IPS best practices.



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

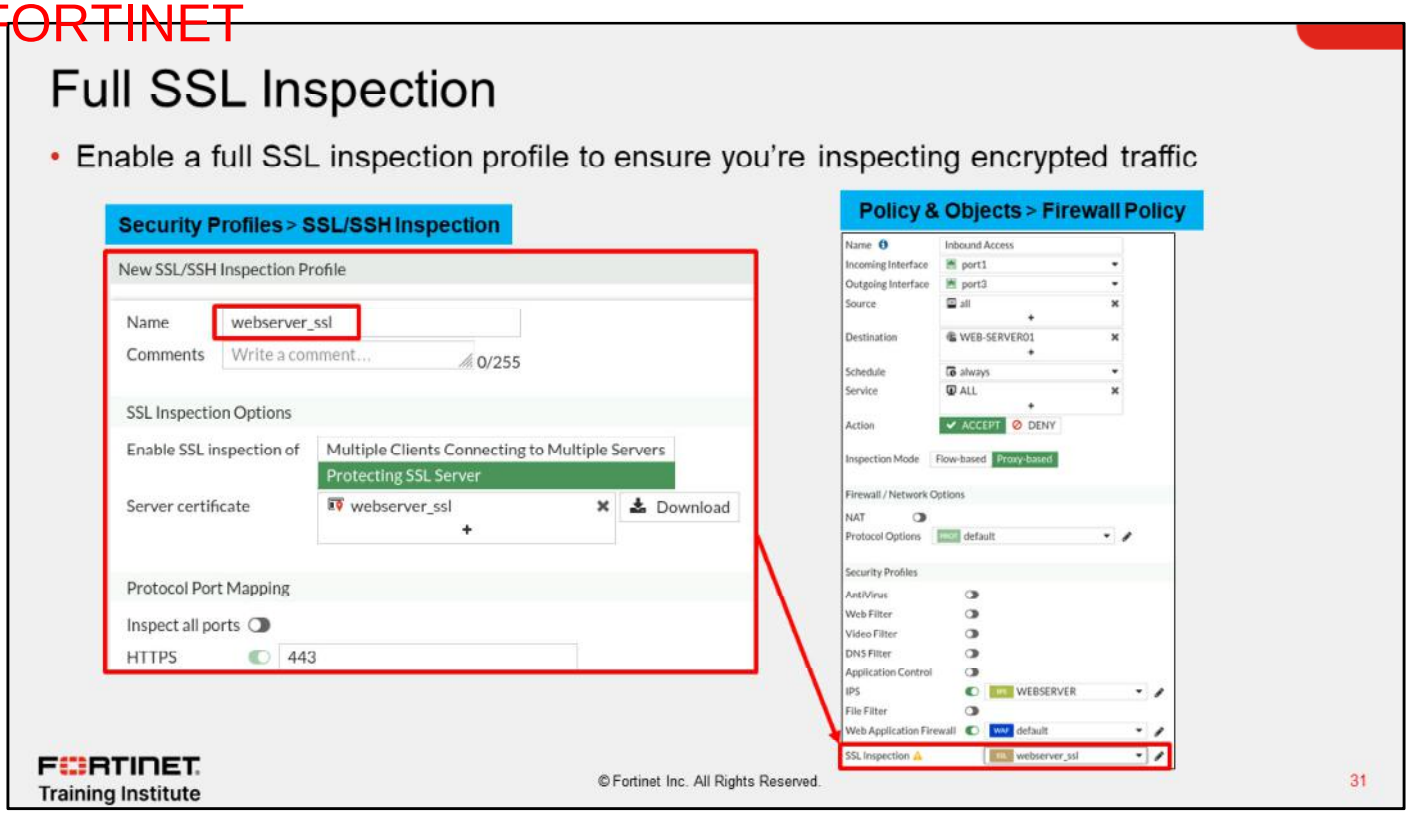
By demonstrating competence in identifying IPS implementation best practices, you should be able to deploy an IPS solution on FortiGate that is efficient and effective. You should also be able to apply full SSL inspection for IPS-inspected traffic, as well as identify hardware acceleration components for IPS.



Before you implement IPS, you must analyze the needs of your network. Enabling the default profiles across all policies quickly causes issues, the least of which are false positives. Performing unnecessary inspections on all network traffic can cause high resource utilization, which can hamper the ability of FortiGate to process regular traffic.

You must also evaluate applicable threats. If your organization runs only Windows, there is no need to scan for Mac OS vulnerabilities. It is also important to consider the direction of the traffic. There are many IPS signatures that apply only to clients, and many signatures that apply only to servers. Create IPS sensors specific to the resources you want to protect. This makes sure that FortiGate is not scanning traffic with irrelevant signatures.

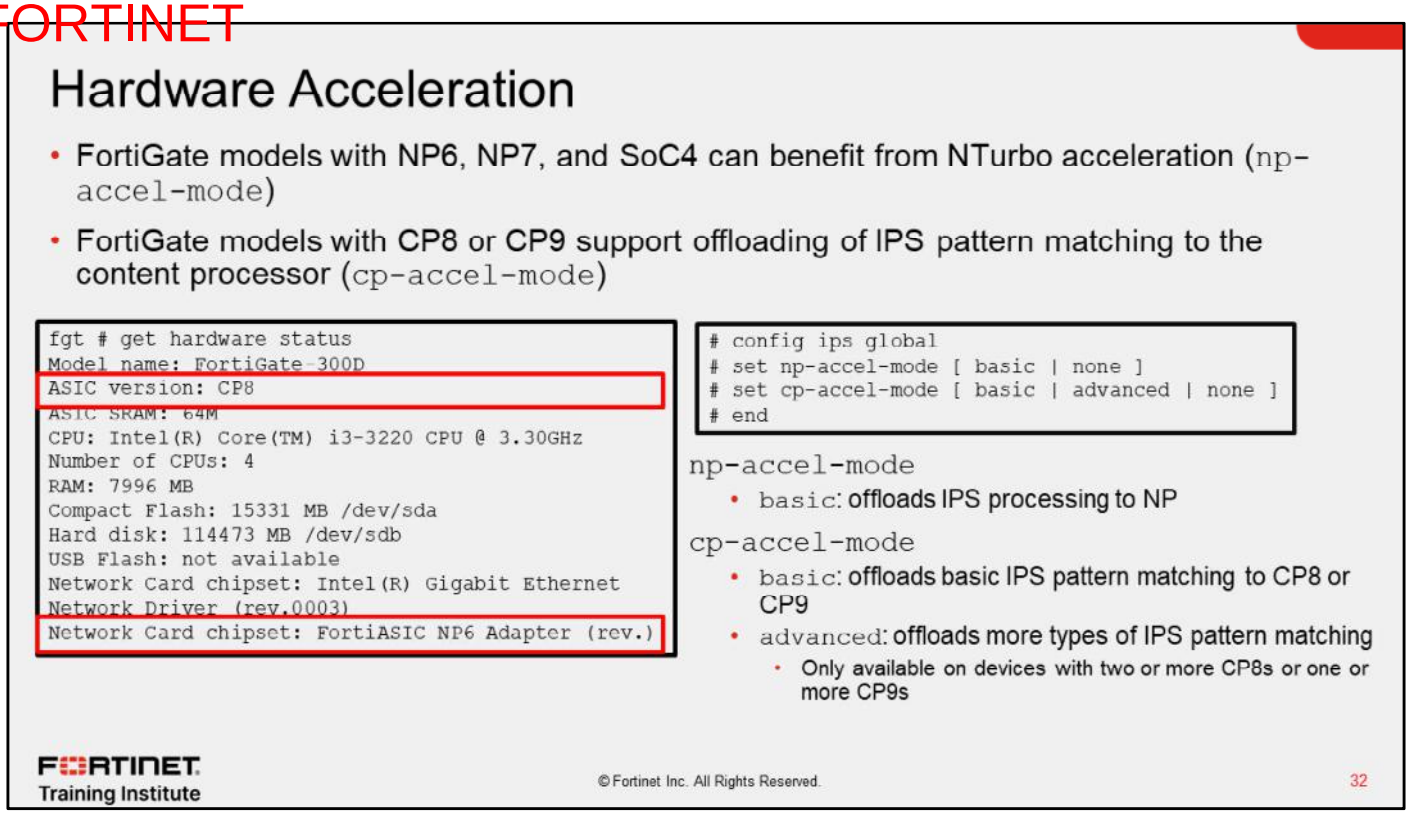
Lastly, IPS is not a *set-and-forget* implementation. You must monitor logs regularly for anomalous traffic patterns, and adjust your IPS profile configuration based on your observations. You should also audit your internal resources regularly to identify if certain vulnerabilities still apply to your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



Certain vulnerabilities apply only to encrypted connections. In some of these cases, FortiGate can't identify the threat reliably if it can't parse the payload. For this reason, you must use an SSL inspection profile if you want to get the maximum benefit from your IPS and WAF features.

The example on this slide shows an SSL inspection profile configured to protect a server. This policy, when applied to inbound traffic, can apply IPS and WAF inspection on encrypted traffic reliably, because FortiGate can decrypt encrypted sessions and inspect all parts of the packet.

It's important to note that DoS policies do not have the ability to assign SSL inspection profiles. This is because DoS does not require SSL inspection to maximize its detection ability, because it does not inspect the packet payload. DoS inspects only specific session types and their associated volume.



Usually, traffic requiring inspection, such as antivirus or IPS, is handled by the CPU on FortiGate. However, there are specialized chips on specific FortiGate models that can offload these inspection tasks. This frees up CPU cycles to manage other tasks, and also accelerates sessions requiring security inspection.

FortiGate models that support a feature called NTurbo can offload IPS processing to NP6, NP7, or SoC4 processors. If the command `np-accel-mode` is available under `config system global`, the FortiGate model supports NTurbo.

Some FortiGate models also support offloading IPS pattern matching to CP8 or CP9 content processors. If the command `cp-accel-mode` is available under `config ips global`, the FortiGate model supports IPS pattern matching acceleration to its CP8 or CP9 processor.

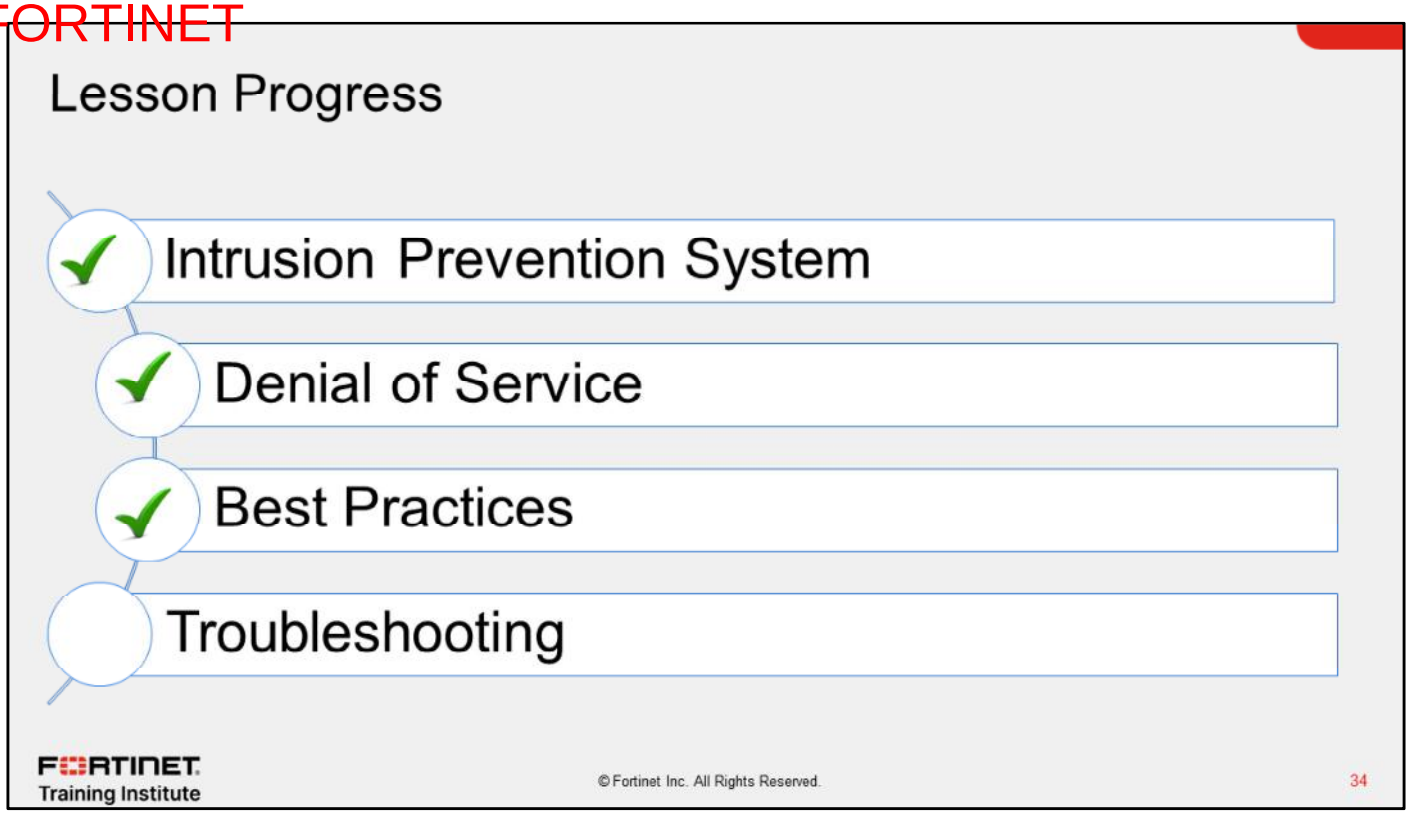
Knowledge Check

1. Which chipset uses NTurbo to accelerate IPS sessions?
   - A. CP9
   - ✓ B. SoC4

2. Which feature requires full SSL inspection to maximize its detection capability?
   - ✓ A. WAF
   - B. DoS

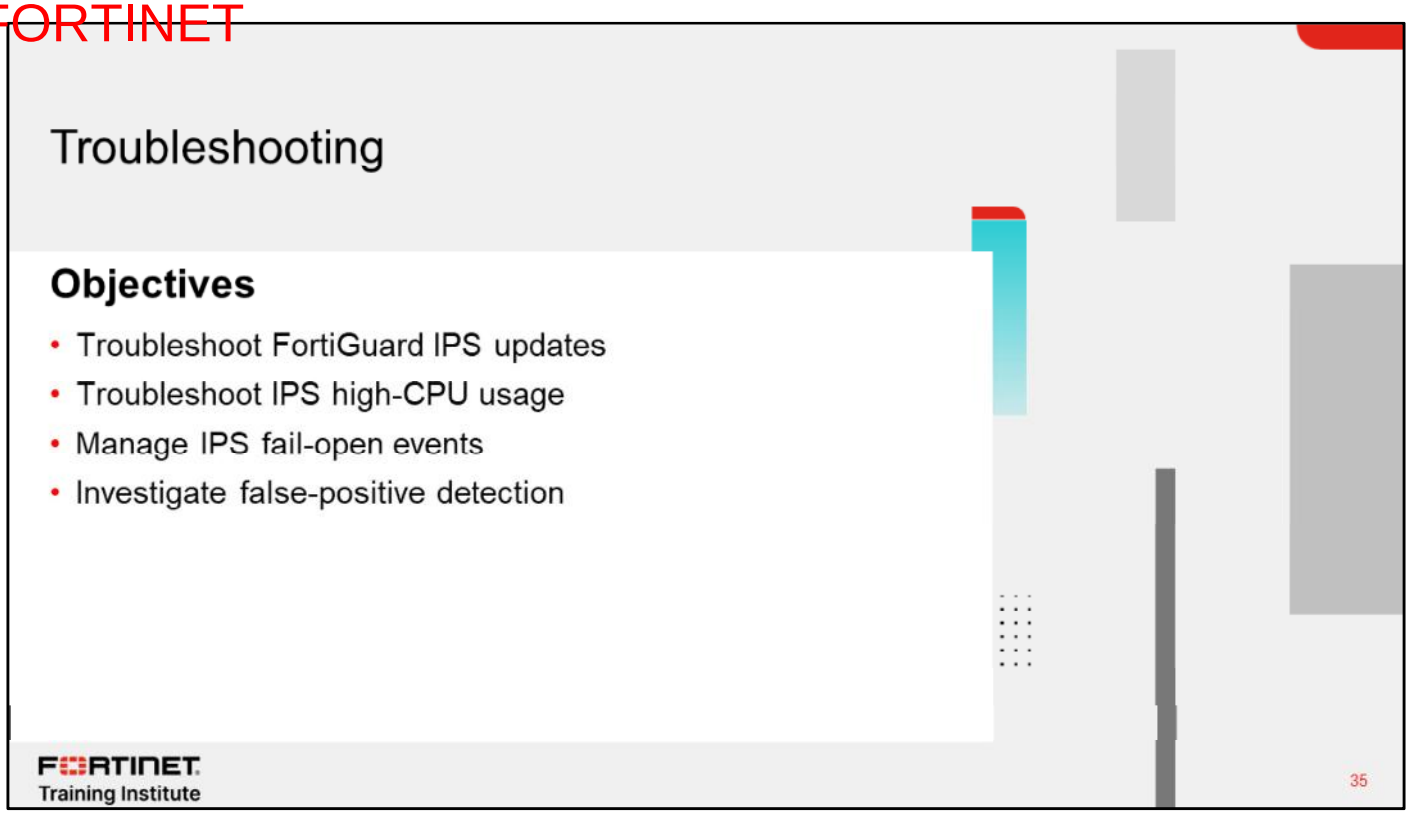
FORTINET Training Institute

33



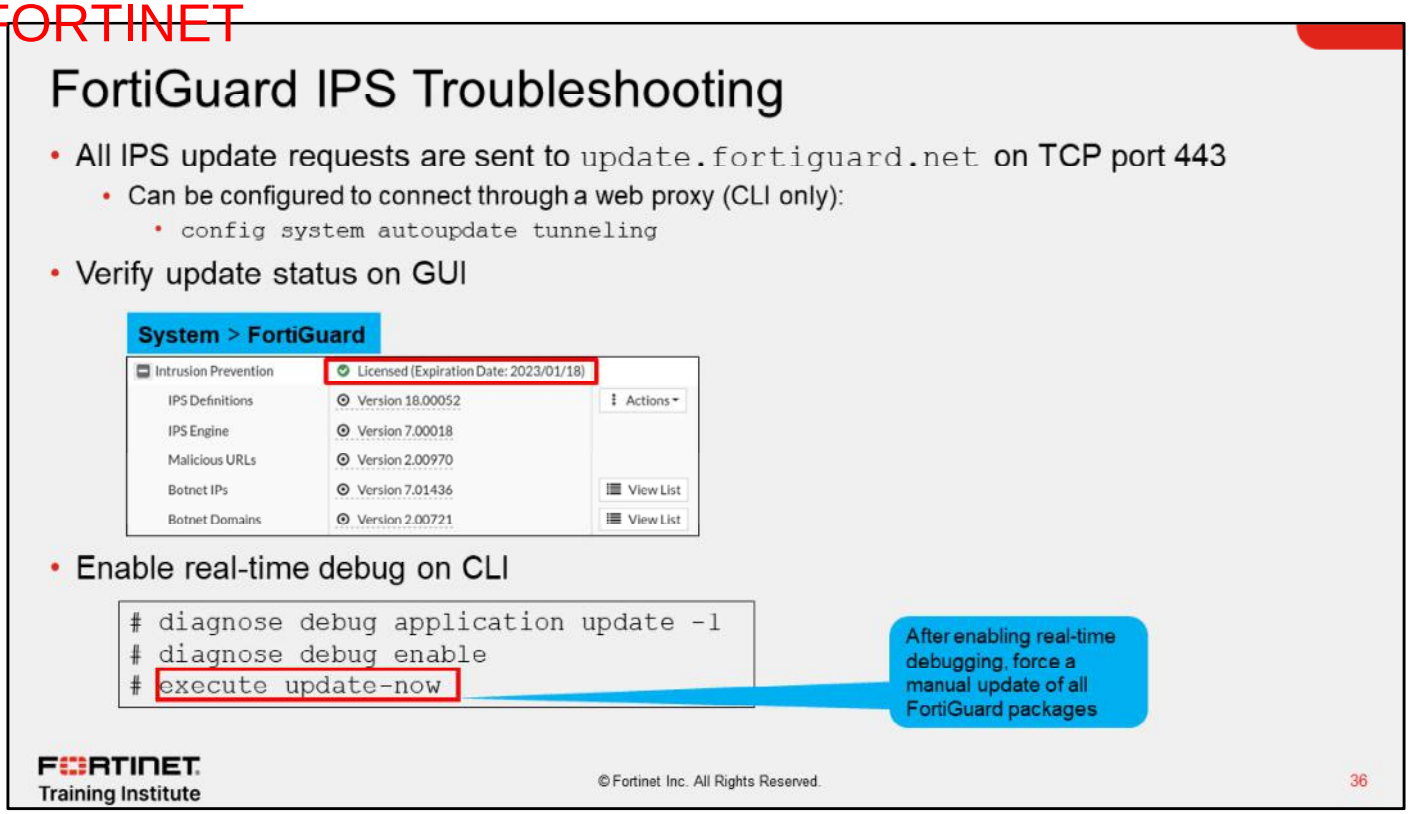
Good job! You now understand some best practices for IPS implementation on FortiGate.

Now, you will learn about IPS troubleshooting.



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

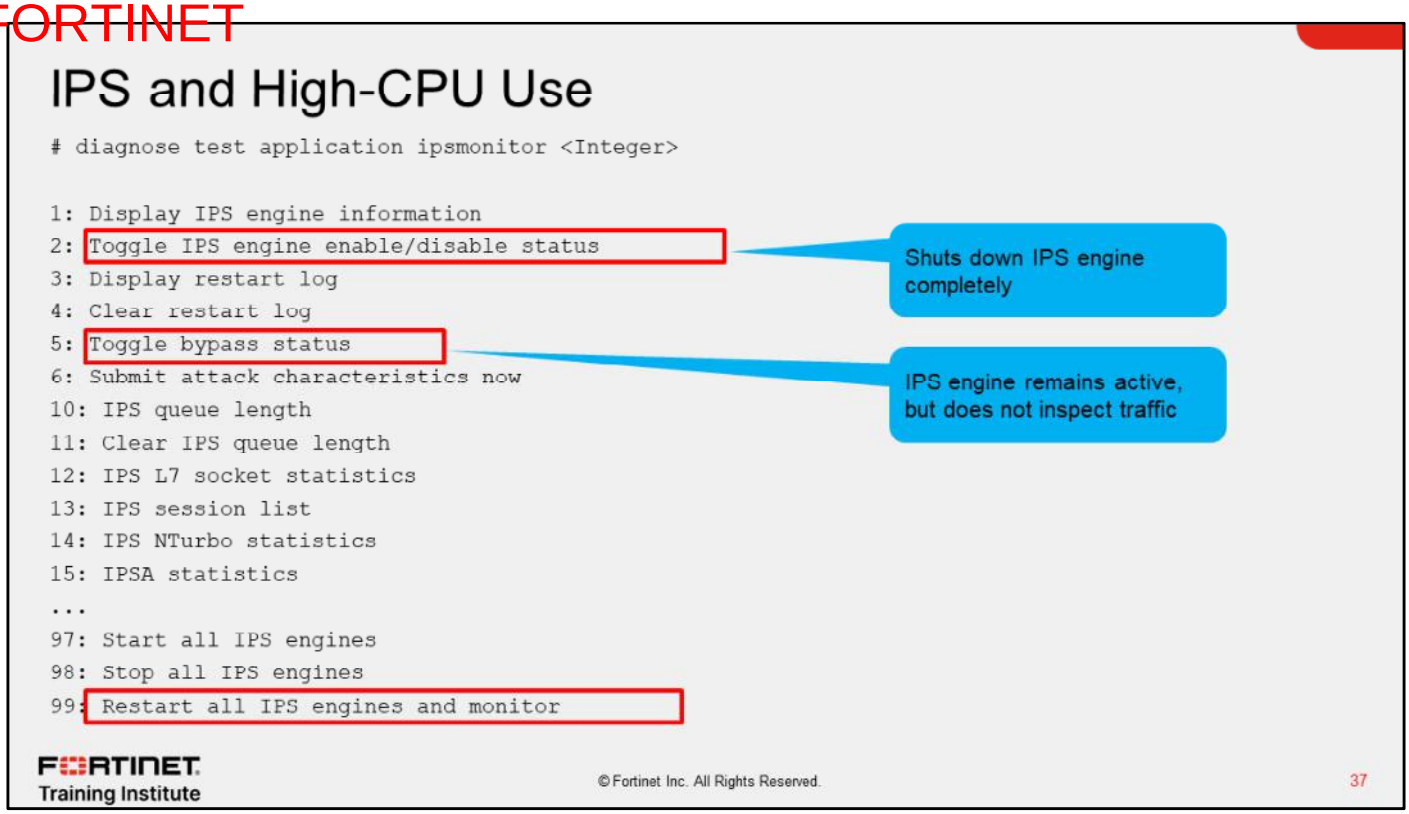
By demonstrating competence in troubleshooting, you should be able to identify, investigate, and manage some common issues with IPS deployments on FortiGate.



FortiGate IPS update requests are sent to `update.fortiguard.net` on TCP port 443. You can also configure FortiGate to connect through a web proxy for updates.

You should check the last update timestamp regularly. You can verify it on the GUI. If there is any indication that the IPS definitions are not updating, you should investigate. Always make sure FortiGate has proper DNS resolution for `update.fortiguard.net`. If, by chance, there are any intermediary devices between the FortiGate and the internet, make sure the correct firewall rules are in place to allow traffic on port443. Any intermediary devices performing SSL inspection on this traffic can also cause issues with updates.

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

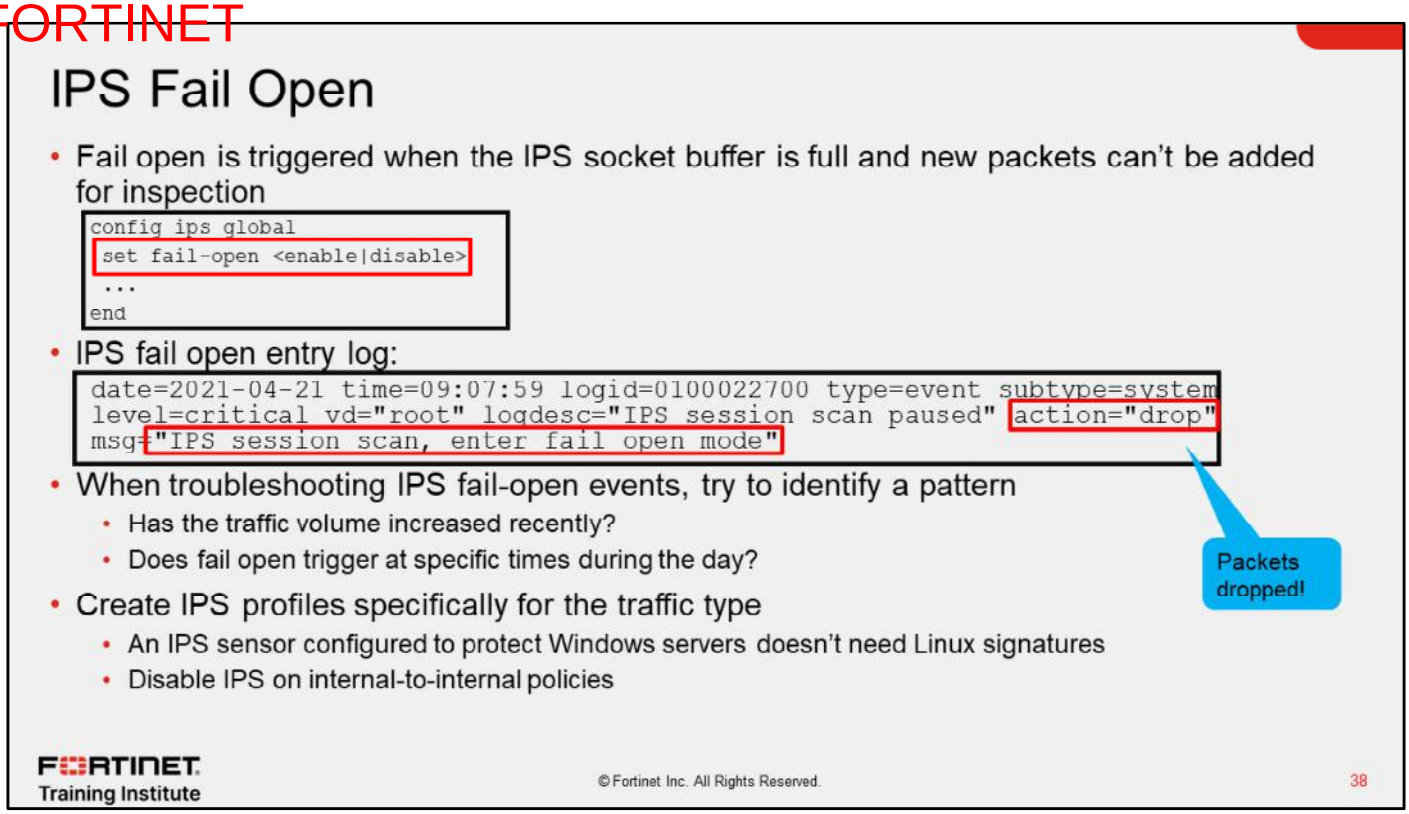


Short spikes in CPU usage by IPS processes can be caused by firewall policy or profile changes. These spikes are usually normal. Spikes might happen when FortiGate has hundreds of policies and profiles, or many virtual domains. Continuous high-CPU use by the IPS engines is not normal, and you should investigate it. You can use the command shown on this slide, along with displayed options, to troubleshoot these issues.

If there are high-CPU use problems caused by the IPS, you can use the `diagnose test application ipsmonitor` command with option `5` to isolate where the problem might be. Option `5` enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

If the CPU use remains high after enabling IPS bypass mode, it usually indicates a problem in the IPS engine, which you must report to Fortinet Support. You can disable the IPS engine completely using option `2`. If you want to restore IPS inspection of traffic after you finish troubleshooting, use option `5` again.

Another recommendation to keep in mind: if you need to restart the IPS, use option `99`, as shown on this slide. This guarantees that all the IPS-related processes restart properly.



IPS goes into fail-open mode when there is not enough available memory in the IPS socket buffer for new packets. What happens during this state depends on the IPS configuration. If the `fail-open` setting is enabled, some new packets (depending on the system load) will pass through without being inspected. If it is disabled, new packets are dropped.

Frequent IPS fail open events usually indicate that IPS can't keep up with the traffic demands. So, try to identify patterns. Has the traffic volume increased recently? Have throughput demands increased? Does fail open trigger at specific times during the day?

Tune and optimize your IPS configuration. Create IPS profiles specific to the type of traffic being inspected, and disable IPS profiles on policies that don't need them.

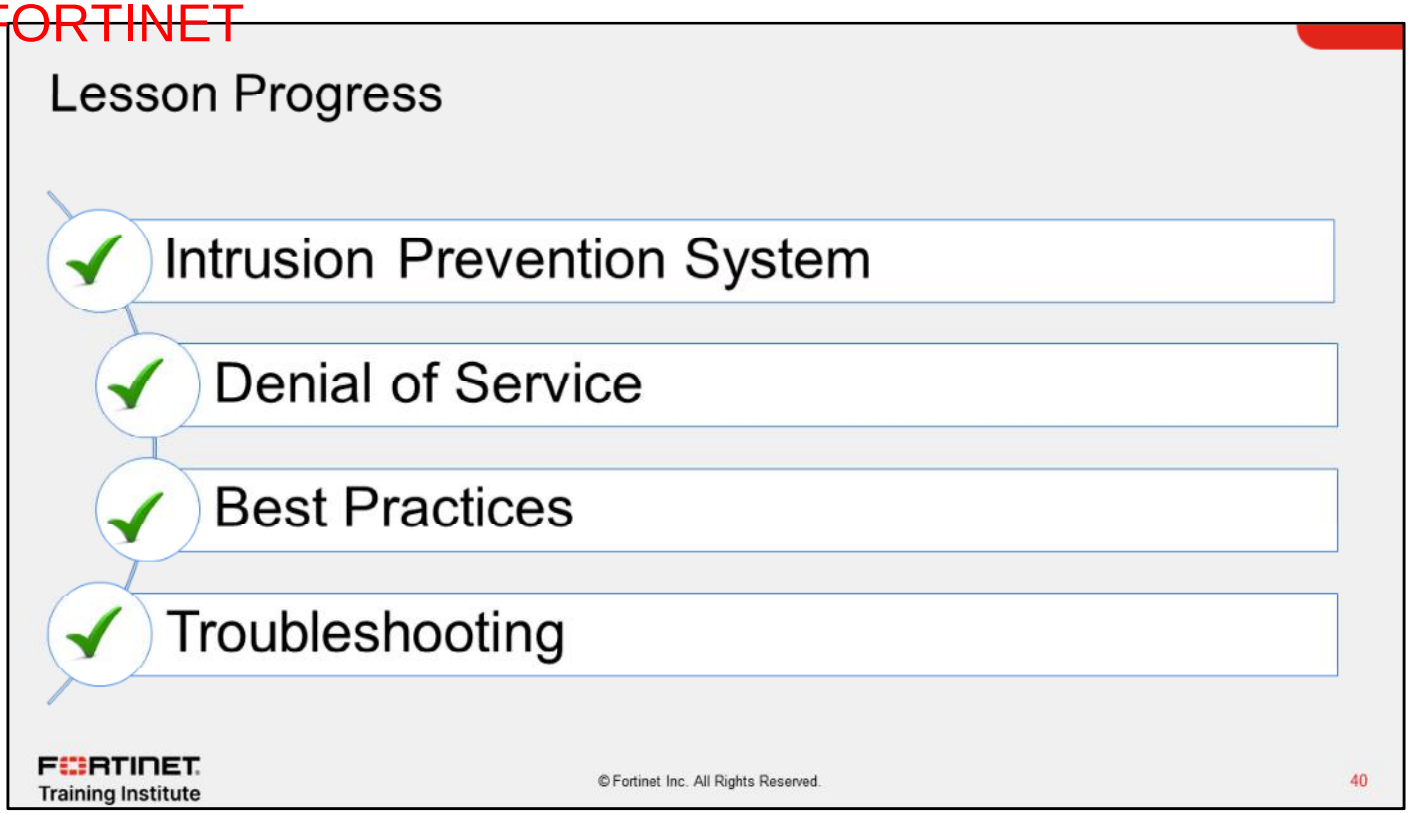
Knowledge Check

1. Which FQDN does FortiGate use to obtain IPS updates?
   - ✓ A. update.fortiguard.net
   - B. service.fortiguard.com

2. When IPS fail open is triggered, what is the expected behavior, if the IPS fail-open option is set to enabled?
   - ✓ A. New packets pass through without inspection
   - B. New packets are dropped

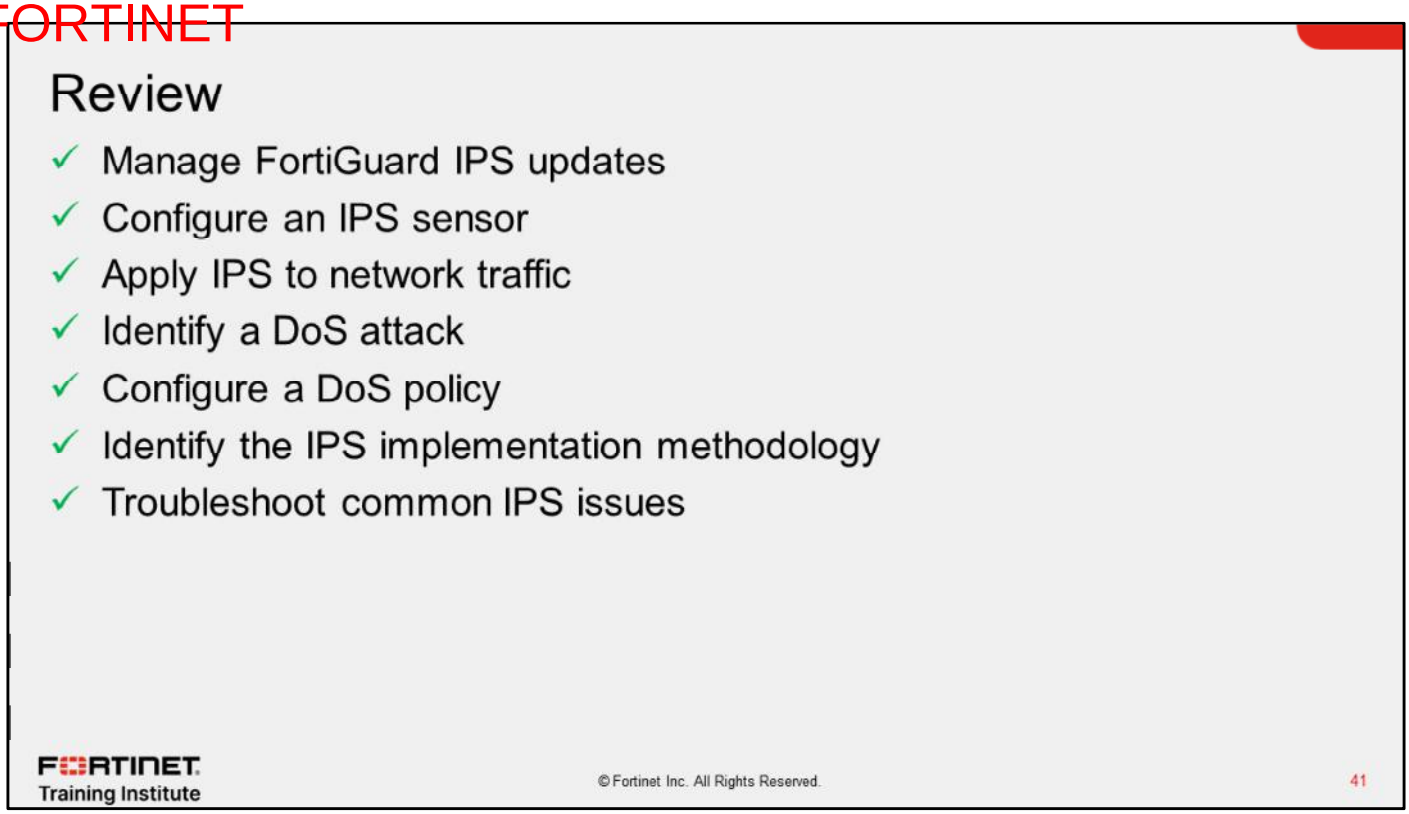
FORTINET Training Institute

39



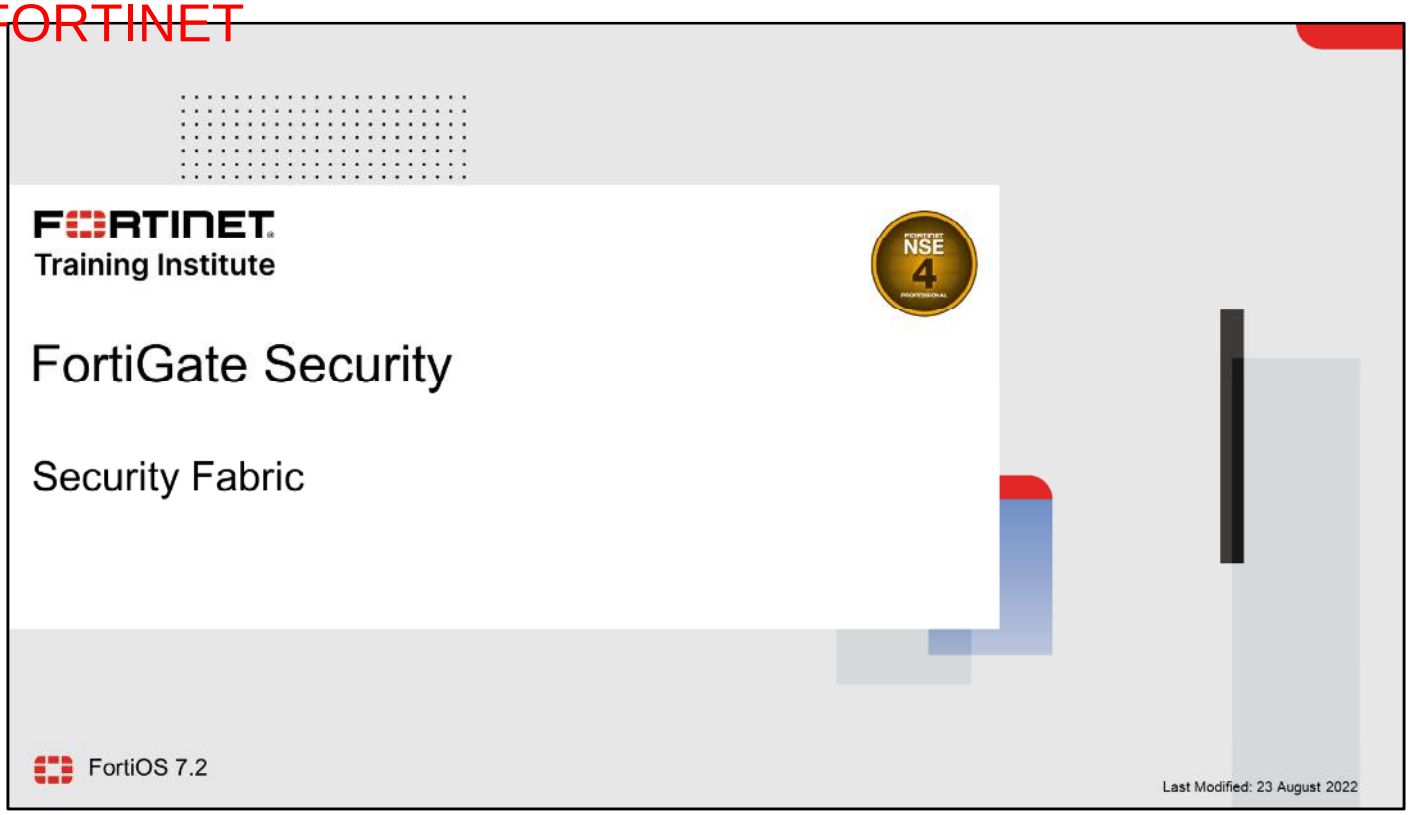
Congratulations! You have completed this lesson.

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

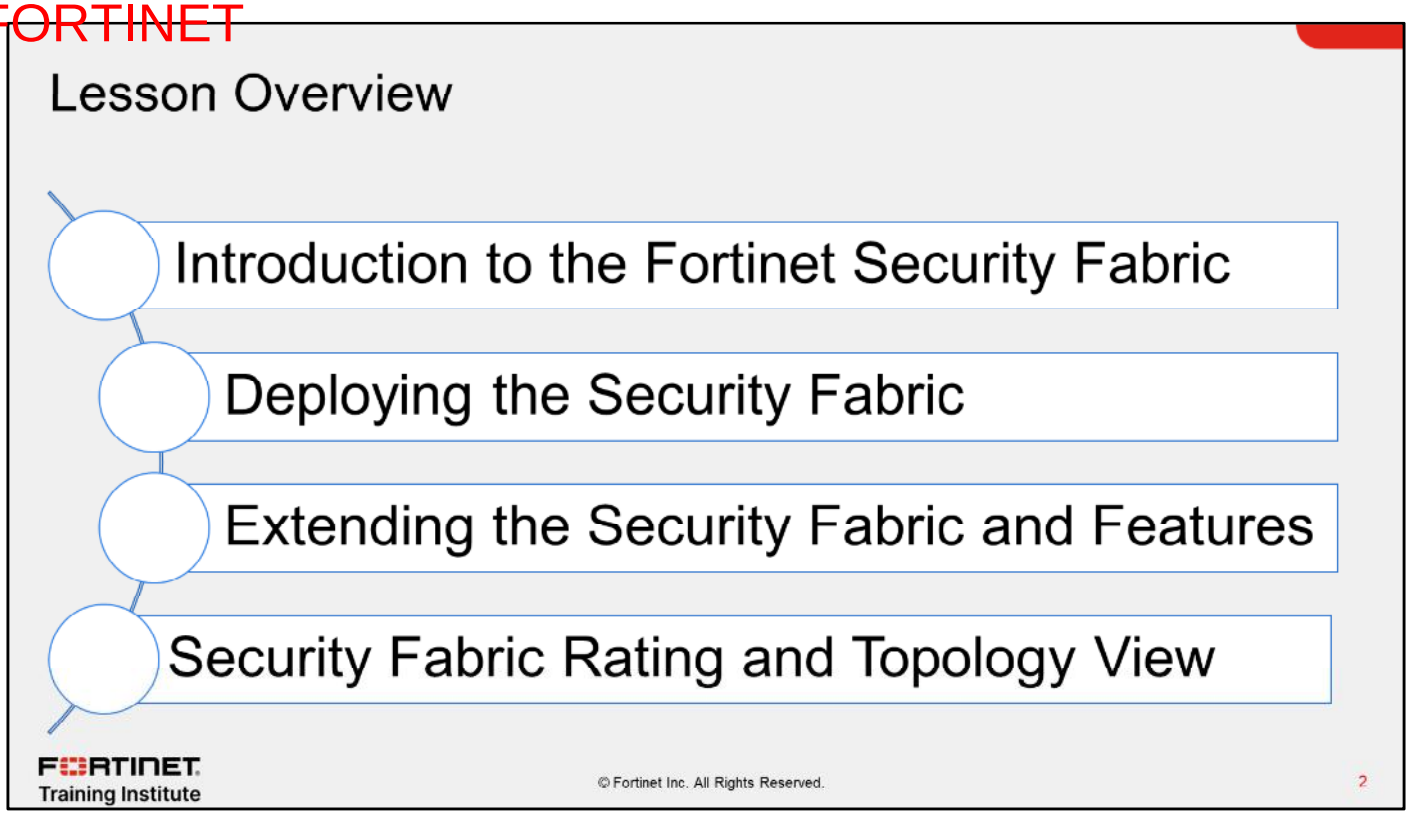


This slide shows the objectives that you covered in this lesson.

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

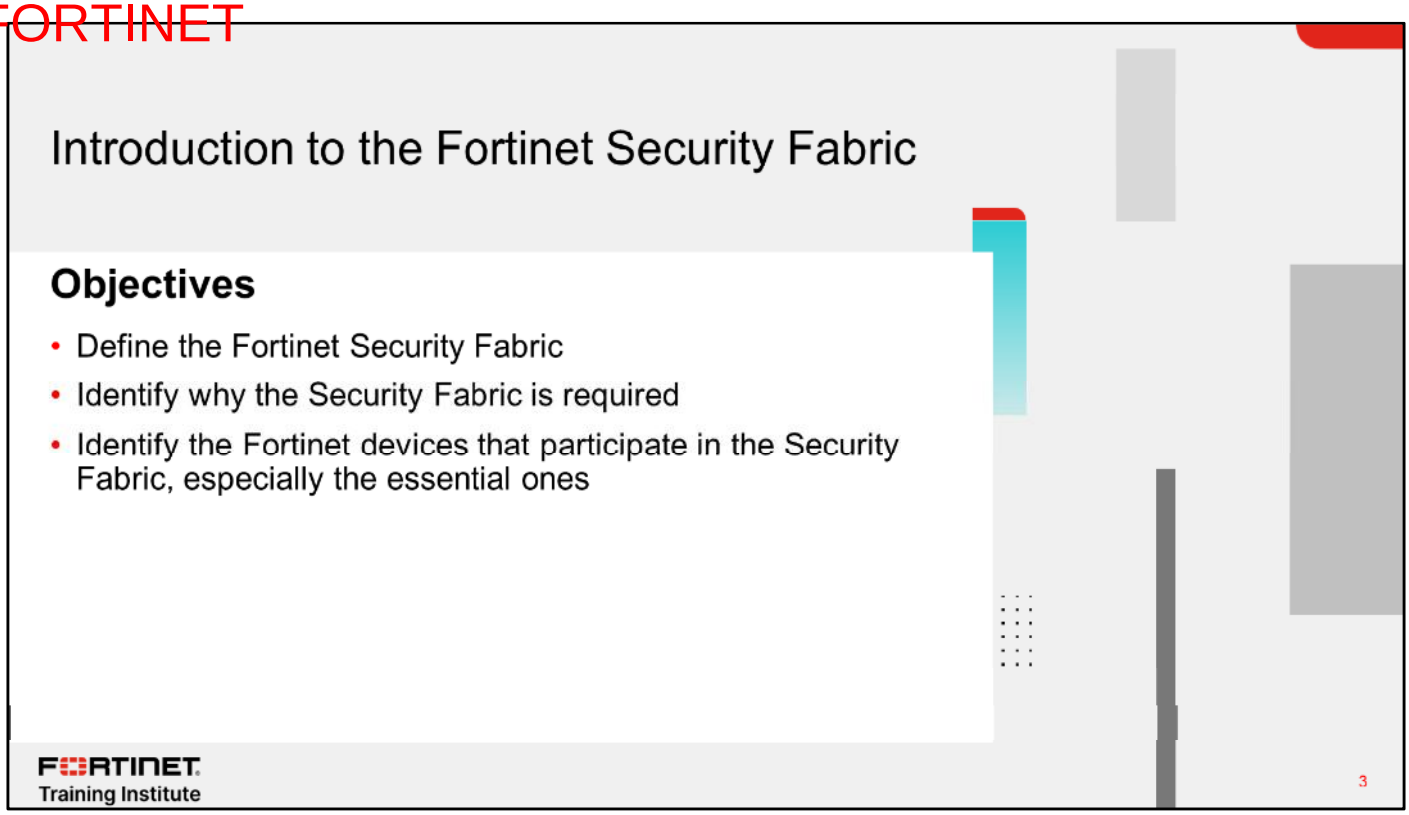


In this lesson, you will learn about the Fortinet Security Fabric.



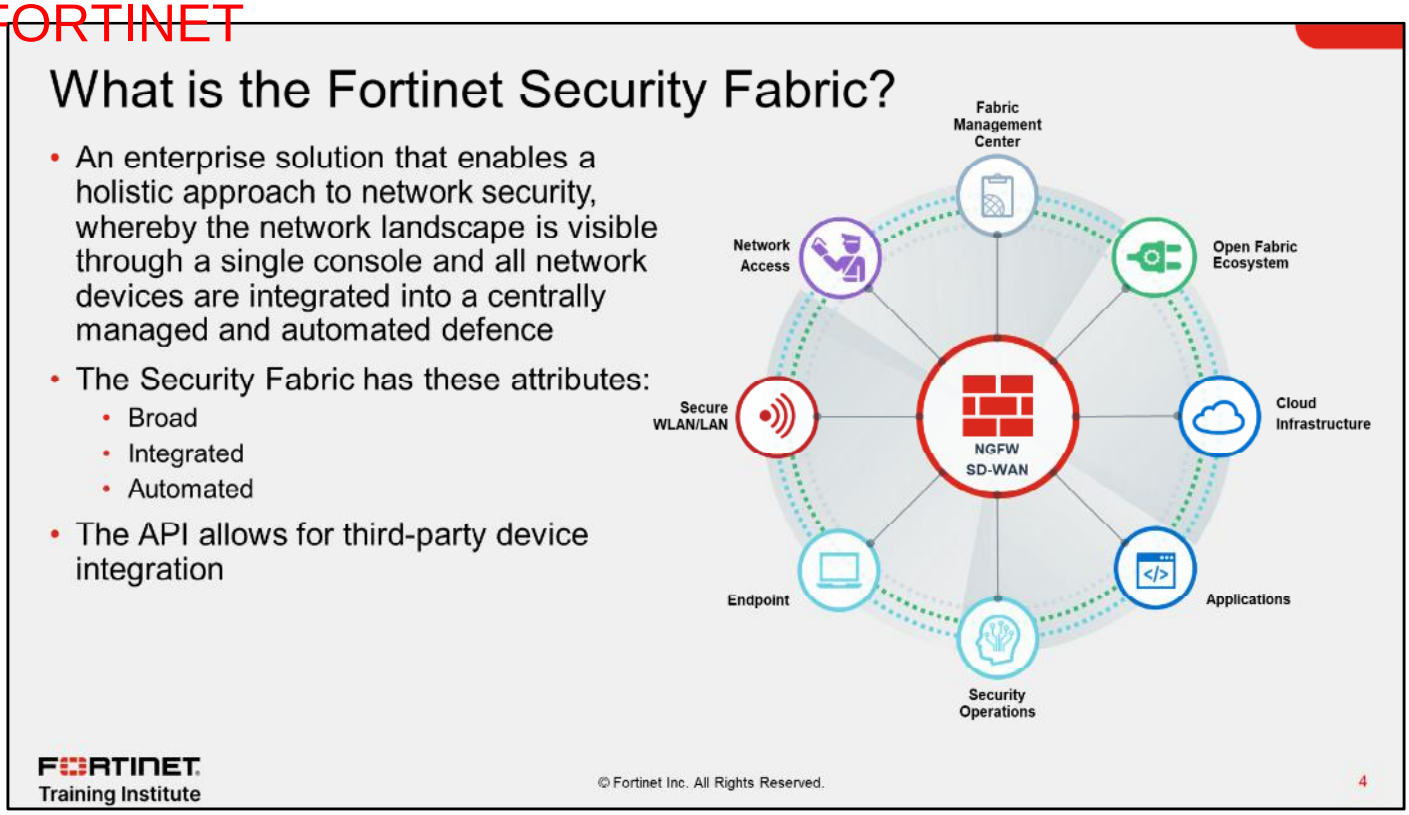
In this lesson, you will learn about the topics shown on this slide.

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



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

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



What is the Fortinet Security Fabric?

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

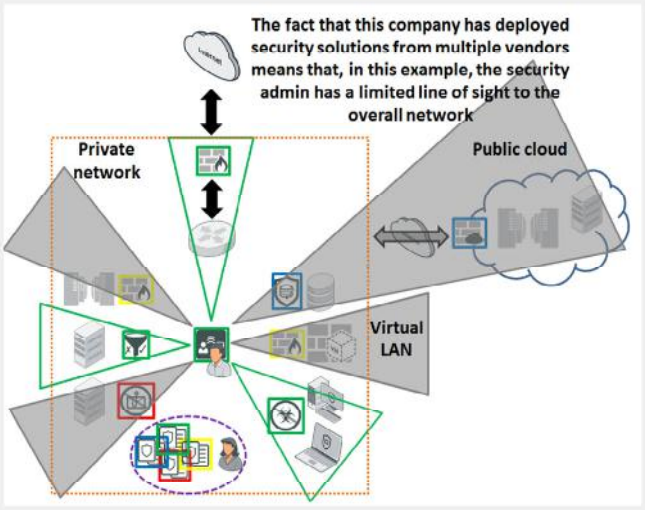
The network devices include all components, from physical endpoints to virtual devices in the cloud. Because devices are centrally managed and are sharing threat intelligence with one another in real time, and are receiving updates from Fortinet at the macro level, your network can quickly identify,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

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

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

Why a Security Fabric?

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



FORTINET Training Institute

5

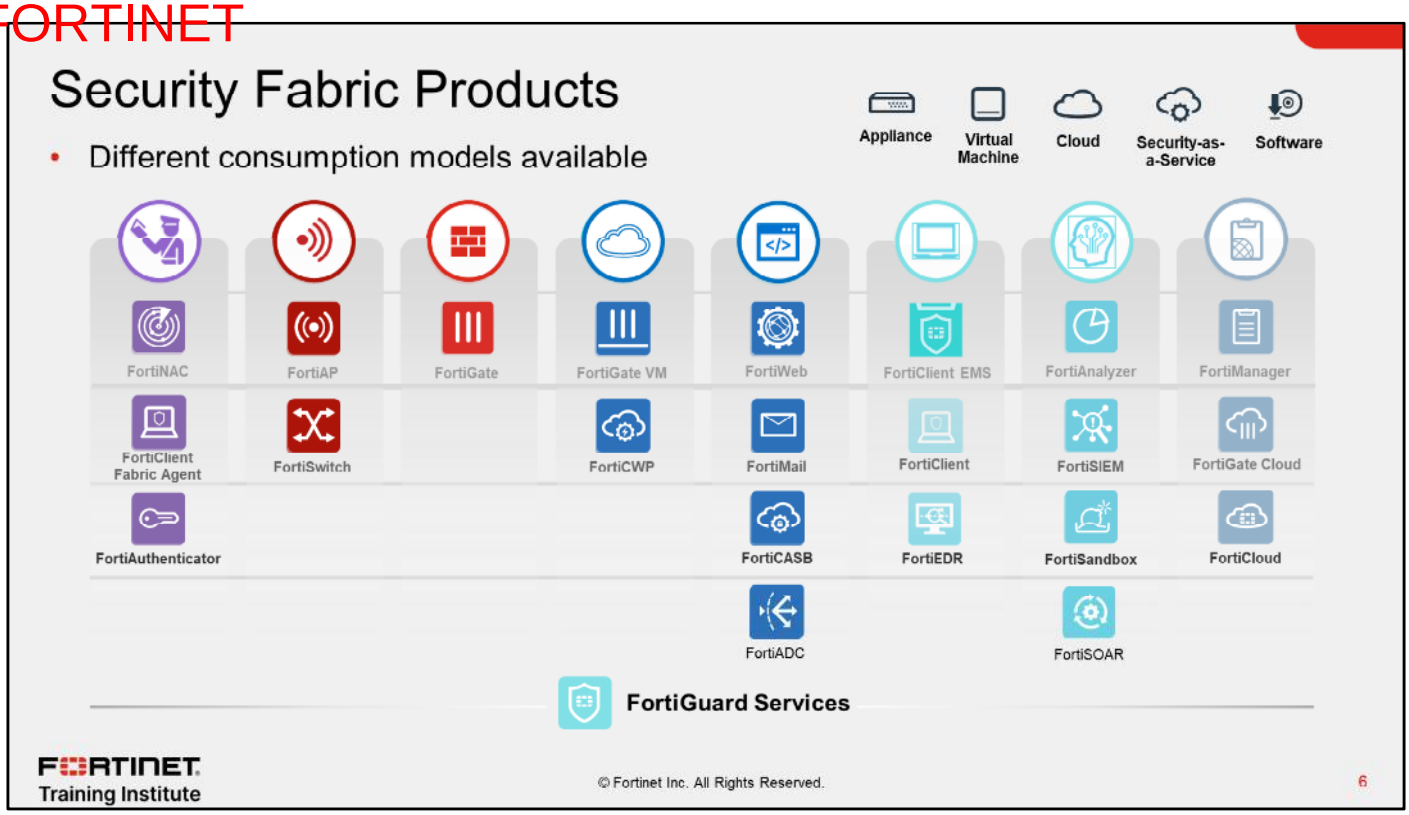
Why has Fortinet deemed the Security Fabric an essential solution for a robust network defence?

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

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

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

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

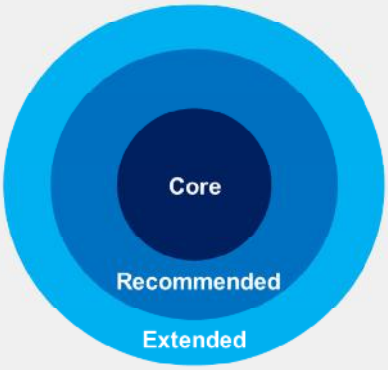


As shown on this slide, the Fortinet Security Fabric offers eight solutions: network access, security WLAN/LAN, public and private cloud infrastructure, applications, endpoint, security operations, open fabric ecosystem, and fabric management center. Each of these solutions is based on specific use cases and involve the integration of specific Fortinet products.

The Fortinet Security Fabric offers network security with FortiGate, IPS, VPN, SD-WAN. It also offers multi-cloud strategy across public clouds, private clouds, hybrid clouds, and software as a service (SaaS). It also offers quite a sophisticated endpoint offering ranging from the Fabric Agent all the way up to full endpoint protection, email security, web application security, secure access across distributed enterprises and SD-WAN environments, advanced threat protection, management and analytics, and security information and event management (SIEM).

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

Devices That Comprise the Security Fabric



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

FORTINET Training Institute

7

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

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

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

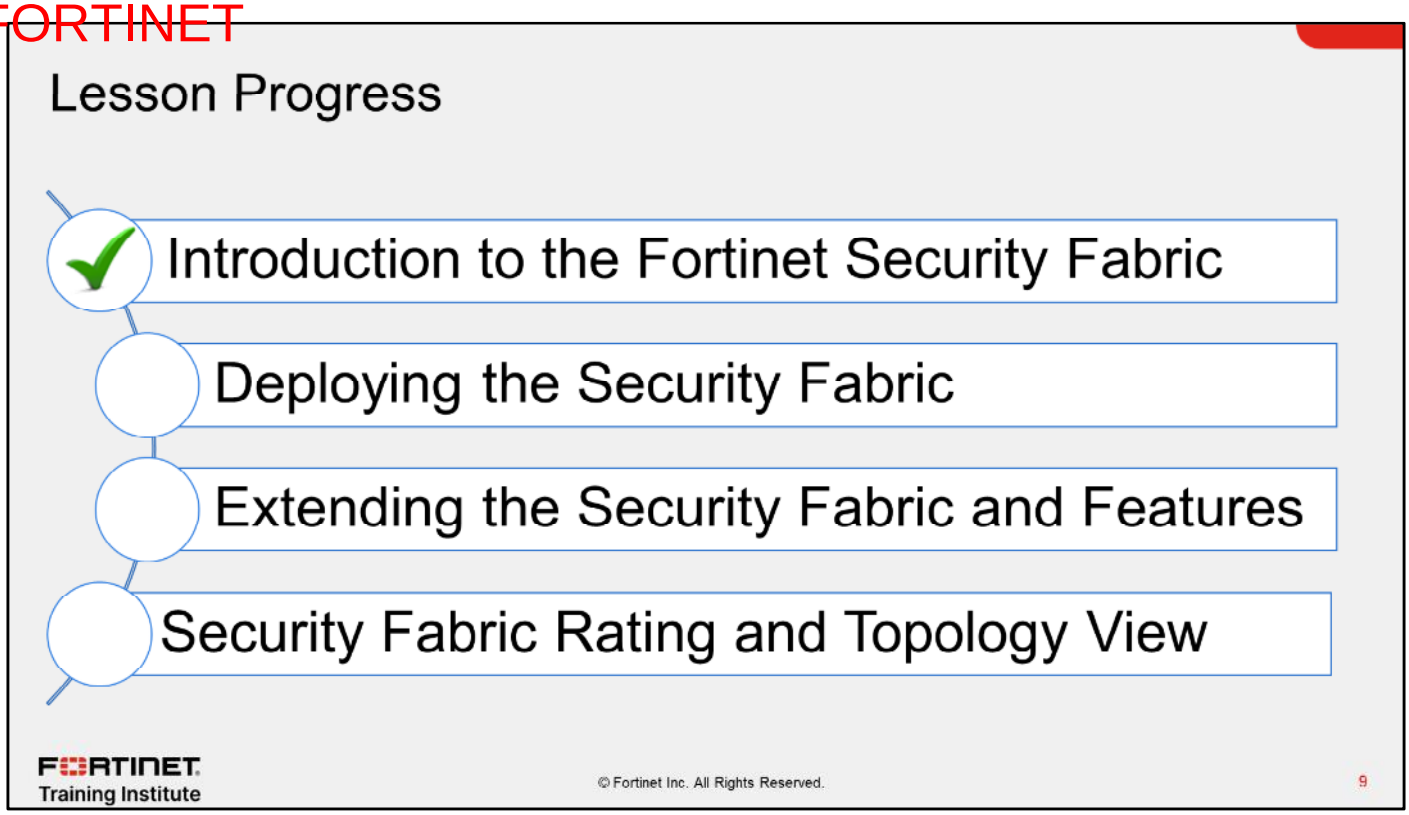
Knowledge Check

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

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

FORTINET Training Institute

8

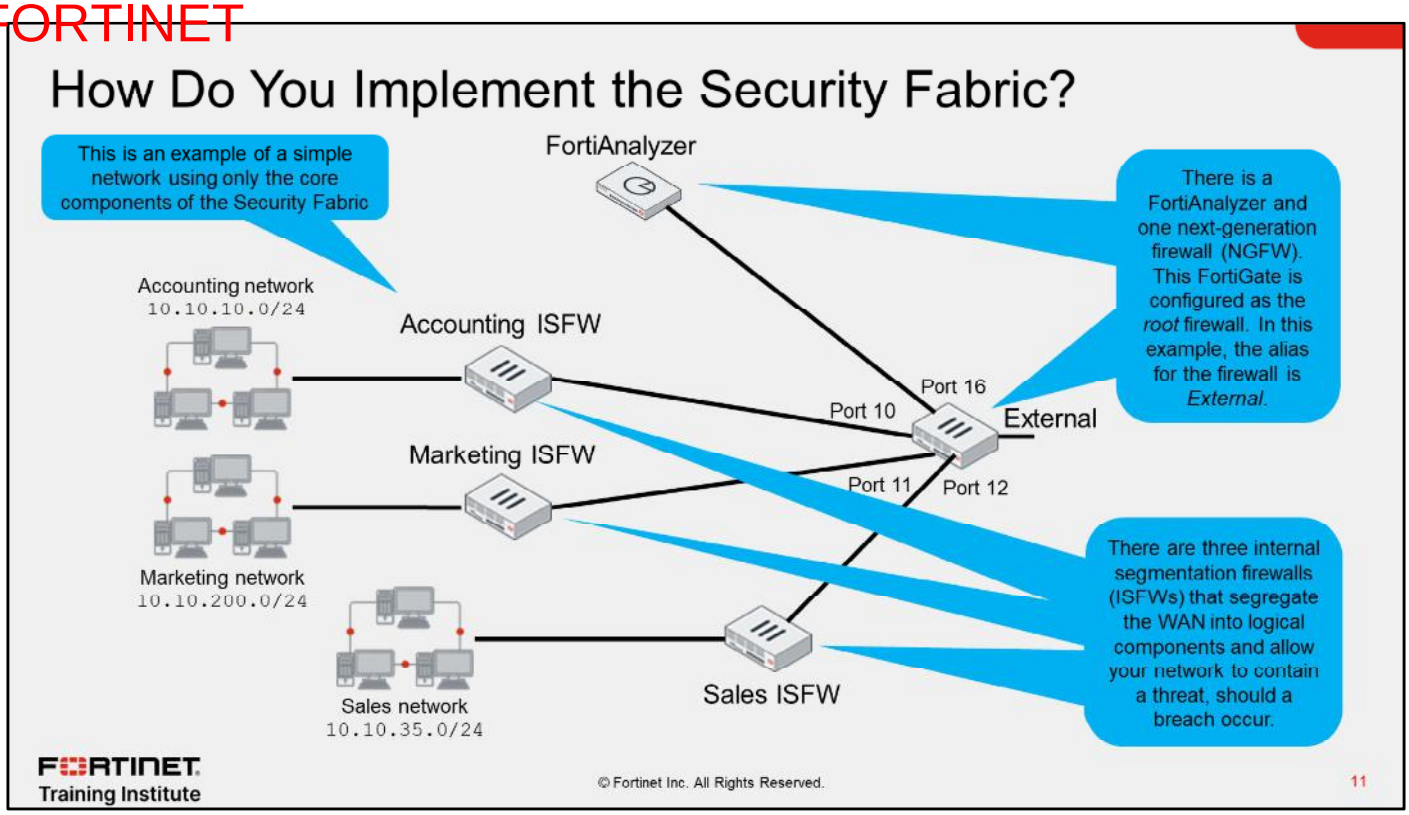


Good job! You now understand the basics of the Fortinet Security Fabric.

Next, you'll learn how to deploy the Security Fabric in your network environment.

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

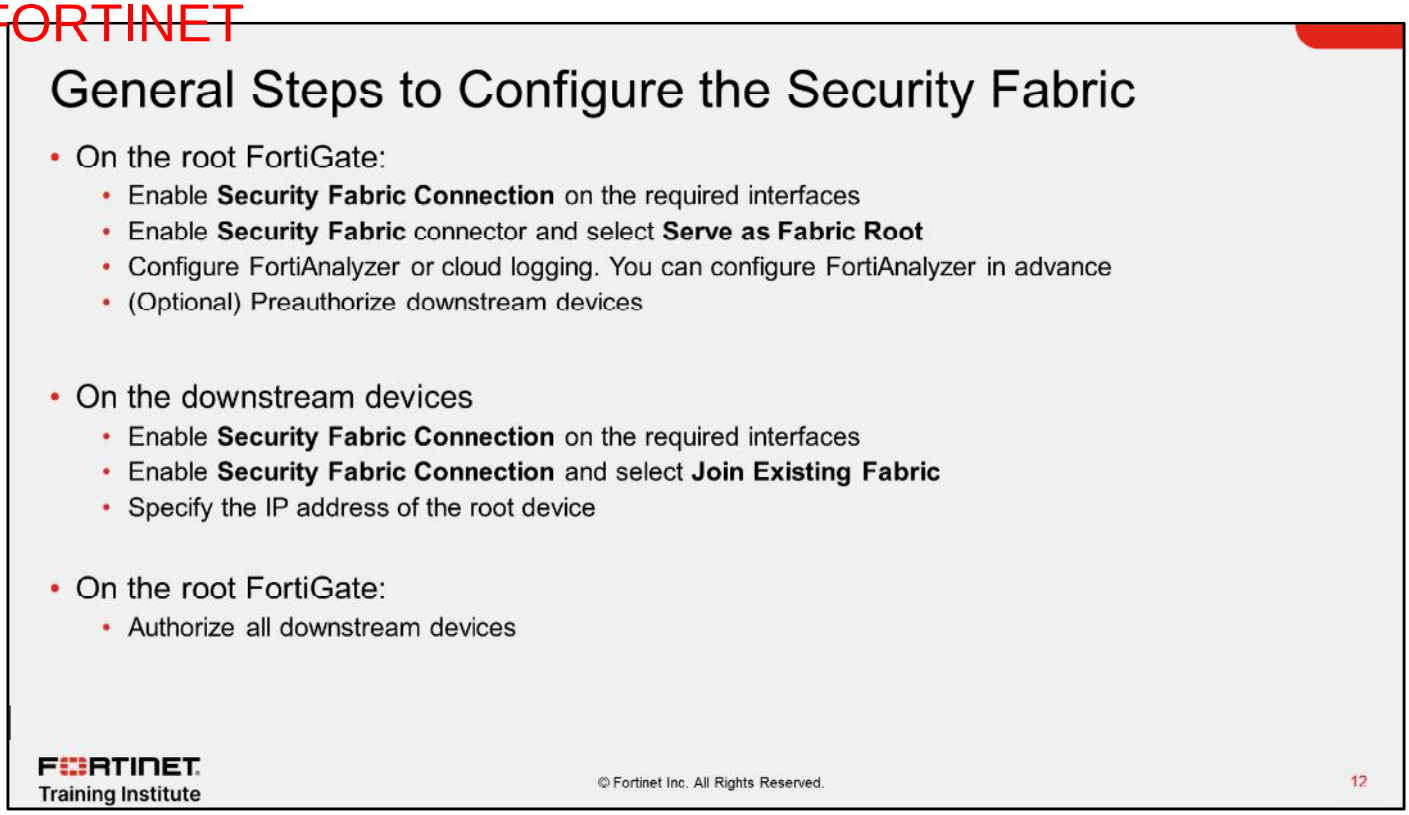
By demonstrating competence in the deployment of the Fortinet Security Fabric, you will better understand the value of the Security Fabric and how it helps to manage all your network devices more efficiently.



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

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

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



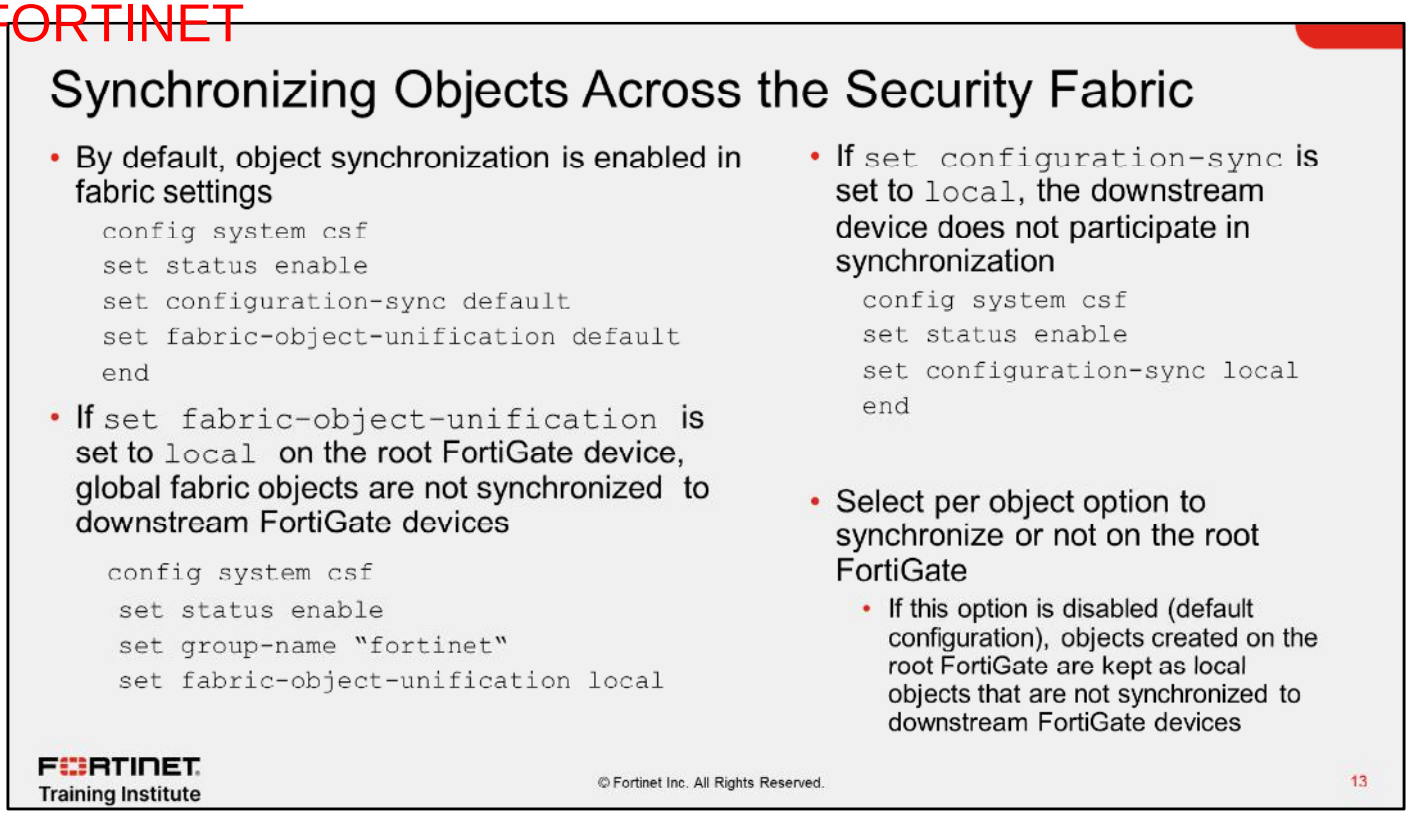
To configure a new security fabric, follow these general steps:

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

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

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

The third step in implementing the Security Fabric is to authorize the downstream FortiGate devices on the root FortiGate.

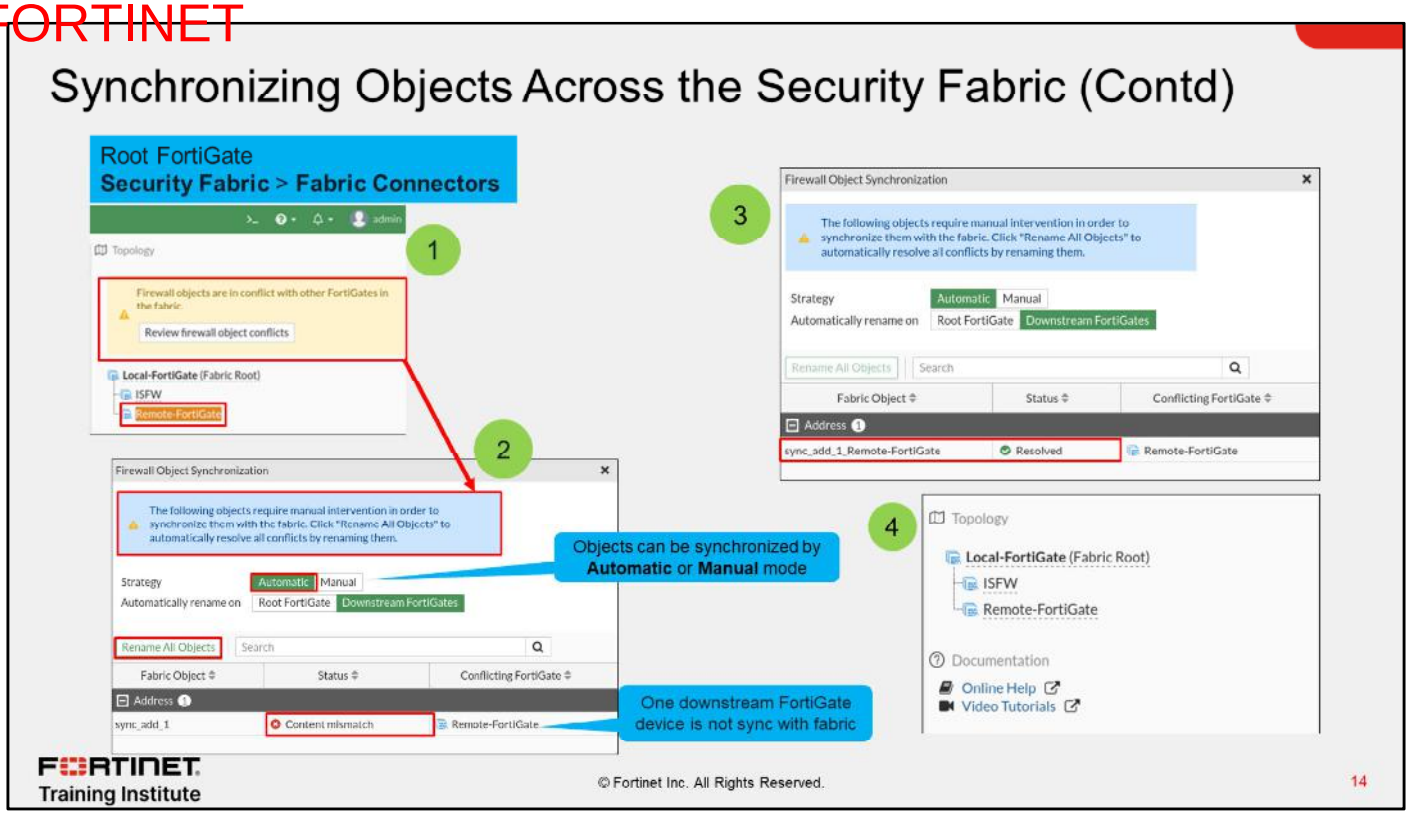


When the Security Fabric is enabled, settings to sync various objects, such as addresses, services, and schedules, from the upstream FortiGate to all downstream FortiGate devices is enabled by default. Synchronization always happens from the root FortiGate to downstream FortiGate devices. Any object that can be synced will be available on downstream FortiGate devices after synchronization.

The CLI command `set fabric-object-unification` is only available on the root FortiGate. When set to `local`, global objects will not be synchronized to downstream devices in the Security Fabric. The default value is `default`.

The CLI command `set configuration-sync local` is used when a downstream FortiGate doesn't need to participate in object synchronization. When set to `local` on a downstream FortiGate, the device does not synchronize objects from the root, but will still participate in sending the synchronized object downstream.

You can also enable or disable per object synchronization in the Security Fabric. This option is not available for objects you create on a downstream FortiGate. Fabric synchronization is disabled by default for supported fabric objects, and these fabric objects are kept as locally created objects on all the FortiGate devices in the Security Fabric. If object synchronization is disabled on the root FortiGate, using the command `set fabric-object disable`, firewall addresses and address groups will not be synchronized to downstream FortiGate devices.



If an object conflict occurs during synchronization, you'll get a notification in the topology tree.

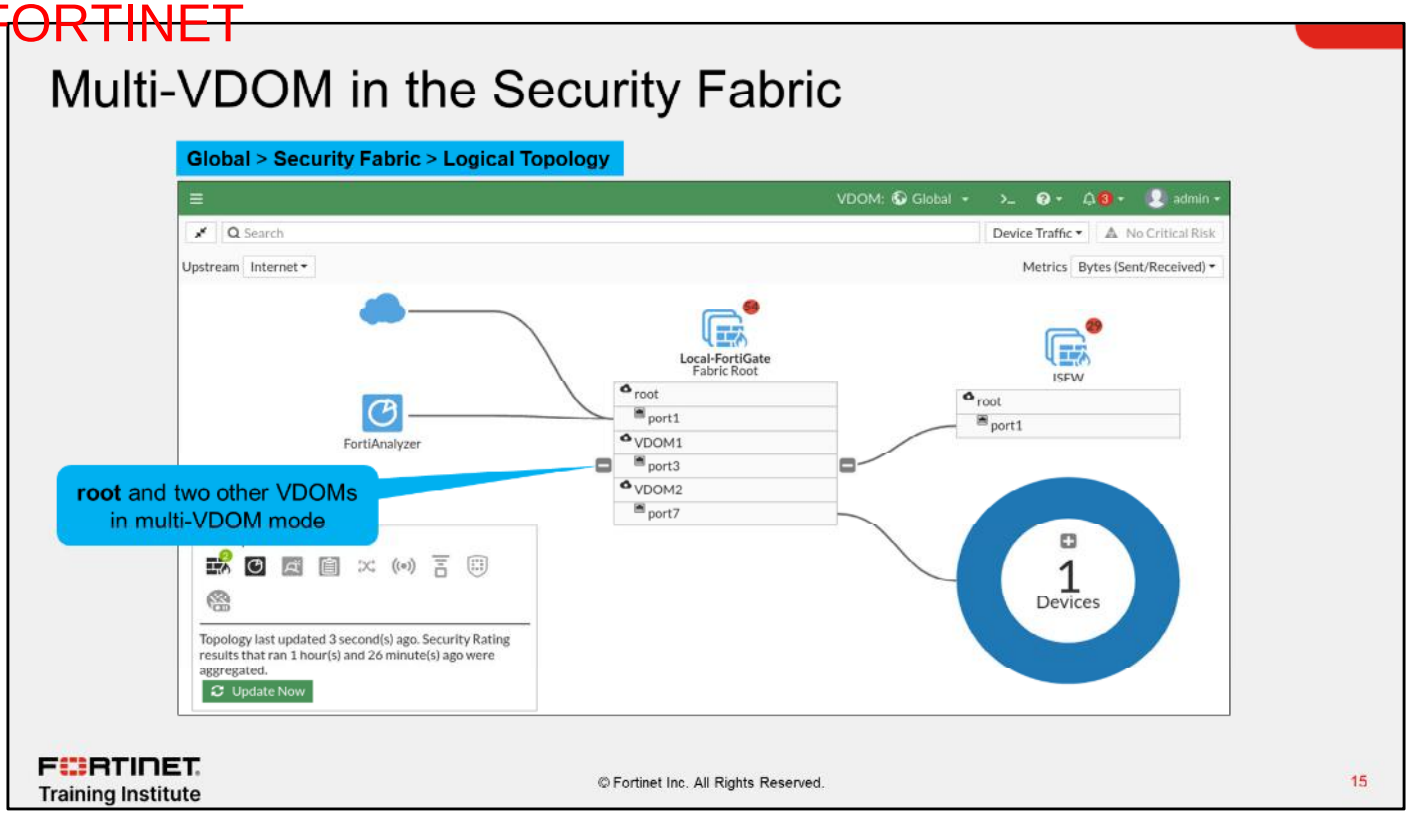
The process to resolve a syncing conflict is as follows:

1. The notification icon displays this message: **Firewall objects are in conflict with other FortiGates in the fabric**. **Remote-FortiGate** is highlighted in amber. Click **Review firewall object conflicts**.

2. On the **Firewall Object Synchronization** page, you can see that both the root FortiGate and downstream FortiGate devices contain the **synn_add_1** object (with a different IP address/subnet schema on each device), causing a status of **Content mismatch**. In the **Strategy** field, there are two options to resolve the conflict: **Automatic** and **Manual**. If you select **Automatic**, as shown in this example, you can then click **Rename All Objects**.

3. **Remote-FortiGate** is appended to the name of the downstream FortiGate device **sync_Add_1** address object and the status changes to **Resolved**.

4. In the topology tree, none of the FortiGate devices are highlighted because there is no conflict.



When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. *Only* the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable **Device Detection** on ports you want to have displayed in the **Security Fabric**. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single **Security Fabric**. In the example shown on this slide, the Local-FortiGate is configured in multi-VDOM mode, and has three VDOMs (root, VDOM1, and VDOM2), each with ports that have connected devices.

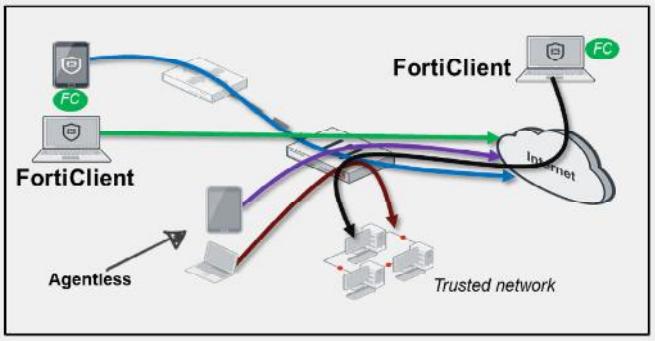
Device Identification–Agentless vs. Agent

Agentless

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

Agent (FortiClient)

- Location and infrastructure independent



FORTINET Training Institute

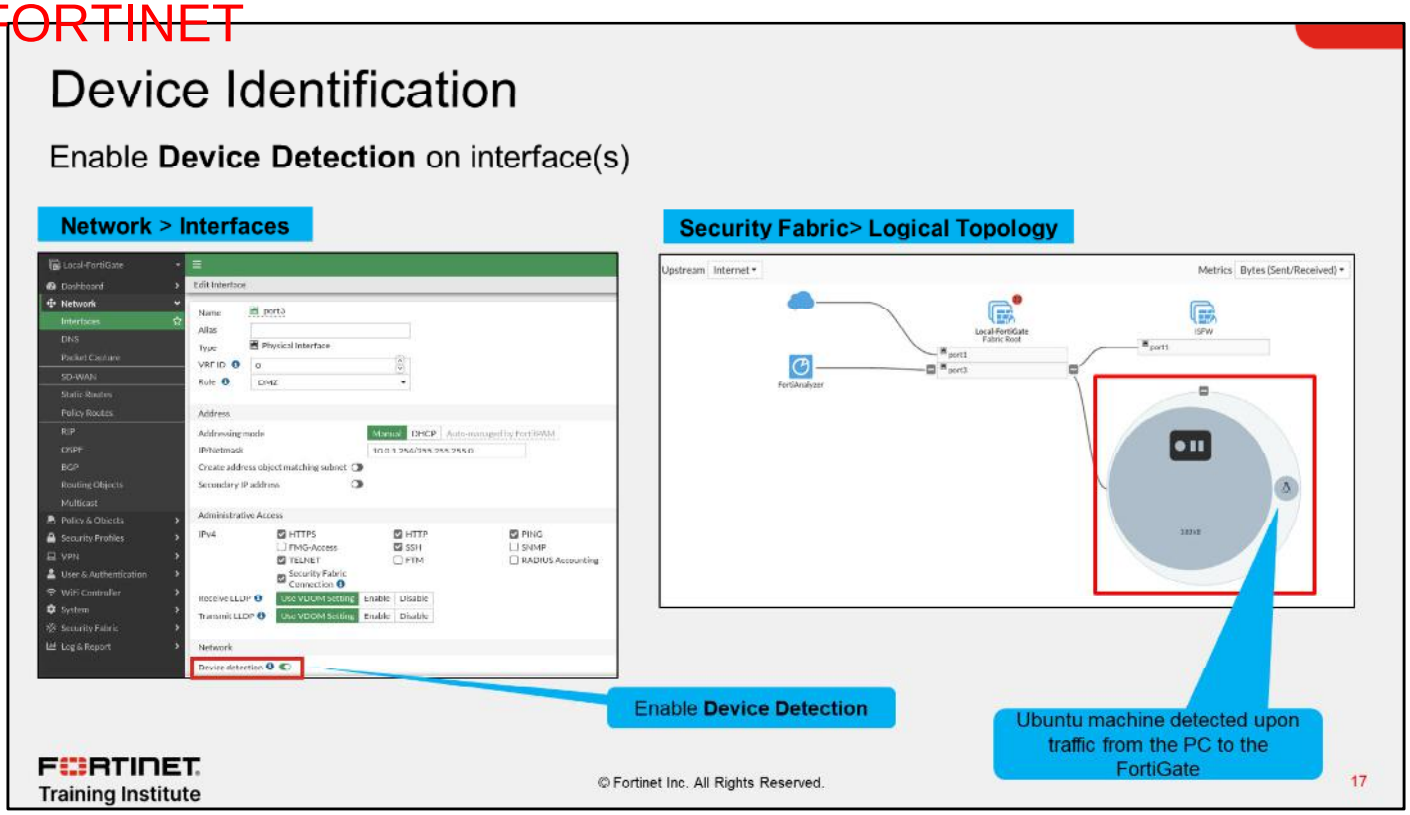
16

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

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

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

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



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

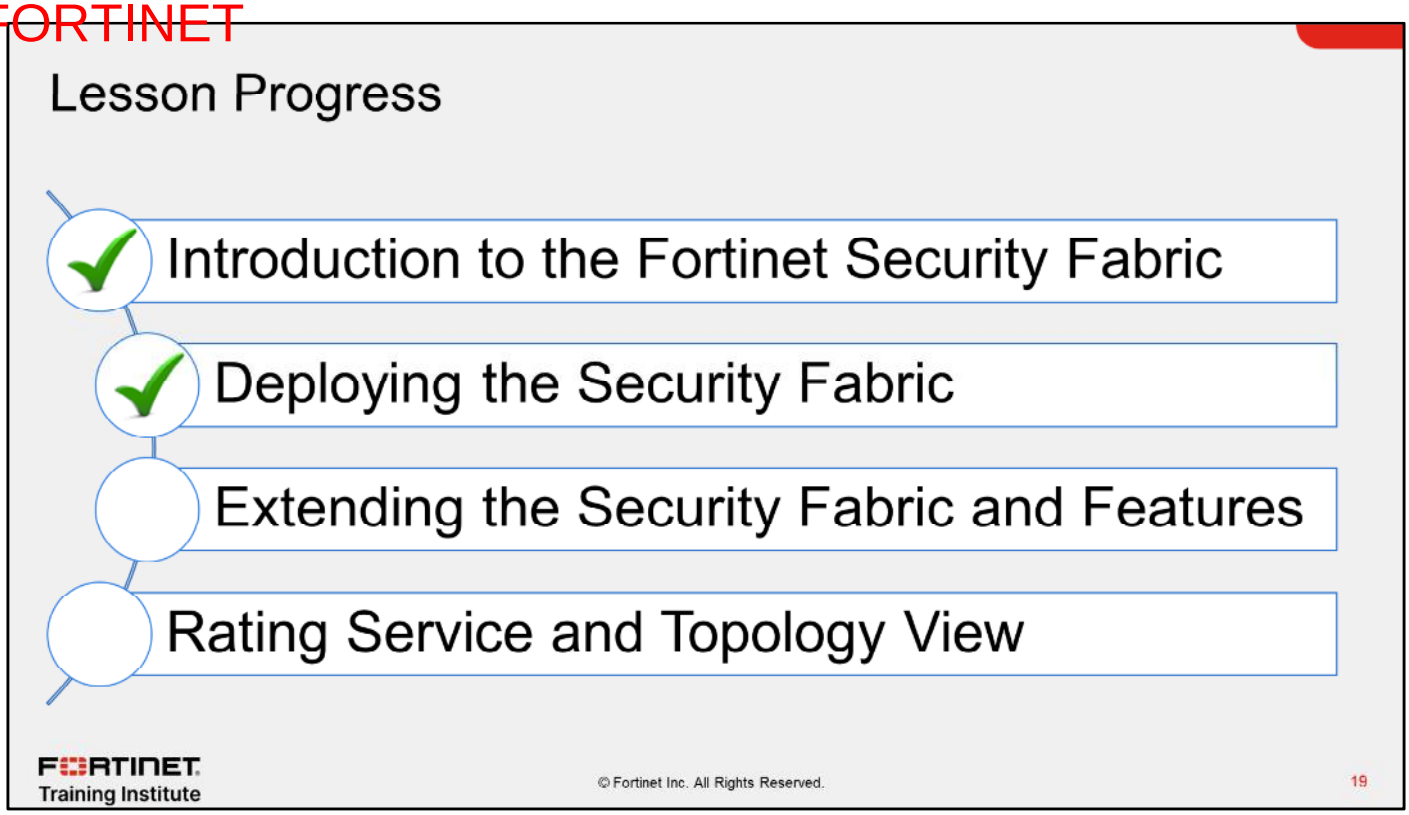
Knowledge Check

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

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

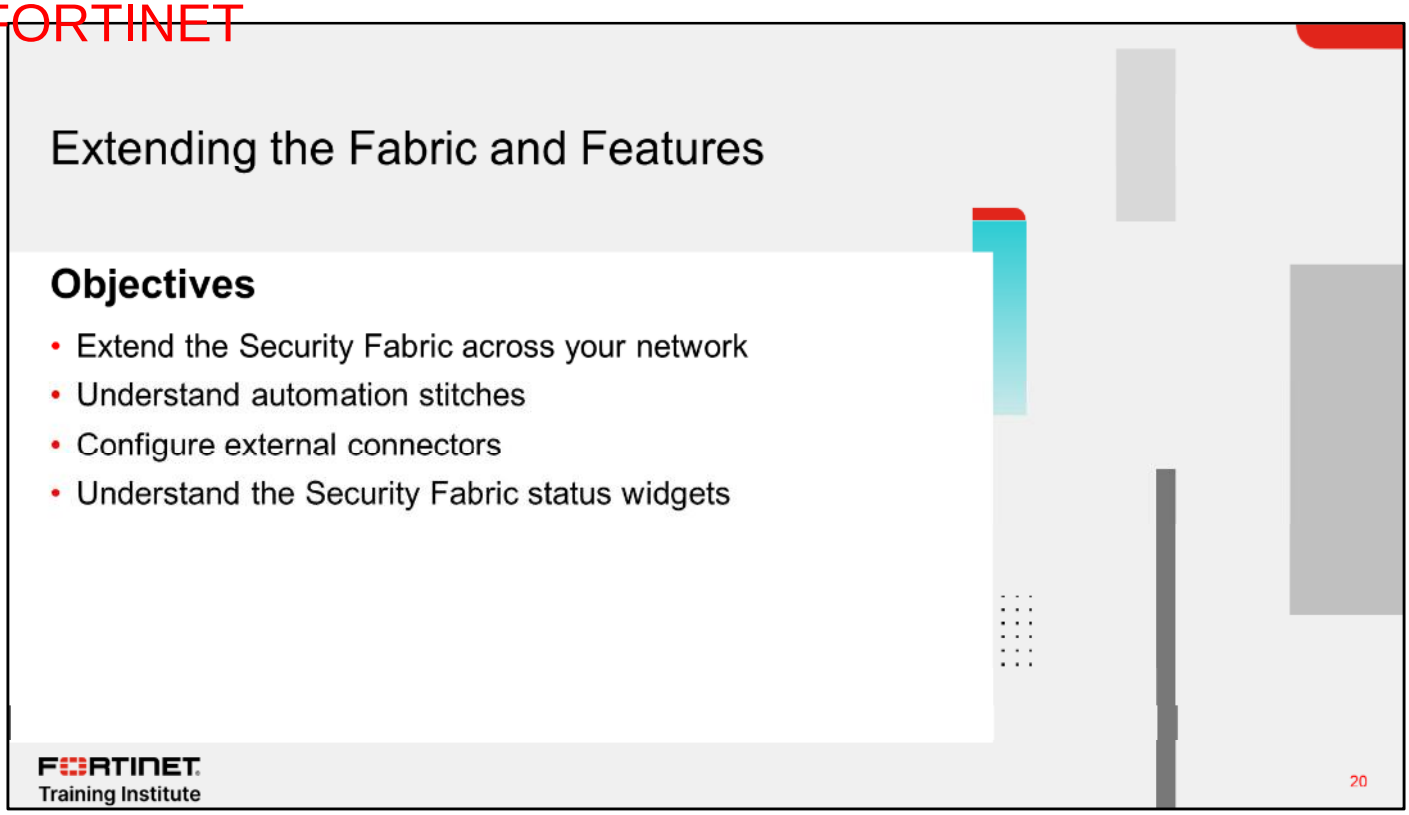
FORTINET Training Institute

18



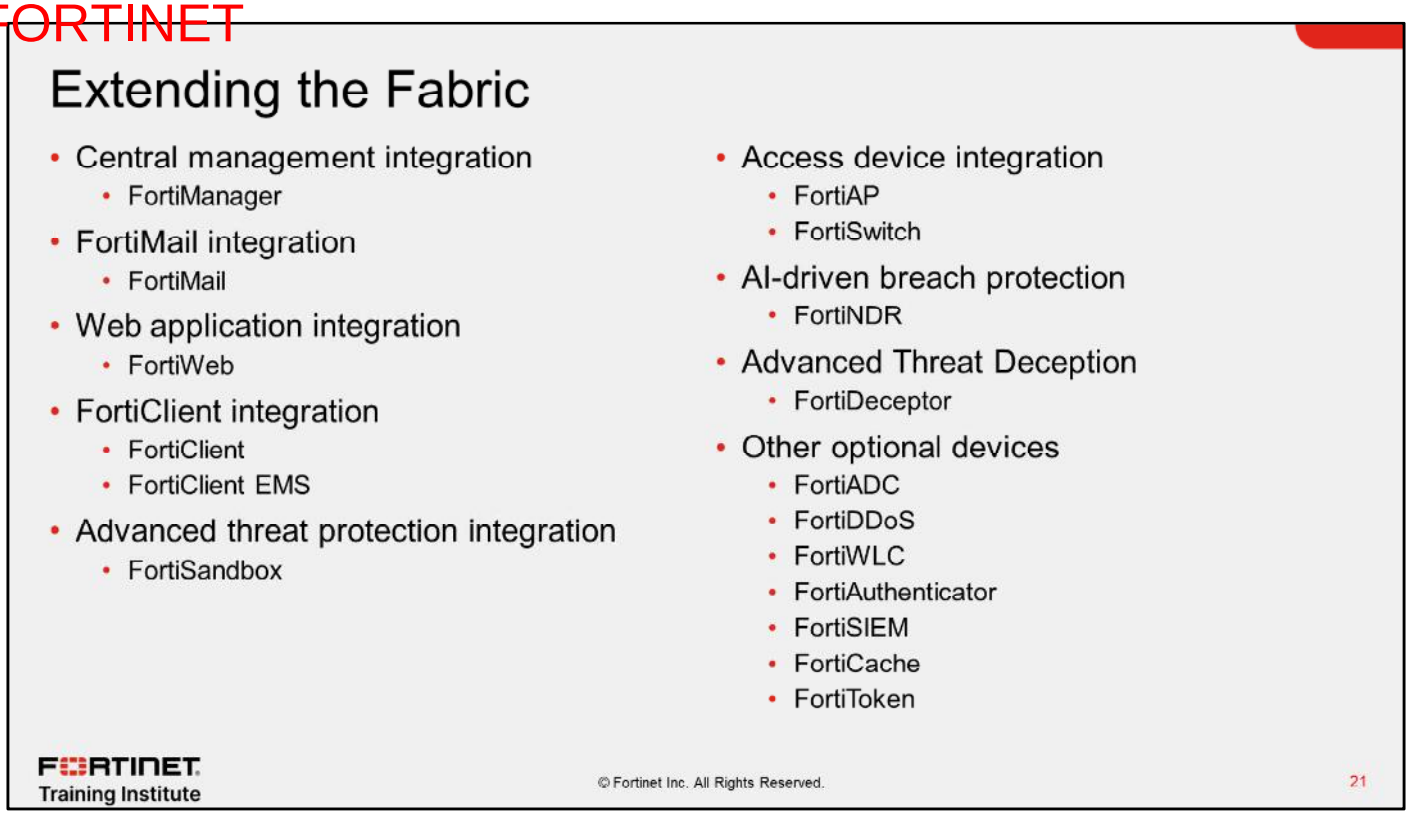
Good job! You now know how to deploy the Security Fabric.

Next, you'll learn about Security Fabric features and how to extend the Security Fabric in your network environment.



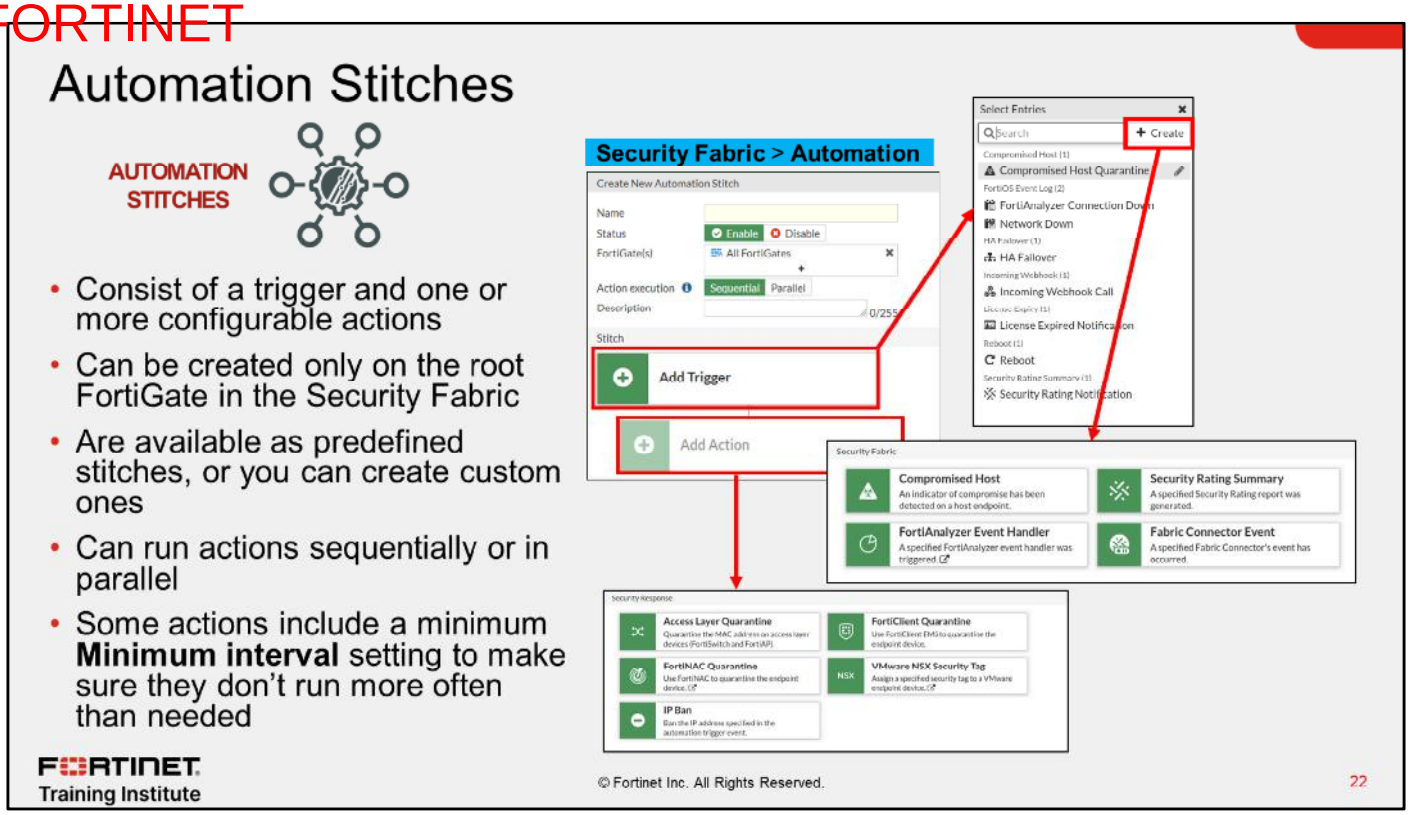
After completing this section, you should be able to achieve the objectives shown on this slide.

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



The slide shows the list of products that Fortinet recommends to extend the Security Fabric.

For example, Fortinet recommends using a FortiManager for centralized management of all FortiGate devices and to access devices in the Security Fabric. You can also extend the Security Fabric down to the access layer by integrating FortiSwitch and FortiAP devices.

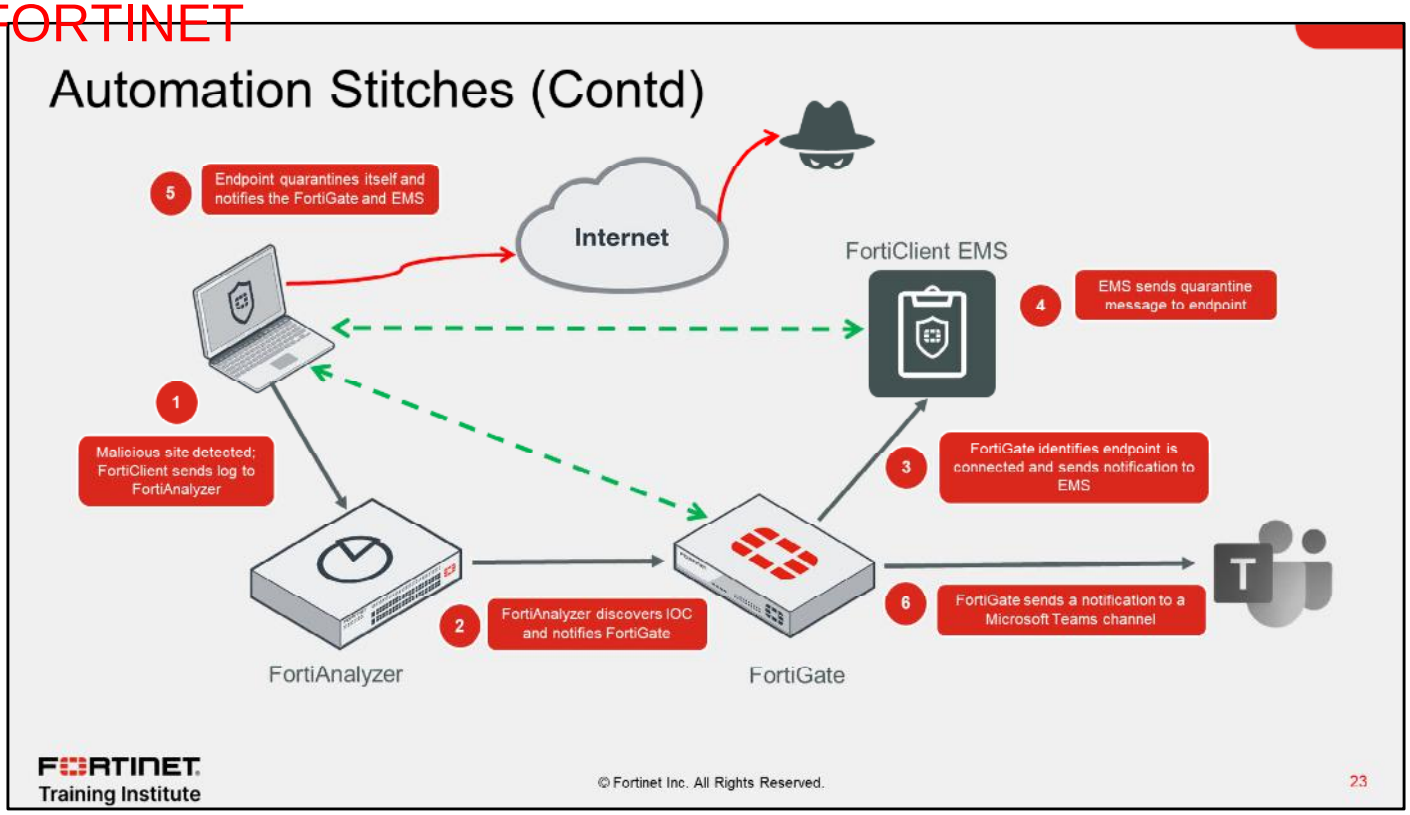


Administrator-defined automated workflows (called stitches) cause FortiOS to automatically respond to an event in a preprogrammed way. Because this workflow is part of the Security Fabric, you can set up automation stitches for any device in the Security Fabric. However, the Security Fabric is not required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

Each automation stitch pairs a trigger and one or more actions. FortiOS has several predefined stitches, triggers and actions. However, you can create custom automation based on the available options.

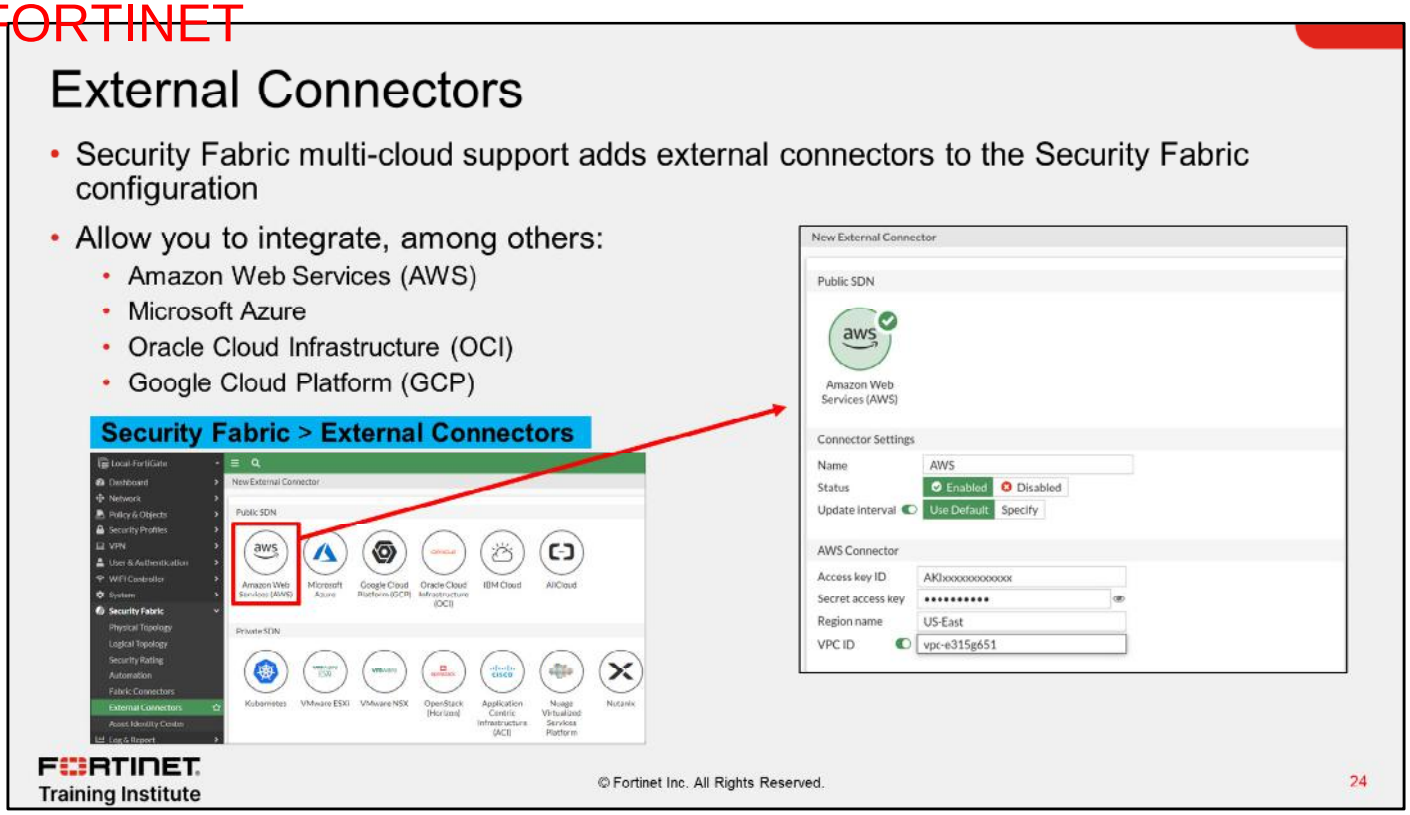
Automation stitches allow you to monitor your network and take appropriate action when the Security Fabric detects a threat. You can use automation stitches to detect events from any source in the Security Fabric and apply actions to any destination.

You can configure the **Minimum internal (seconds)** setting on some of the available actions to make sure they don't run more often than needed.



This slide shows an example of how automation stitches can be configured to work in the Security Fabric:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies FortiGate.
3. FortiGate identifies whether FortiClient is a connected endpoint, and whether it has the login credentials for the FortiClient EMS that FortiClient is connected to. With this information, FortiGate sends a notification to FortiClient EMS to quarantine the endpoint.
4. FortiClient EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies FortiGate and EMS of the status change.
6. FortiGate sends a notification to a Microsoft Teams channel to alert the administrators about the event.

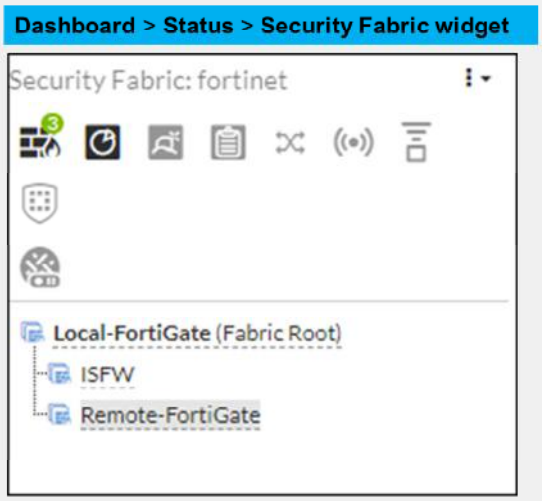


External connectors allow you to integrate multi-cloud support, such as Microsoft Azure and AWS, among others.

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

The Security Fabric Status Widget

- The name of your Security Fabric
- Icons indicating the other devices in the Security Fabric
- The names of the FortiGate devices in the Security Fabric



FORTINET Training Institute

25

The **Security Fabric Status** widget shows a visual summary of the devices in the Security Fabric.

You can hover over the icons at the top of the widget to display a quick view of their statuses. From here, you can click to authorize FortiAP and FortiSwitch devices that are connected to an authorized FortiGate.

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

- Devices in blue are connected in your network.
- Devices in gray are not configured, or not detected in your network.
- Devices in red are no longer connected, or not authorized in your network.

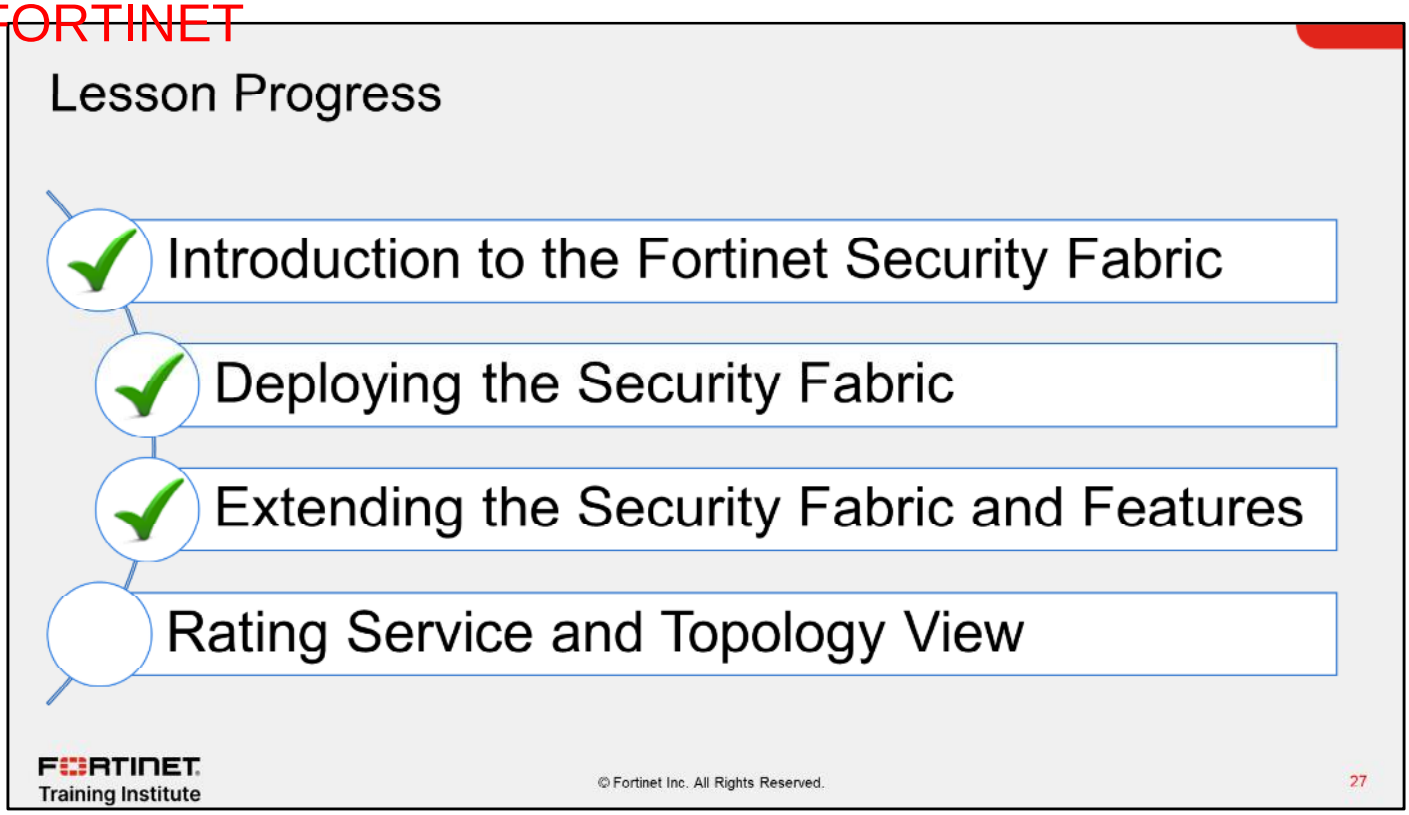
Knowledge Check

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

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

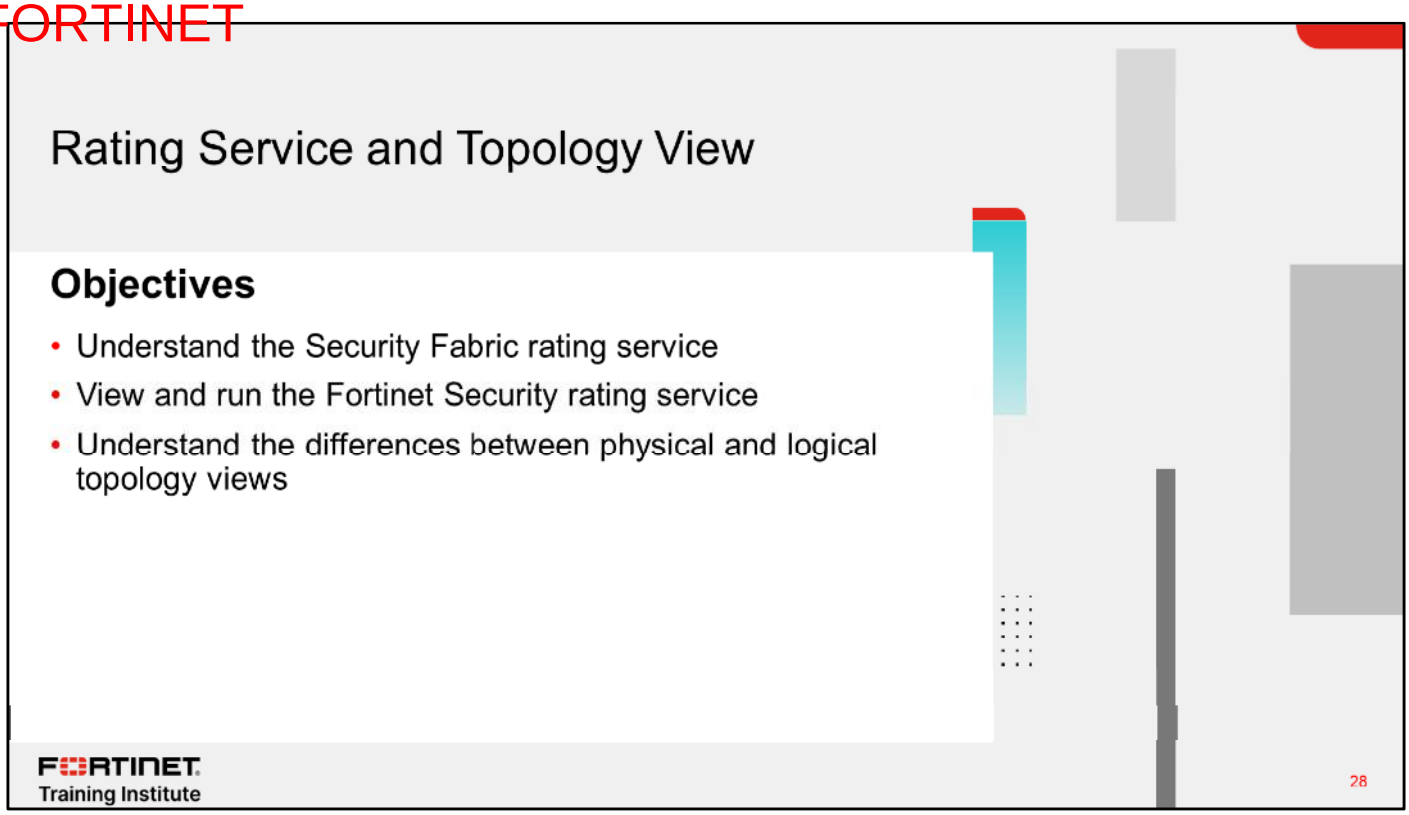
FORTINET Training Institute

26



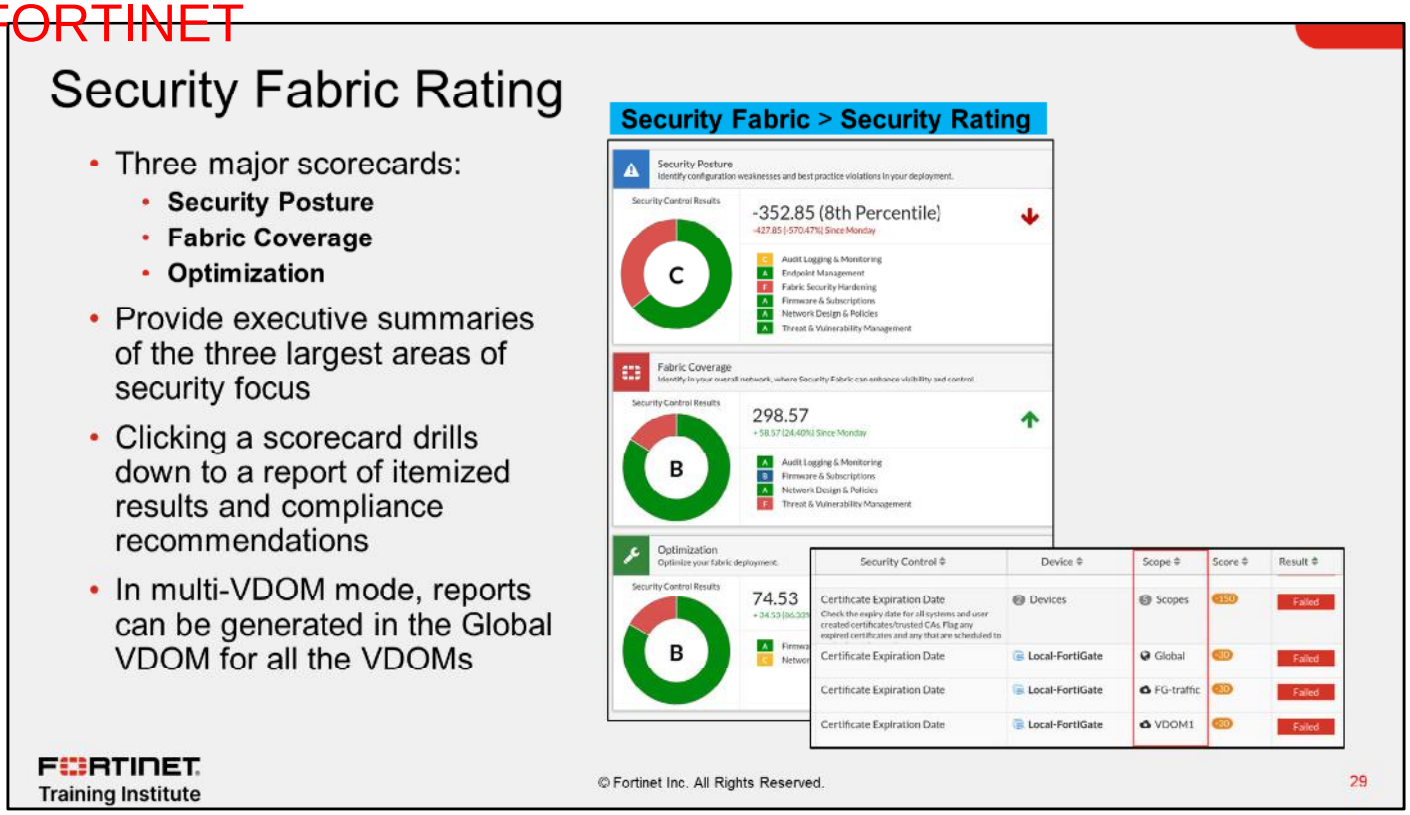
Good job! You now know how to extend the Security Fabric and its features.

Next, you'll learn about the Security Fabric Rating service and topology view.



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

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



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

The **Security Rating** page is separated into three major scorecards: **Security Posture, Fabric Coverage**, and **Optimization**.

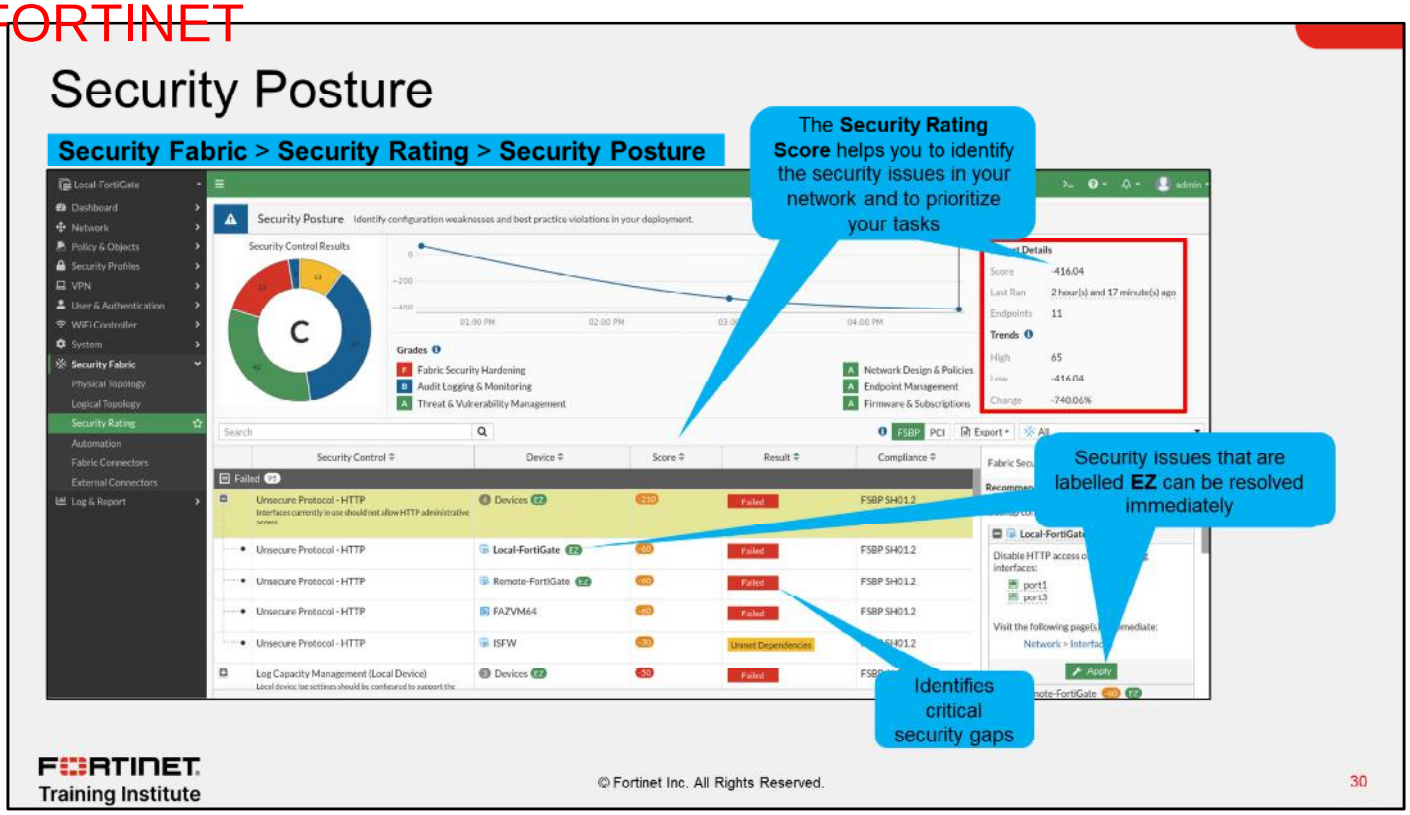
These scorecards provide executive summaries of the three largest areas of security focus in the Security Fabric.

The scorecards show an overall letter grade and breakdown of the performance in subcategories. Click a scorecard to drill down to a detailed report of itemized results and compliance recommendations. The point score represents all passed and failed items in that area. The report includes the security controls that were tested, linking them to specific FSBP or PCI compliance policies. You can click **FSBP** and **PCI** to reference the corresponding standard.

In multi-VDOM mode, administrators with read/write access can generate security rating reports in the Global VDOM for all the VDOMs on the device. Administrators with read-only access can view the report, but not generate it.

On the scorecards, the **Scope** column shows the VDOM or VDOMs that the security rating checked. On checks that support **Easy Apply**, you can run the remediation on all the associated VDOMs.

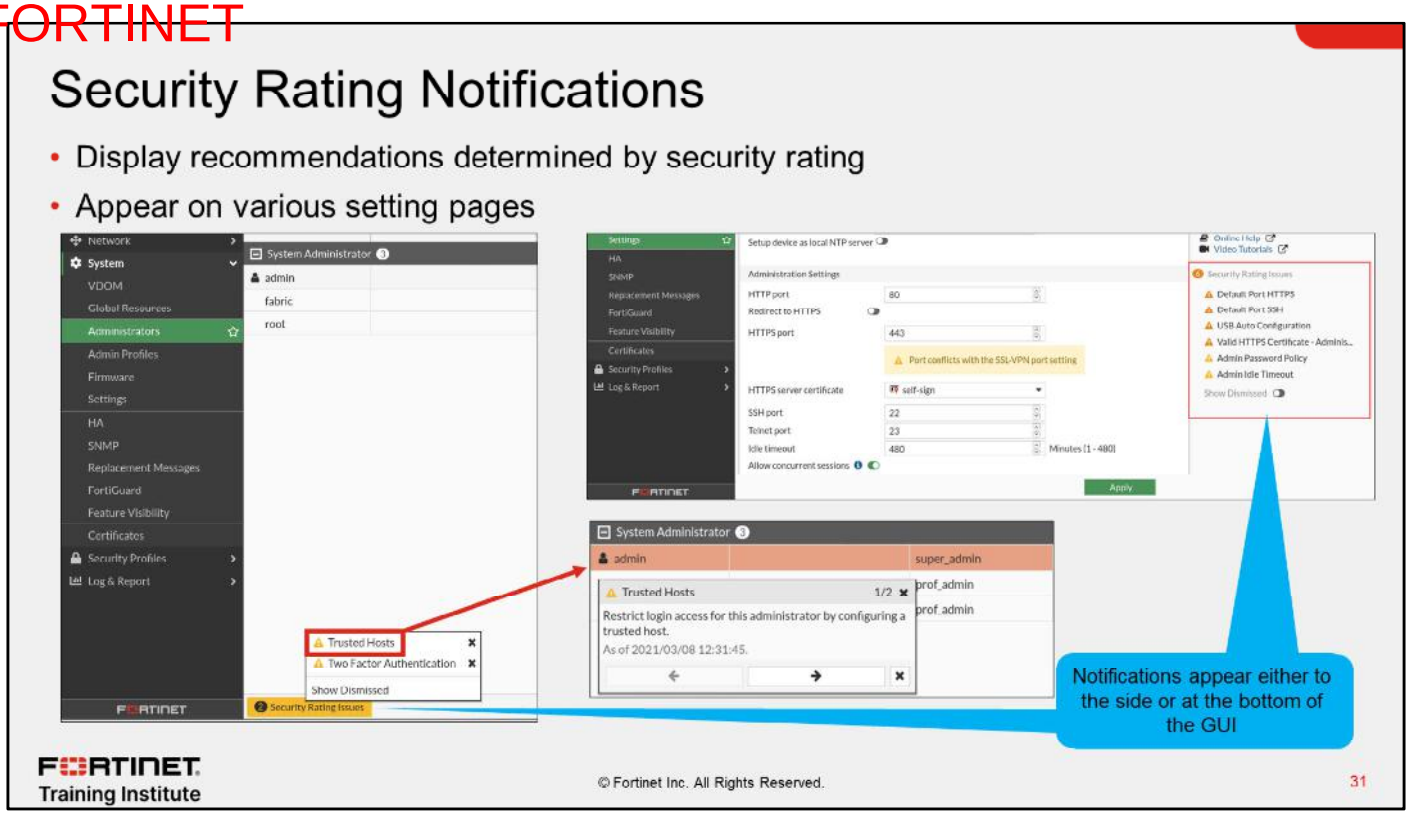
The security rating event log is available on the root VDOM.



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

The security posture service now supports the following:

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

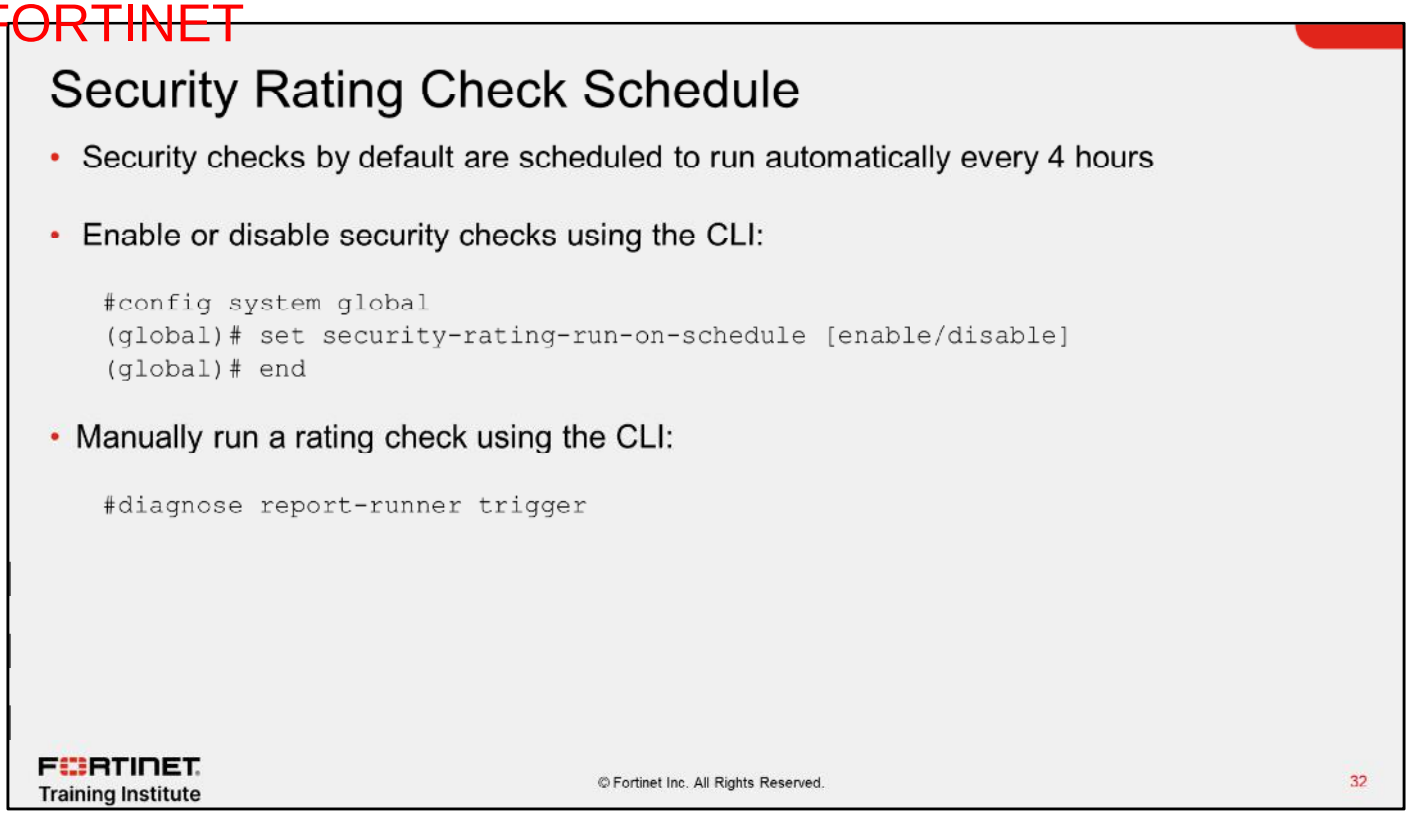


Security rating provides recommendations and highlights issues with the configuration of the FortiGate settings. These recommendations and issues appear as notifications on the **Settings** page.

Click a notification to display the page where the setting needs to be fixed. This prevents you from having to go back and forth between the **Security Fabric** > **Security Rating** page and the various settings pages.

Notifications appear either to the side or at the bottom of the GUI. You can also dismiss the notifications.

In the example shown on this slide, some of the issues found are that FortiGate is using the default HTTPS and SSH ports, and that the administrator password policy is not enabled. The security rating check also recommends that you configure trusted hosts and two-factor authentication.



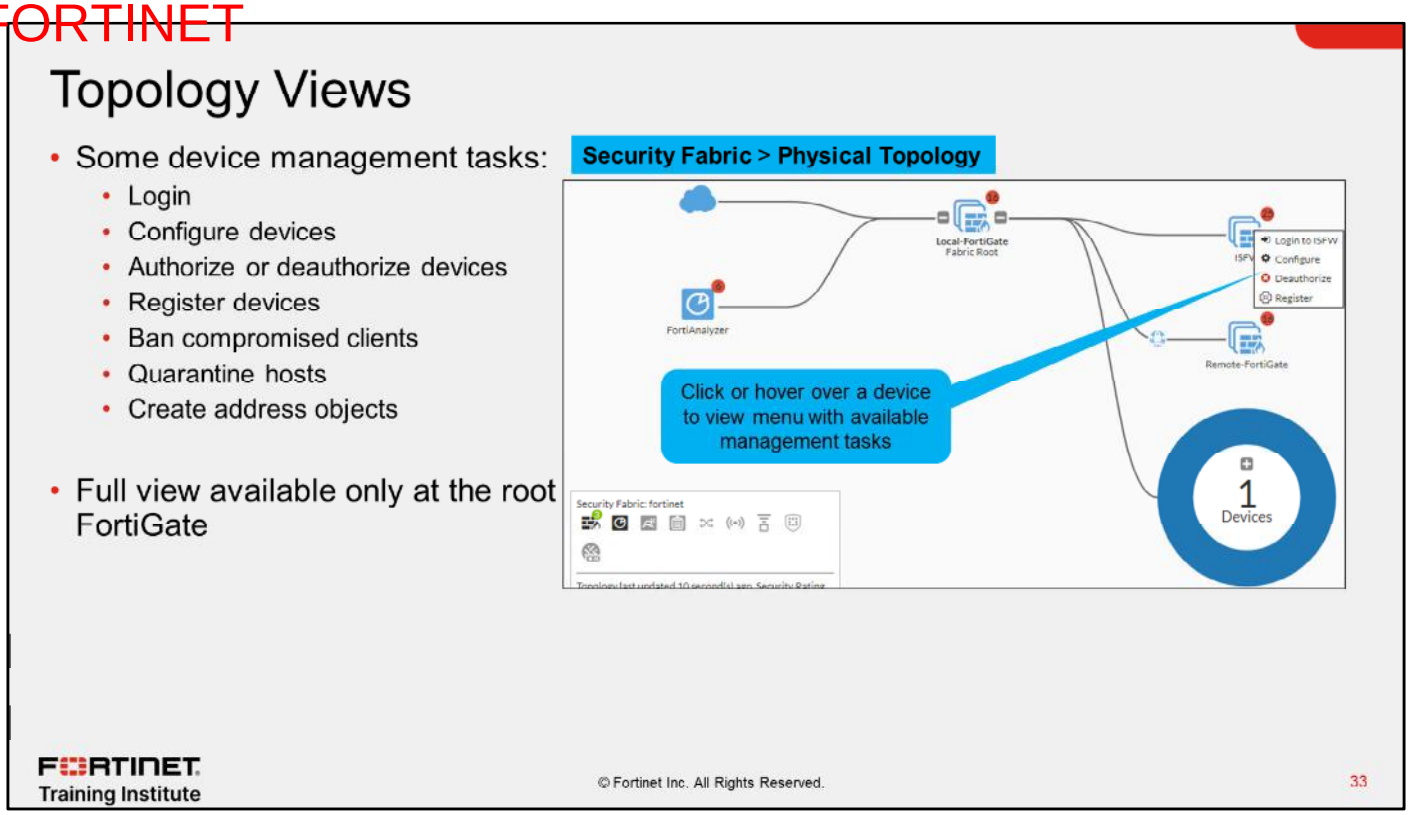
Security rating checks by default are scheduled to run automatically every four hours.

Use the following commands to enable or disable security checks using the CLI:

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

Use the following command to manually run a rating check using the CLI:

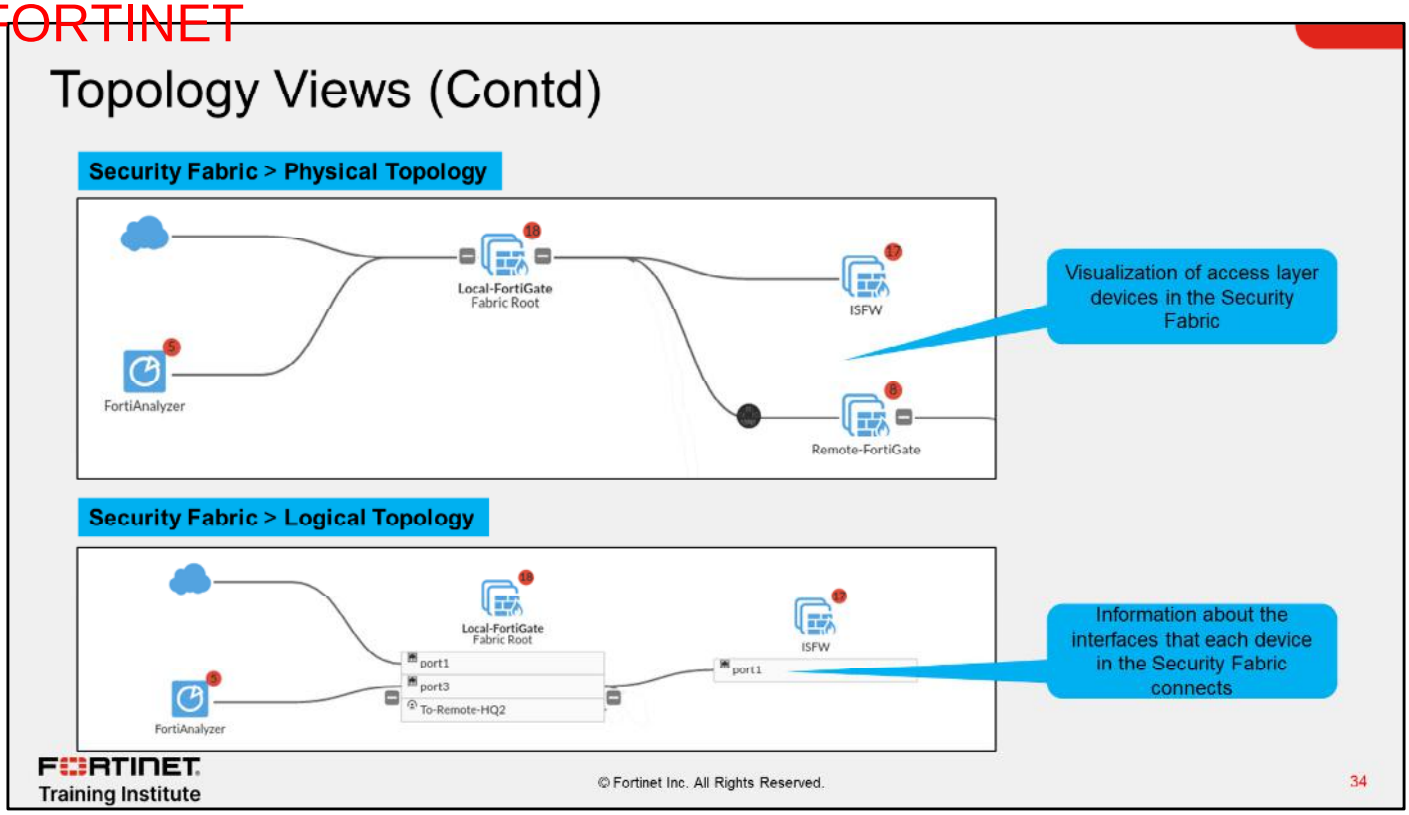
```
#diagnose report-runner trigger
```



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

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

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



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

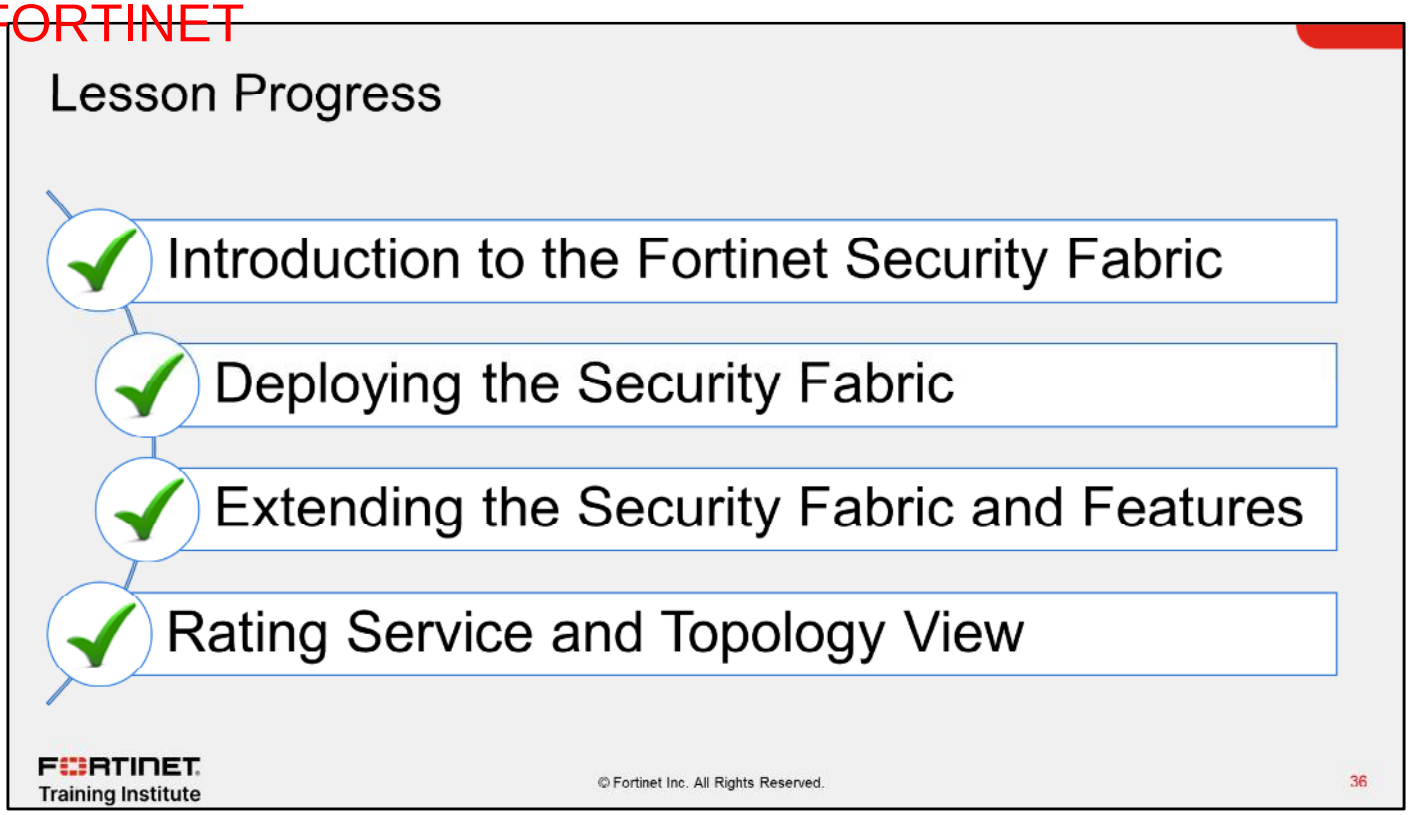
Knowledge Check

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

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

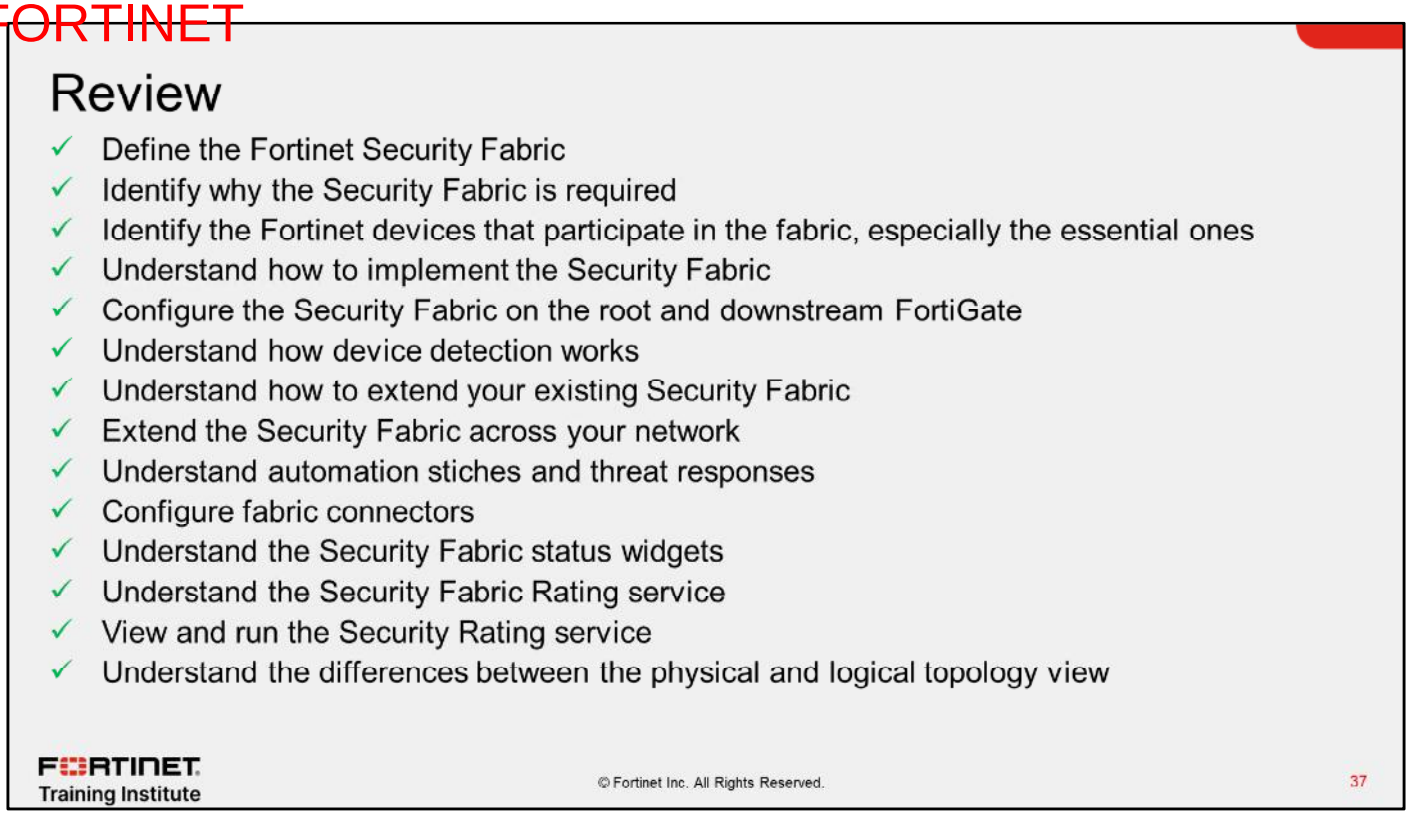
FORTINET Training Institute

35



Congratulations! You have completed this lesson.

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



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

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

FortiGate Infrastructure Study Guide

for FortiOS 7.2

FORTINET®
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

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

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

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

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

FORTINET

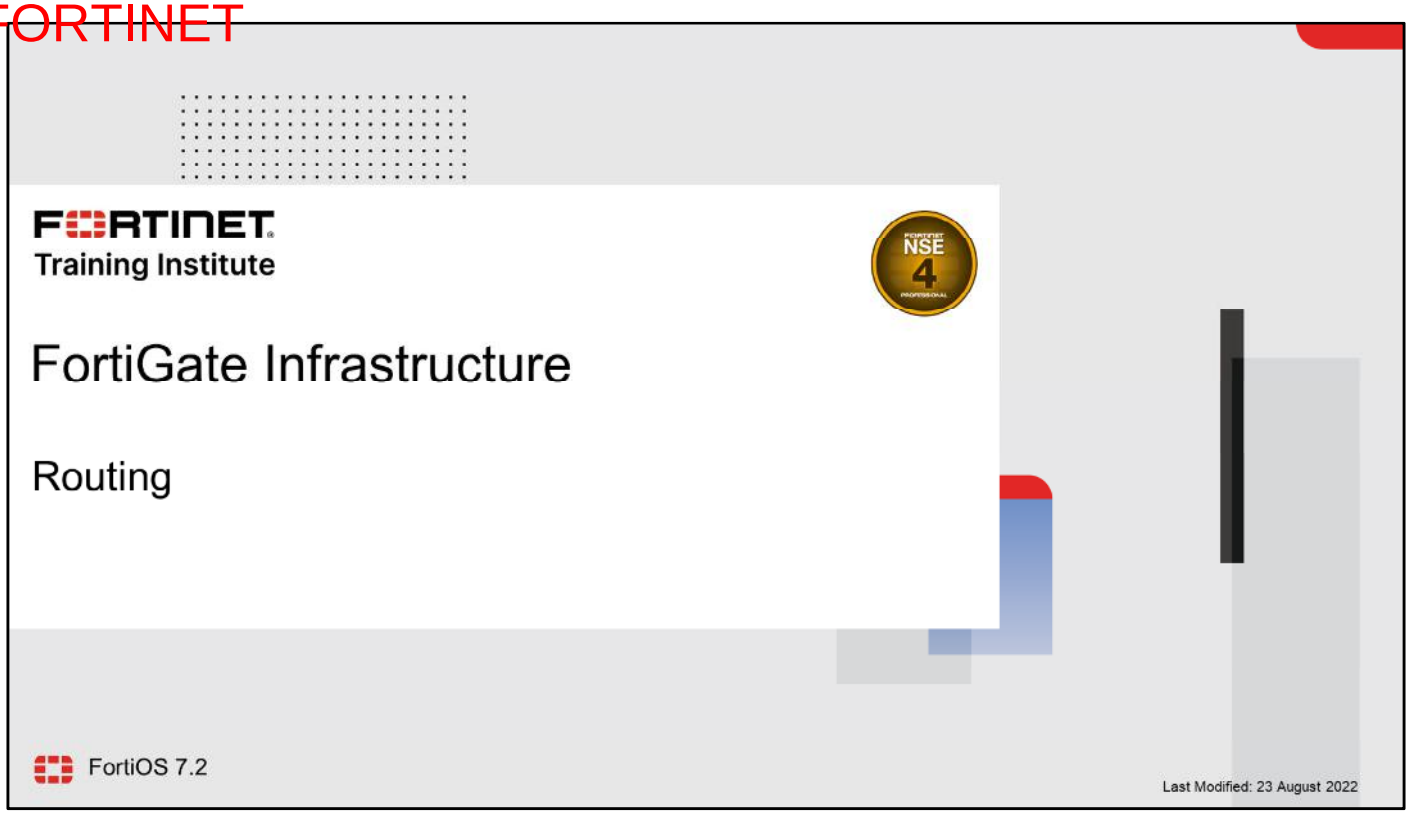
8/30/2022

TABLE OF CONTENTS

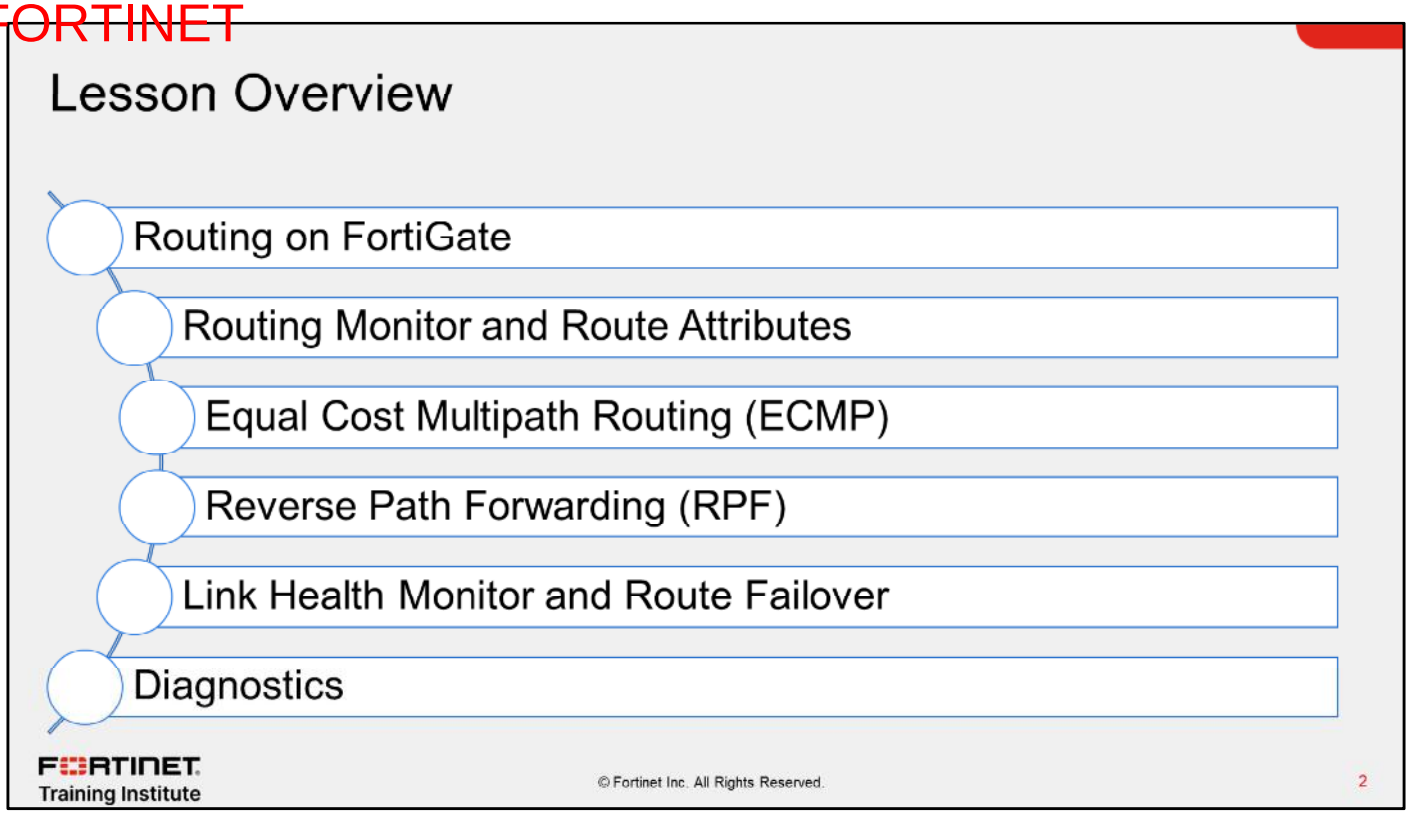
Change Log

This table includes updates to the *FortiGate Infrastructure 7.2 Study Guide* dated 6/13/2022 to the updated document version dated 8/30/2022.

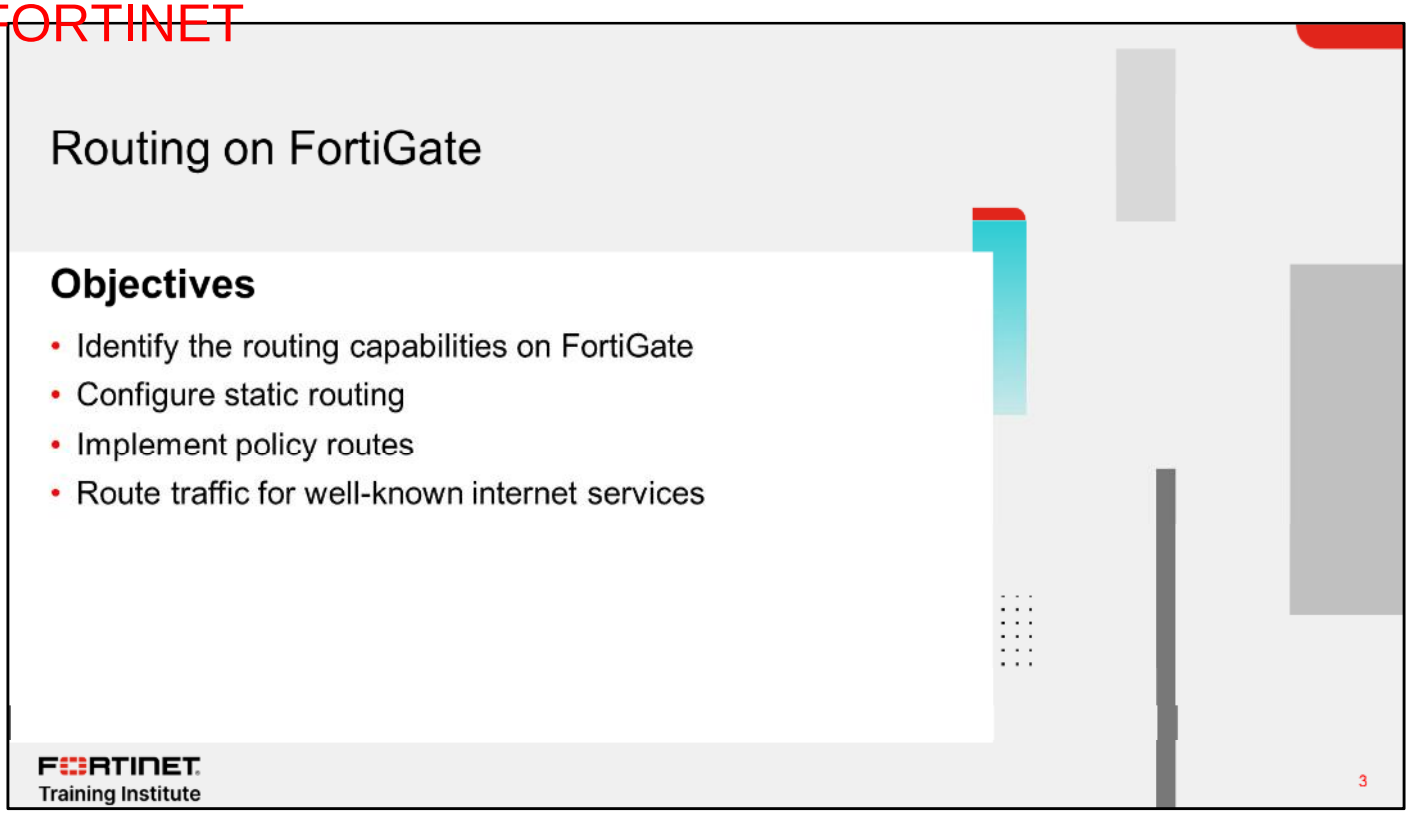
Change	Location
Various formatting fixes	Entire Guide
Fixed notes	Lesson 6, slide 50
Updated notes	Lesson 7, slide 19 and 42



In this lesson, you will learn about the routing capabilities and features available on FortiGate.

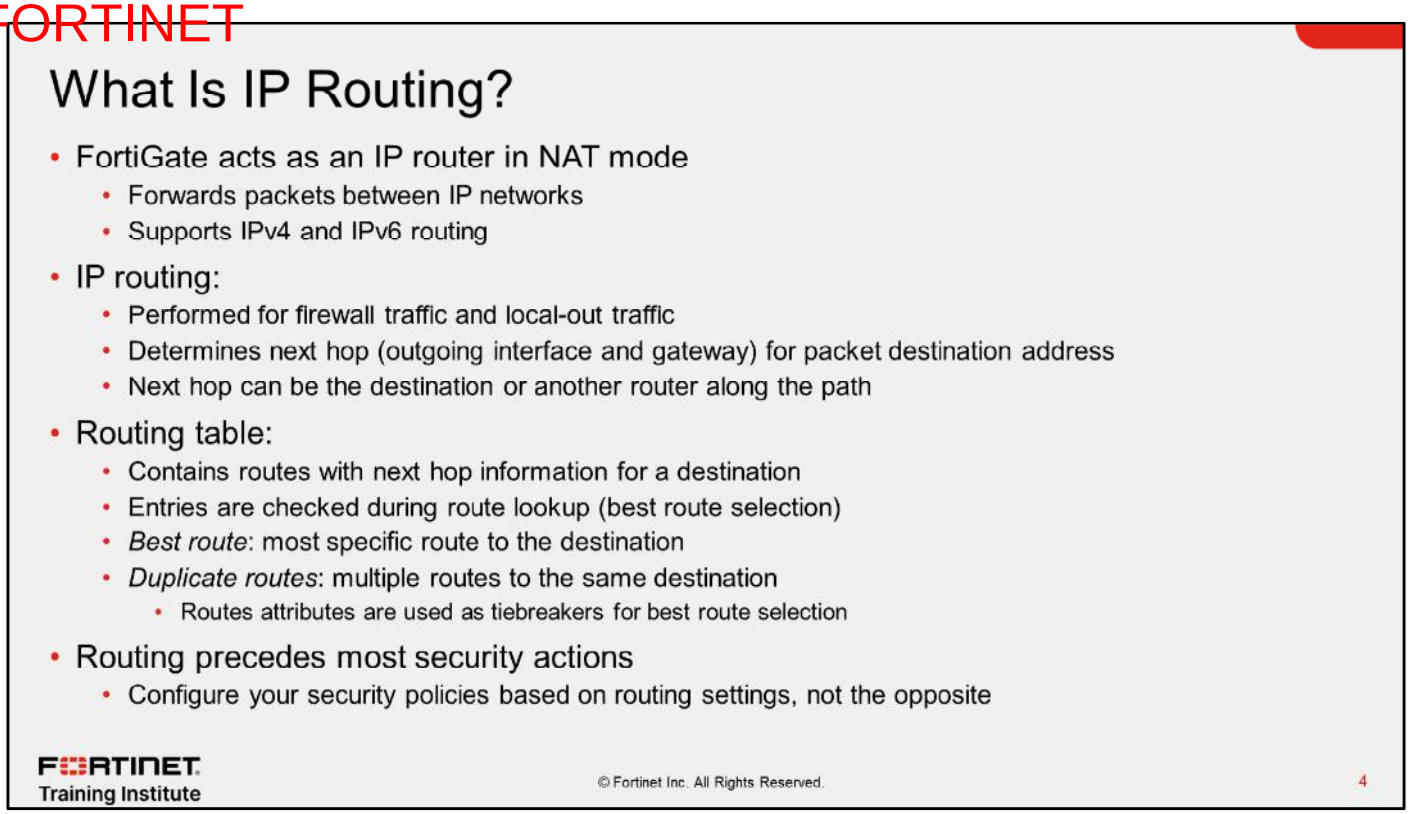


In this lesson, you will learn about the topics shown on this slide.



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

By demonstrating competence in routing on FortiGate, you should be able to implement static and policy routing. You will also be able to route traffic for well-known internet services.



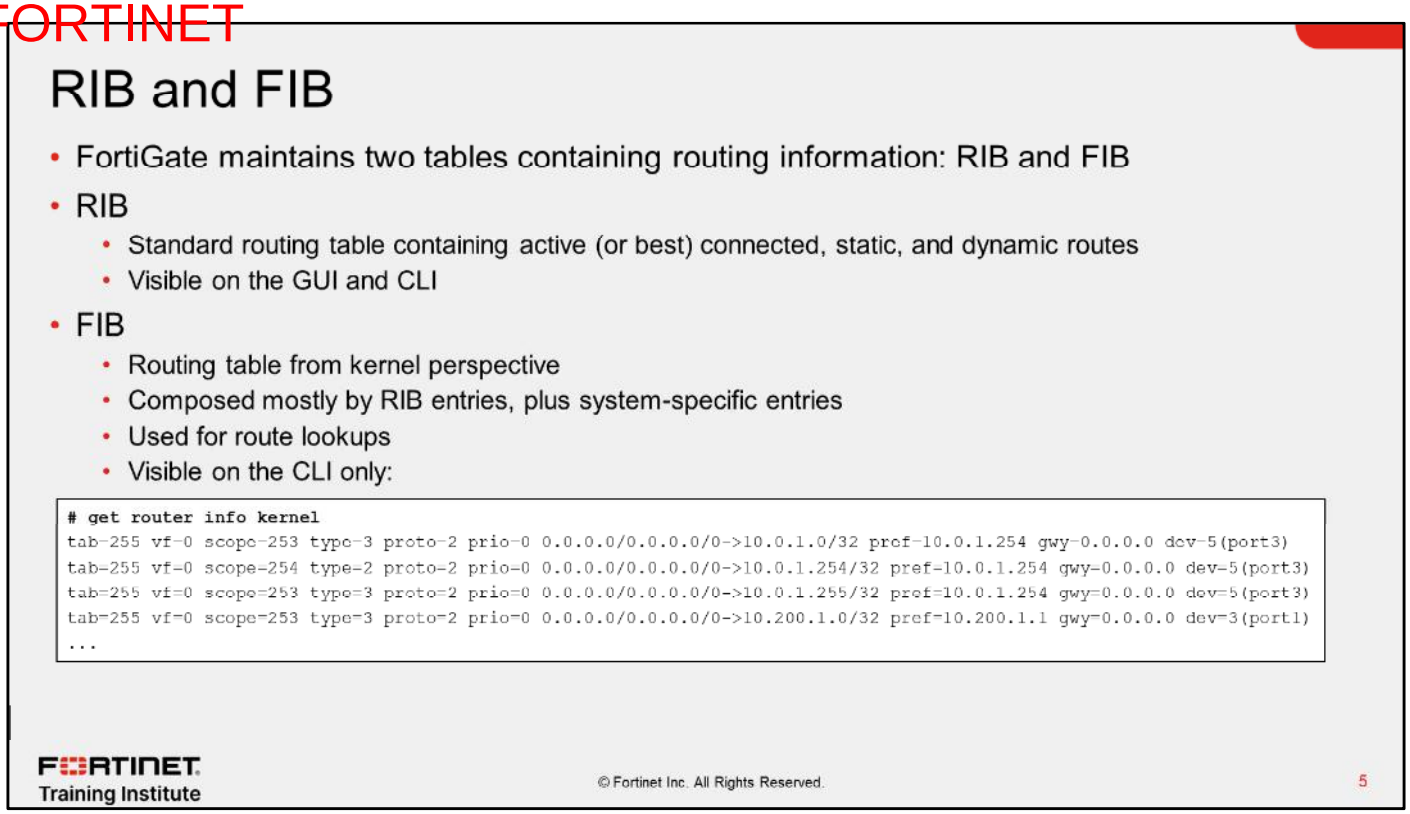
When FortiGate operates in NAT mode—the default operation mode—FortiGate behaves as an IP router. An IP router is a device that forwards packets between IP networks. For that, a router performs IP routing, which is the process of determining the next hop to forward a packet to based on the packet destination IP address. FortiGate supports both IPv4 and IPv6 routing.

FortiGate performs routing for both firewall traffic (also known as user traffic) and local-out traffic. Firewall traffic is the traffic that travels through FortiGate. Local-out traffic is the traffic generated by FortiGate, usually for management purposes. For example, when you ping a device from FortiGate, that's local-out traffic. When FortiGate connects to FortiGuard to download the latest definitions, that's also local-out traffic.

Routers maintain a routing table. A routing table contains a series of entries, also known as routes. Each route in the routing table indicates the *next hop* for a particular destination. The next hop refers to the outgoing interface and gateway to use for forwarding the packet. The next hop can be the destination of the packet or another router along the path to the destination. If the next hop isn't the destination, the next router in the path routes the packet to the next hop. The routing process is repeated on each router along the path until the packet reaches its destination.

To route packets, FortiGate performs a route lookup to identify the best route to the destination. The best route is the most specific route to the destination. If FortiGate finds duplicate routes—that is, multiple routes to the same destination—it uses various route attributes as a tiebreak to determine the best route.

Routing takes place before most security features. For example, routing precedes firewall policy evaluation, content inspection, traffic shaping, and source NAT (SNAT). This means that the security actions that FortiGate performs depend on the outgoing interface determined by the routing process. This also means that your security policy configuration must follow your routing configuration, and not the opposite.

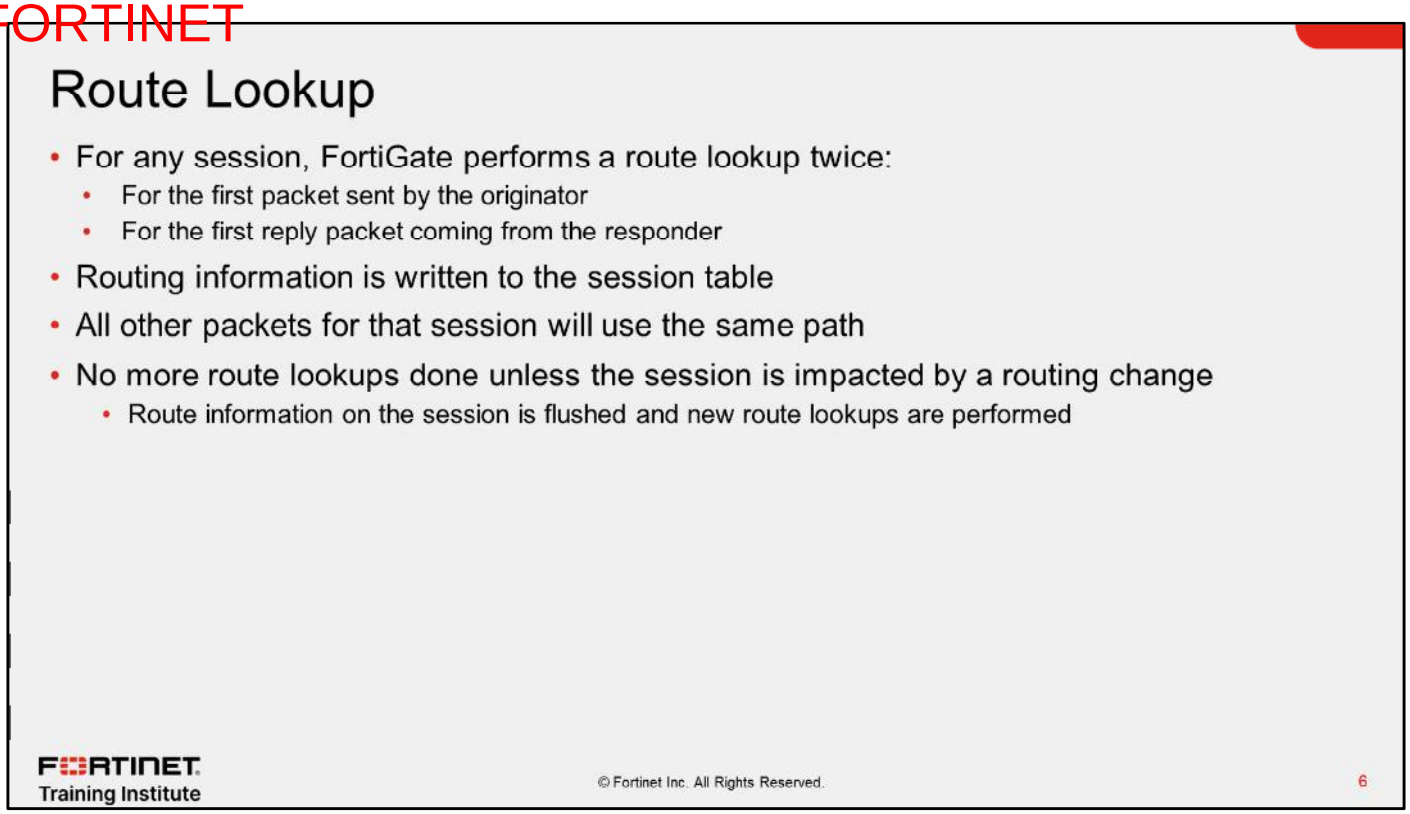


FortiGate maintains its routing information in two tables: RIB and FIB. The routing table, also known as the routing information base (RIB), is a standard routing table containing active (or the best) connected, static, and dynamic routes. The forwarding information base (FIB) can be described as the routing table from the kernel point of view, and is built mostly out of RIB entries plus some system-specific entries required by FortiOS.

When FortiGate performs a route lookup, it checks the FIB and not the RIB. However, because the FIB is composed mostly by RIB entries, then the route lookup mainly involves checking routes from the RIB. For this reason, the route lookup is often referred to as the routing table lookup process. Nonetheless, a more accurate statement is to refer to it as the FIB lookup process.

You can display the RIB entries on the FortiGate GUI and CLI. However, for the FIB, you can display its entries on the FortiGate CLI only. The output on this slide shows the CLI command that displays the FIB. Note that the output has been cut to fit the slide. You will learn how to display the routing table entries in this lesson.

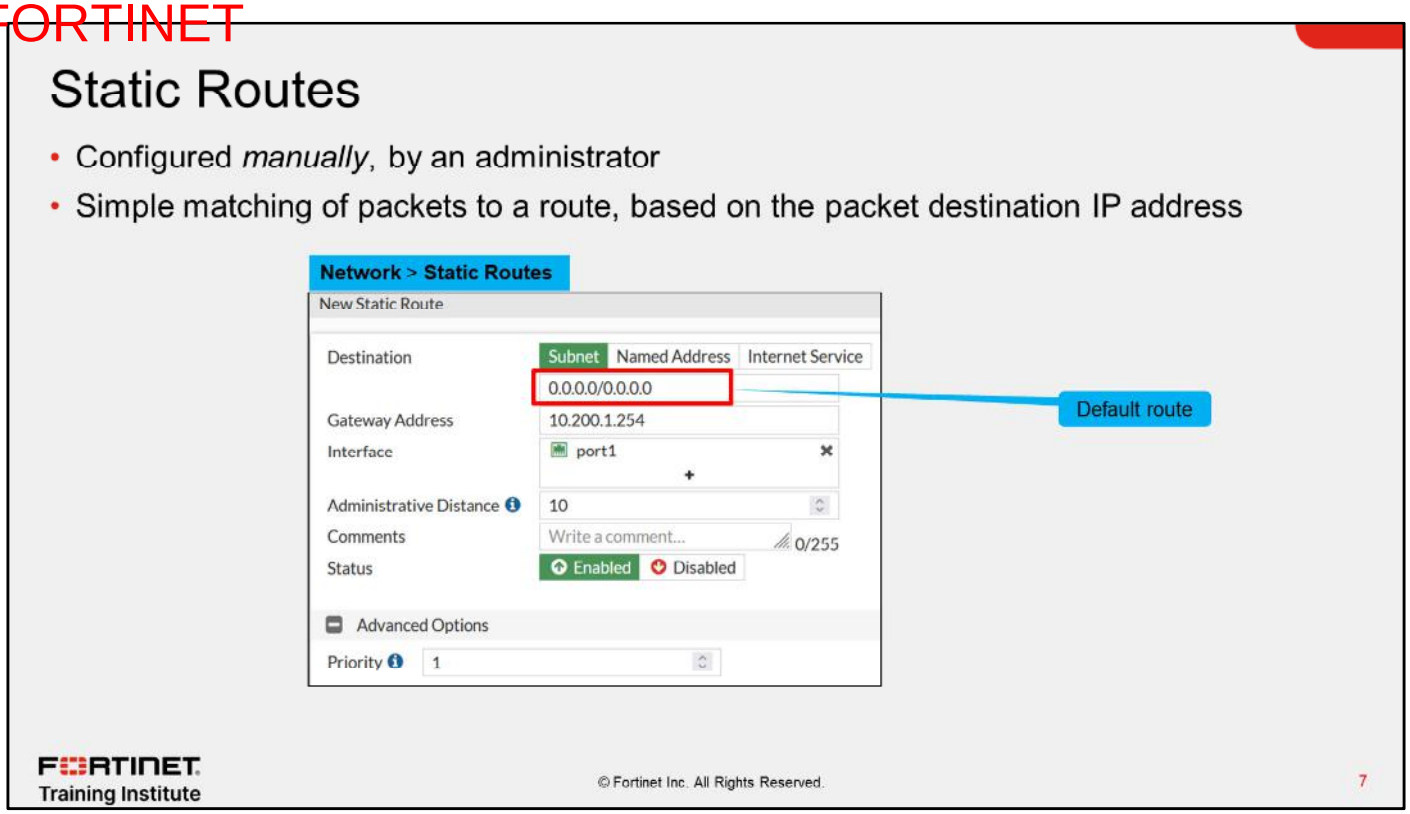
This lesson focuses on the RIB (or routing table) only, and you will learn more about it, including how to monitor its entries, in this lesson.



For each session, FortiGate performs two route lookups:

- For the first packet sent by the originator
- For the first reply packet coming from the responder

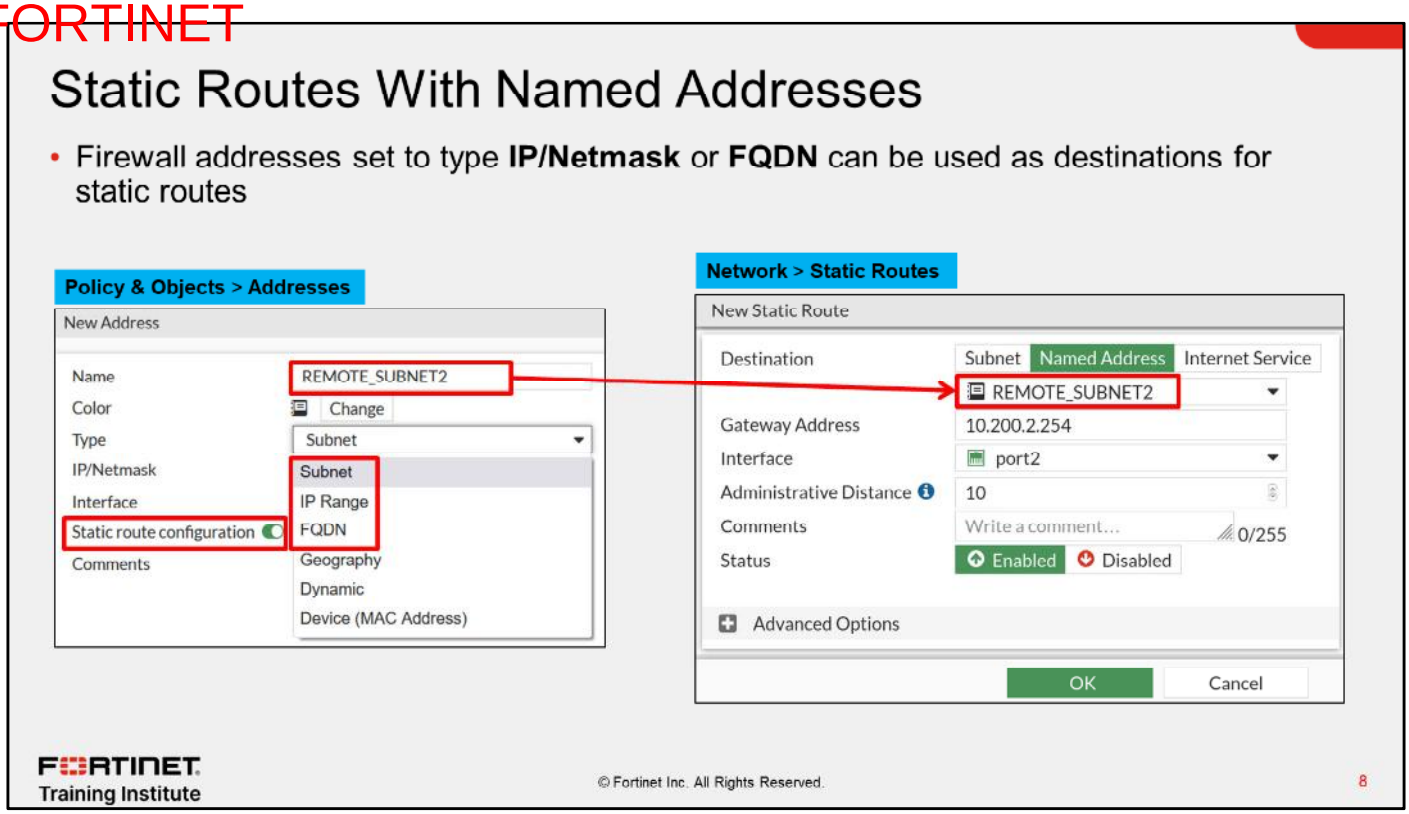
After completing these two lookups, FortiGate writes the routing information to its session table. Subsequent packets are routed according to the *session table*, not the routing table. So, all packets that belong to the same session follow the same path. However, there is an exception to this rule: if there is a change in the routing table that impacts the session, then FortiGate removes the route information for the session table, and then performs additional route lookups to rebuild this information.



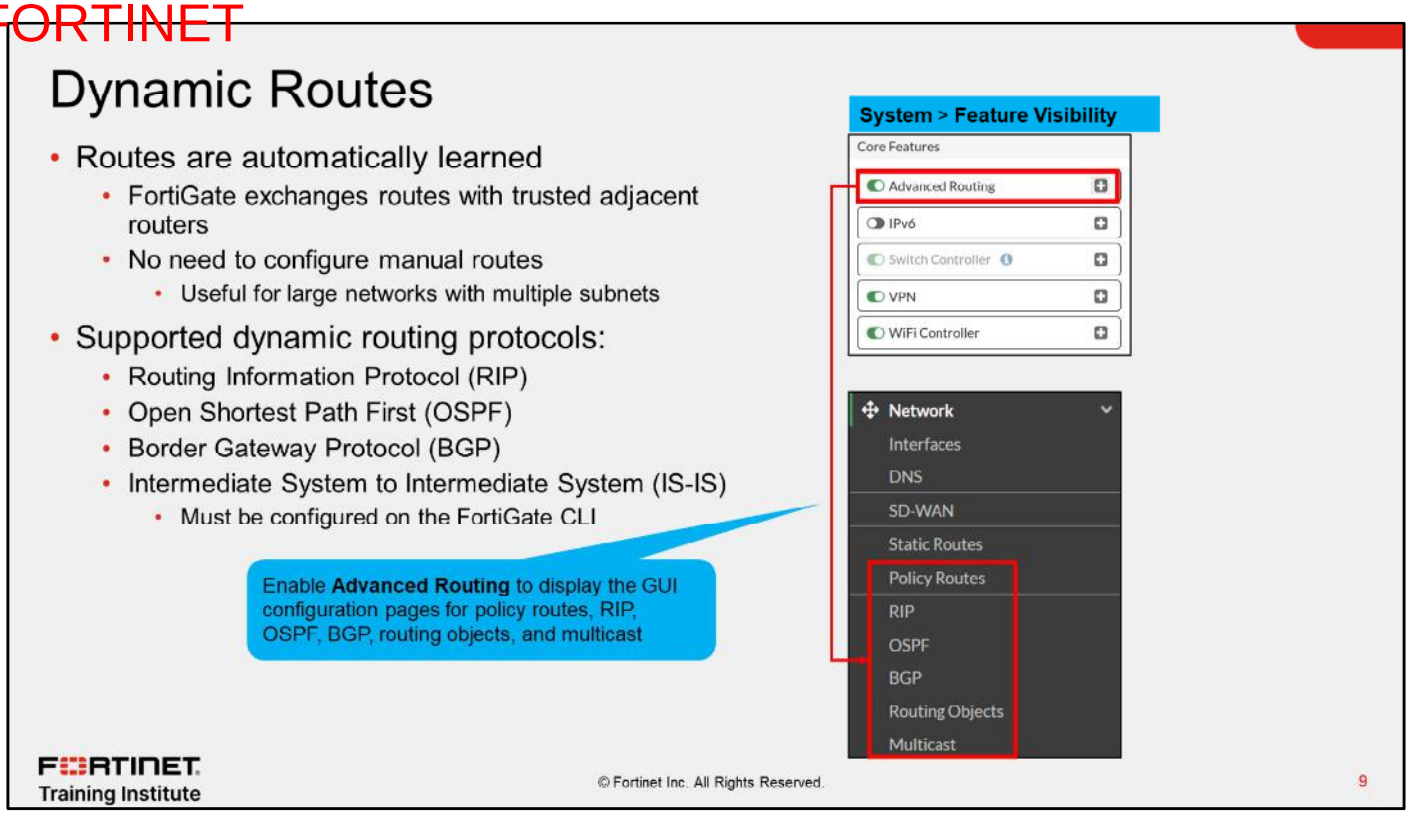
One type of manually configured route is called a static route. When you configure a static route, you are telling FortiGate, “When you see a packet whose destination is within a specific range, send it through a specific network interface, towards a specific router.” You can also configure the distance and priority so that FortiGate can identify the best route to any destination matching multiple routes. You will learn about distance and priority in this lesson.

For example, in simple home networks, DHCP automatically retrieves and configures a route. Your modem then sends all outgoing traffic through your ISP internet router, which can relay packets to their destination. This is typically referred to as a default route, because all traffic not matching any other routes will, by default, be routed using this route. The example shown on this slide is a default route. The destination subnet value of `0.0.0.0/0.0.0.0` matches all addresses within any subnet. Most FortiGate devices deployed at the edge of the network have at least one of these default routes to ensure internet traffic is forwarded to the ISP network.

Static routes are not needed for subnets to which FortiGate has direct Layer 2 connectivity.



If you create a firewall address object with the type **IP/Netmask** or **FQDN**, you can use that firewall address as the destination of one or more static routes. First, enable **Static route configuration** in the firewall address configuration. After you enable it, the firewall address object becomes available for use in the **Destination** drop-down list for static routes with named addresses.



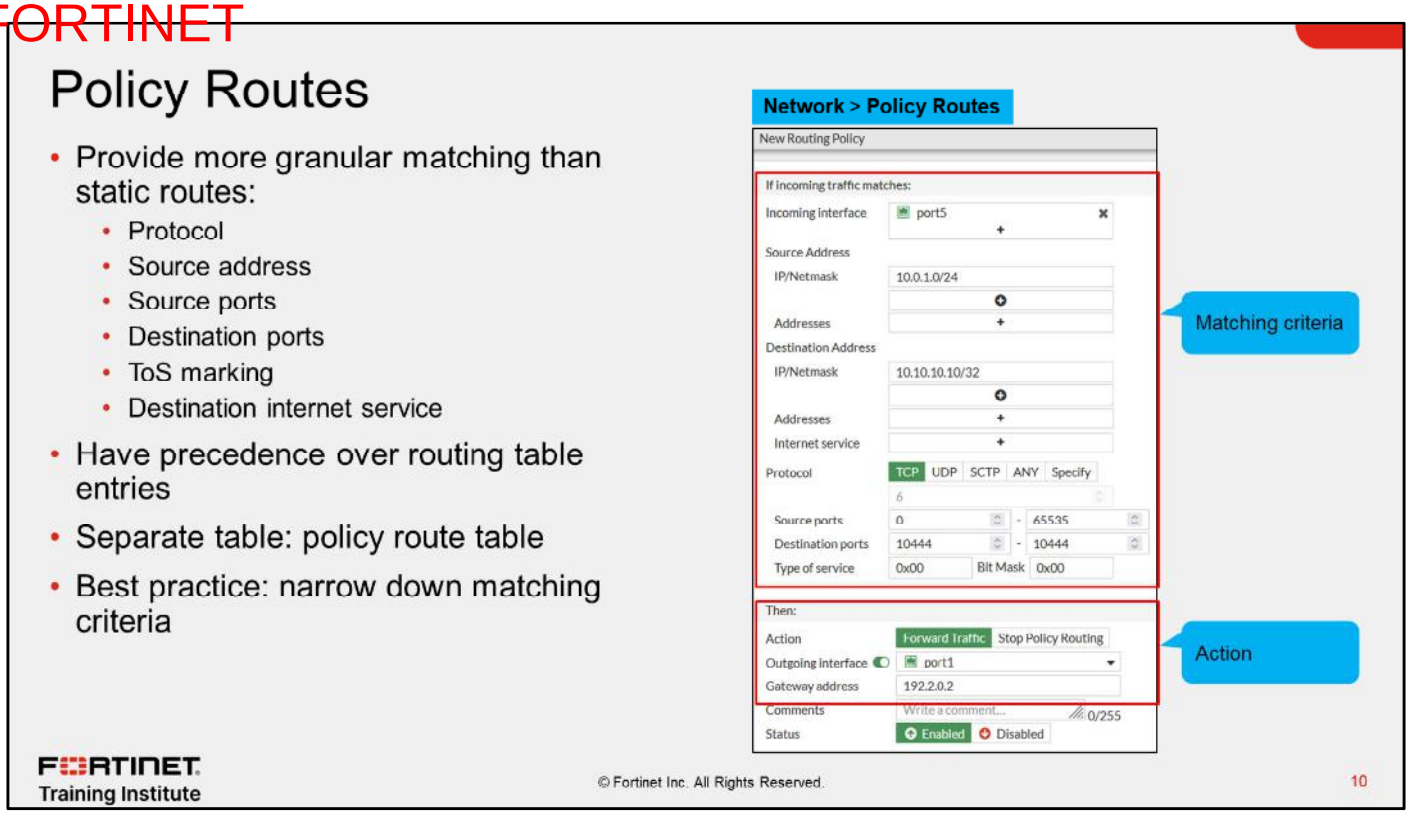
For large networks, manually configuring hundreds of static routes may not be practical. Your FortiGate can help, by learning routes automatically. FortiGate supports several dynamic routing protocols: RIP, OSPF, BGP, and IS-IS.

In dynamic routing, FortiGate communicates with trusted adjacent routers to exchange routing information about their known networks. Then, FortiGate adds the learned routes into its local routing table and considers them during the route lookup process.

You can configure dynamic routing for RIP, OSPF, and BGP protocols using the FortiGate GUI. You just need to make sure that the **Advanced Routing** option in the **Feature Visibility** page is enabled—it's enabled by default. However, for configuring IS-IS, you must use the FortiGate CLI.

Note that when you enable **Advanced Routing** on the **Feature Visibility** page, you also enable the configuration pages for other advanced routing features such as **Policy Routes**, **Routing Objects**, and **Multicast**. You will learn more about policy routes in this lesson.

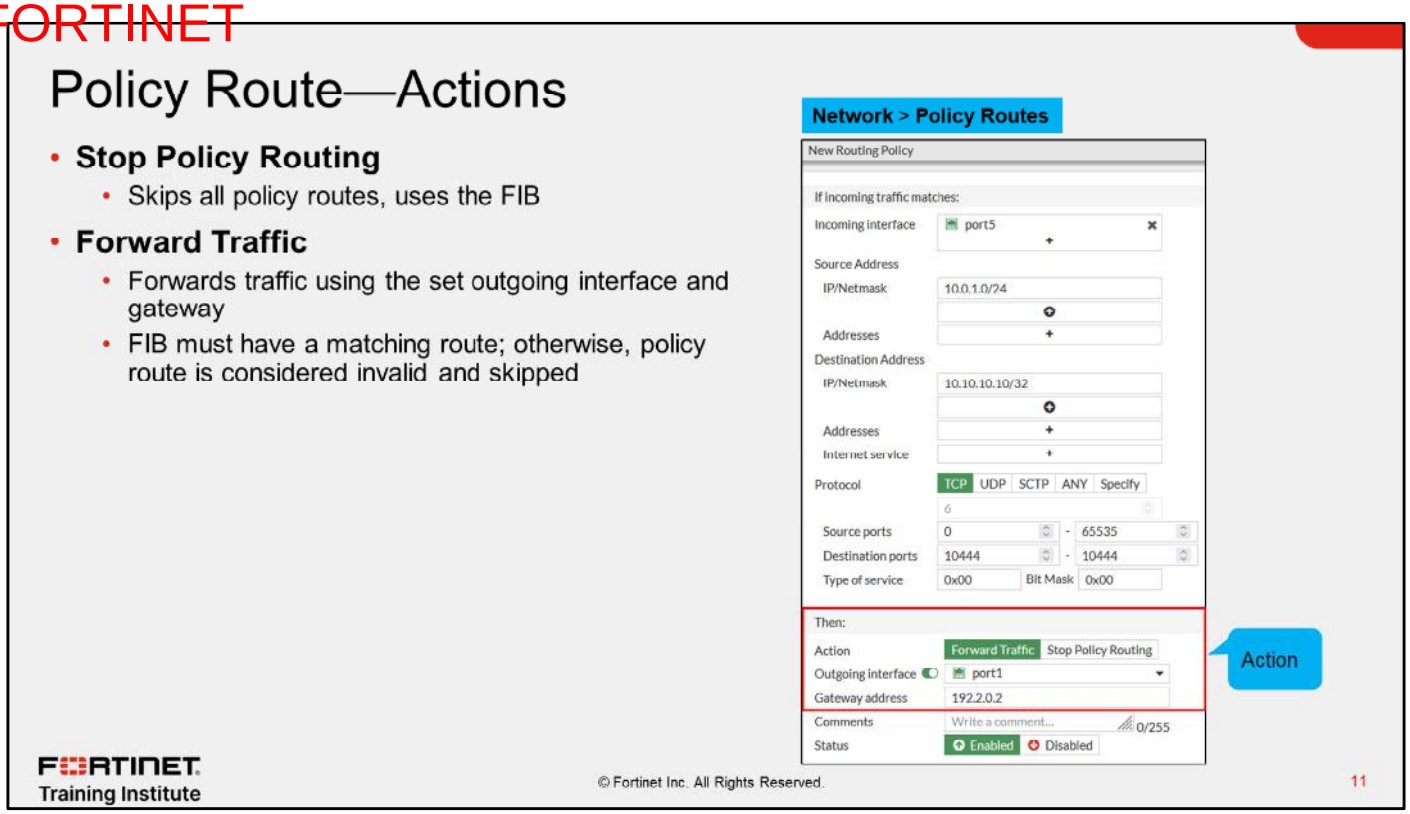
Larger networks also may need to balance the routing load among multiple valid paths and detect and avoid routers that are down. You will learn more about that in this lesson.



Static routes are simple and are often used in small networks. Policy routes, however, are more flexible because they can match more than just the destination IP address. For example, you can configure as matching criteria the incoming interface, the source and destination subnets, protocol, and port number.

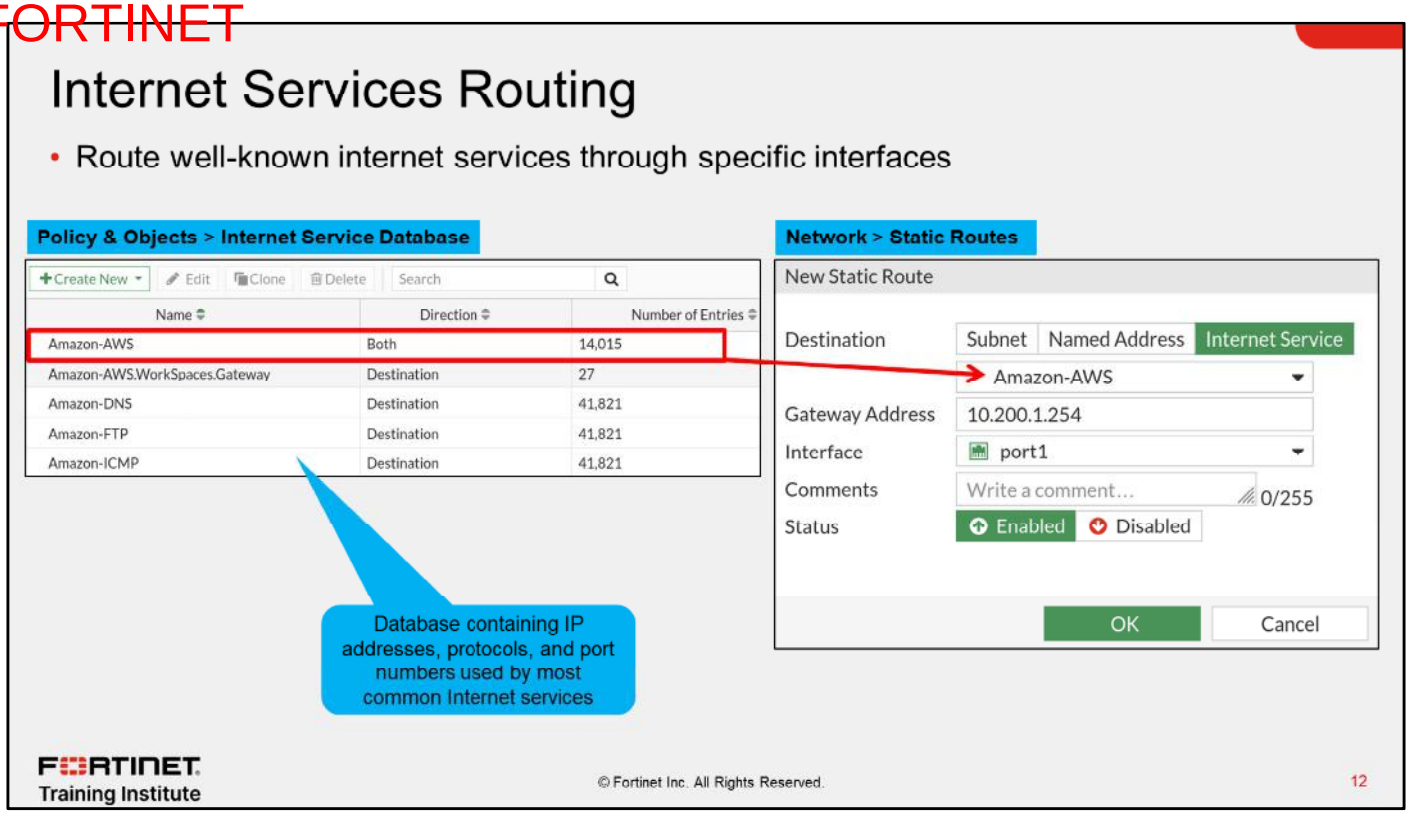
Policy routes are maintained in a separate routing table by FortiGate and have precedence over the entries in the routing table. Because of its precedence, it is a best practice to narrow down the matching criteria of policy routes as much as possible. Otherwise, traffic that is expected to be routed using standard routing, that is, based on the destination address only and the routing table entries, could be handled by policy routes instead.

This slide shows an example of a policy route configured using the FortiGate GUI. The policy route instructs FortiGate to match traffic received at **port5**, sourced from `10.0.1.0/24` and destined to the host `10.10.10.10`. The traffic must also be destined to TCP port 10444 for the policy route to match. FortiGate then forwards the traffic—**Forward Traffic** action—to **port1** through the gateway `192.2.0.2`.



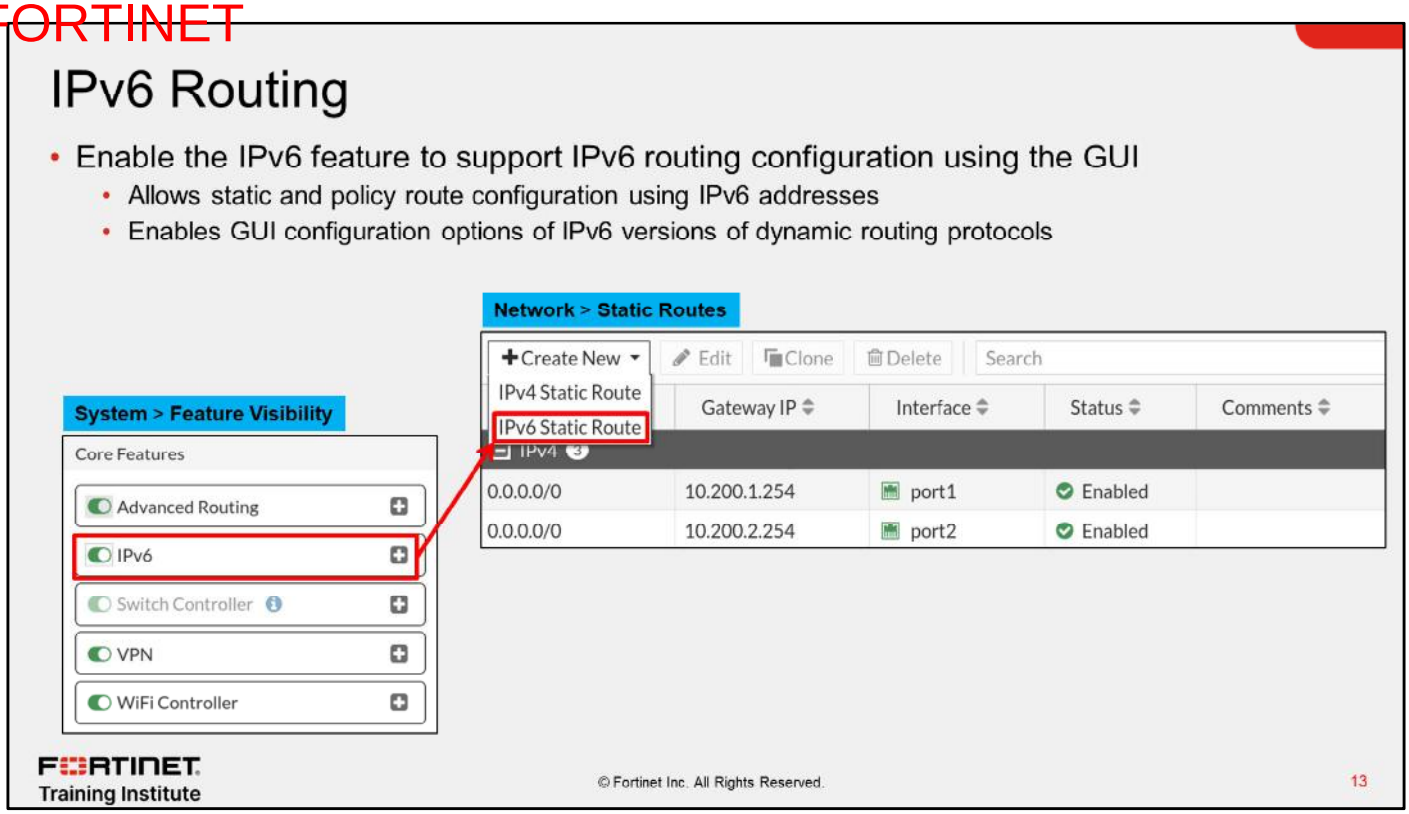
When a packet matches a policy route, FortiGate takes one of two actions. Either it routes the packet to the configured outgoing interface and gateway—**Forward Traffic** action—or it stops checking the policy routes—**Stop Policy Routing** action—so the packet is routed based on the routing table.

Note that when you configure **Forward Traffic** as the action, the **Destination Address**, **Outgoing interface**, and the **Gateway address** settings must match a route in the FIB. Otherwise, the policy route is considered invalid and, as a result, skipped.



What happens if you need to route traffic to a public internet service (such as Amazon-AWS or Apple Store) through a specific WAN link? Say you have two ISPs and you want to route Netflix traffic through one ISP and all your other internet traffic though the other ISP. To achieve this goal, you need to know the Netflix IP addresses and configure the static route. After that, you must frequently check that none of the IP addresses have changed. The internet service database (ISDB) helps make this type of routing easier and simpler. ISDB entries are applied to static routes to selectively route traffic though specific WAN interfaces.

Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.



To enable routing configuration for IPv6 addresses using the GUI, you must enable **IPv6** in the **Feature Visibility** menu. Then, you can create static routes and policy routes with IPv6 addresses. Enabling the IPv6 feature also enables GUI configuration options for IPv6 versions of the dynamic routing protocols.

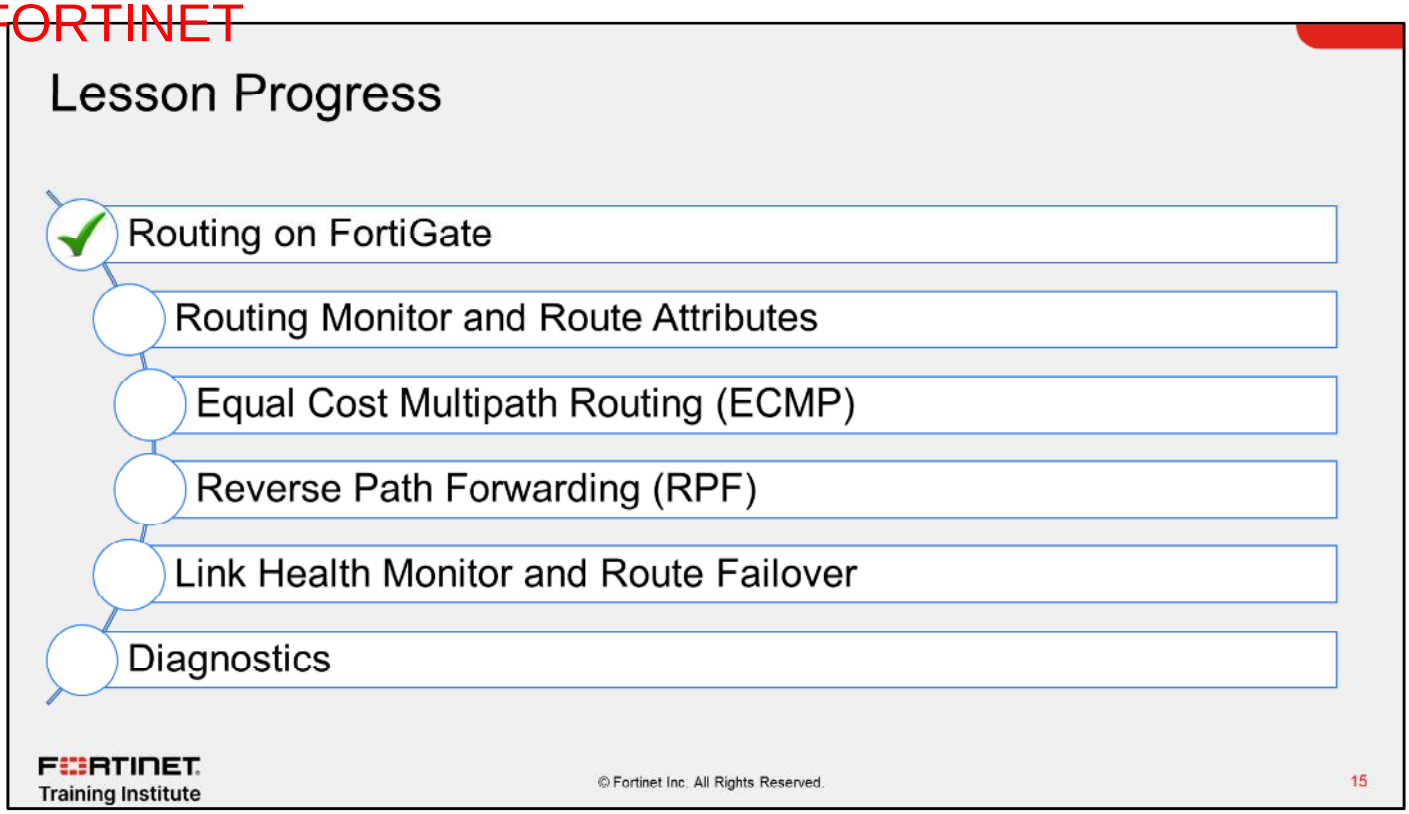
Knowledge Check

1. Which objects can you use to create static routes?
   - ✓ A. ISDB objects
   - B. Service objects

2. When the **Stop policy routing** action is used in a policy route, which behavior is expected?
   - A. FortiGate skips over this policy route and tries to match another in the list.
   - ✓ B. FortiGate routes the traffic based on the regular routing table.

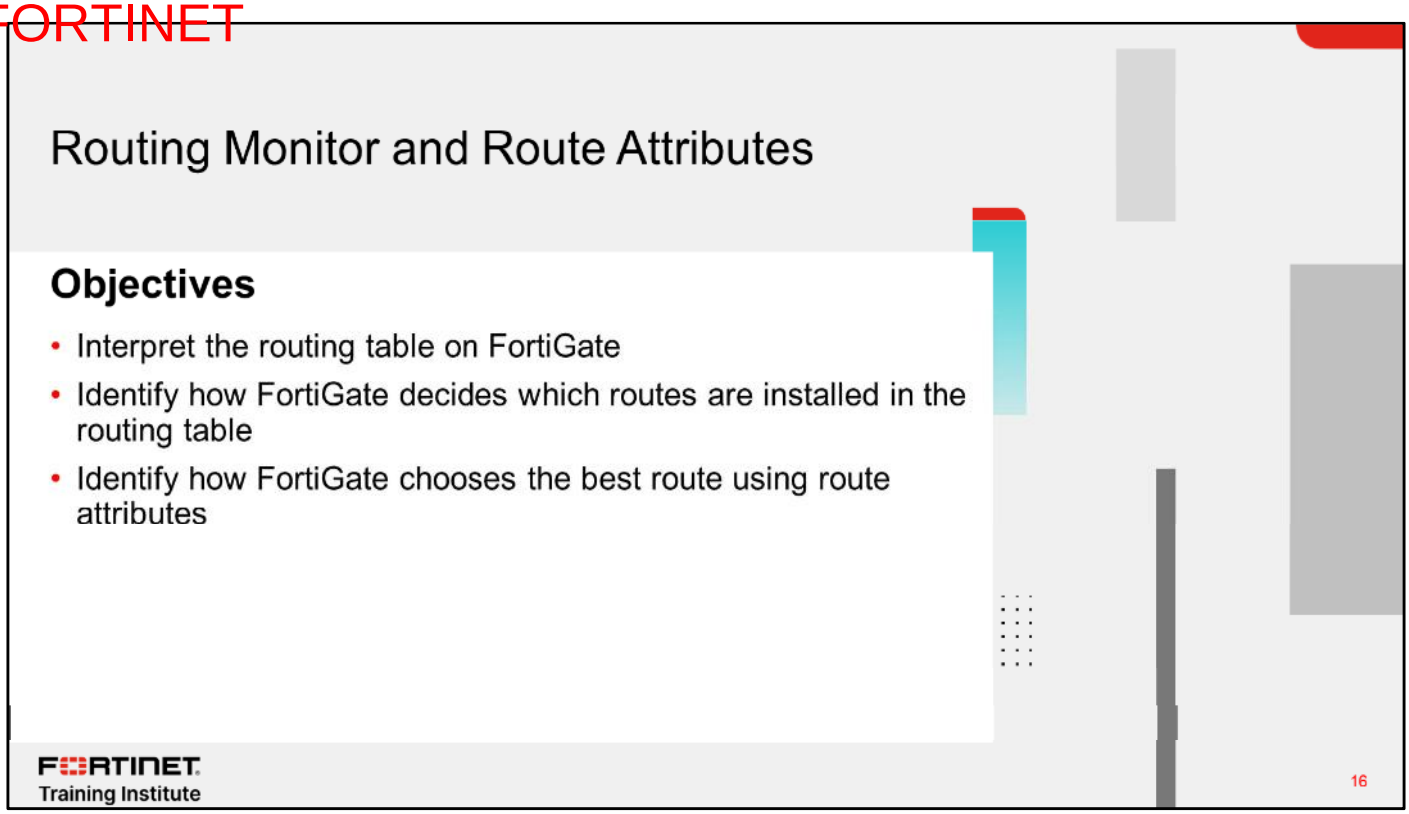
FORTINET Training Institute

14



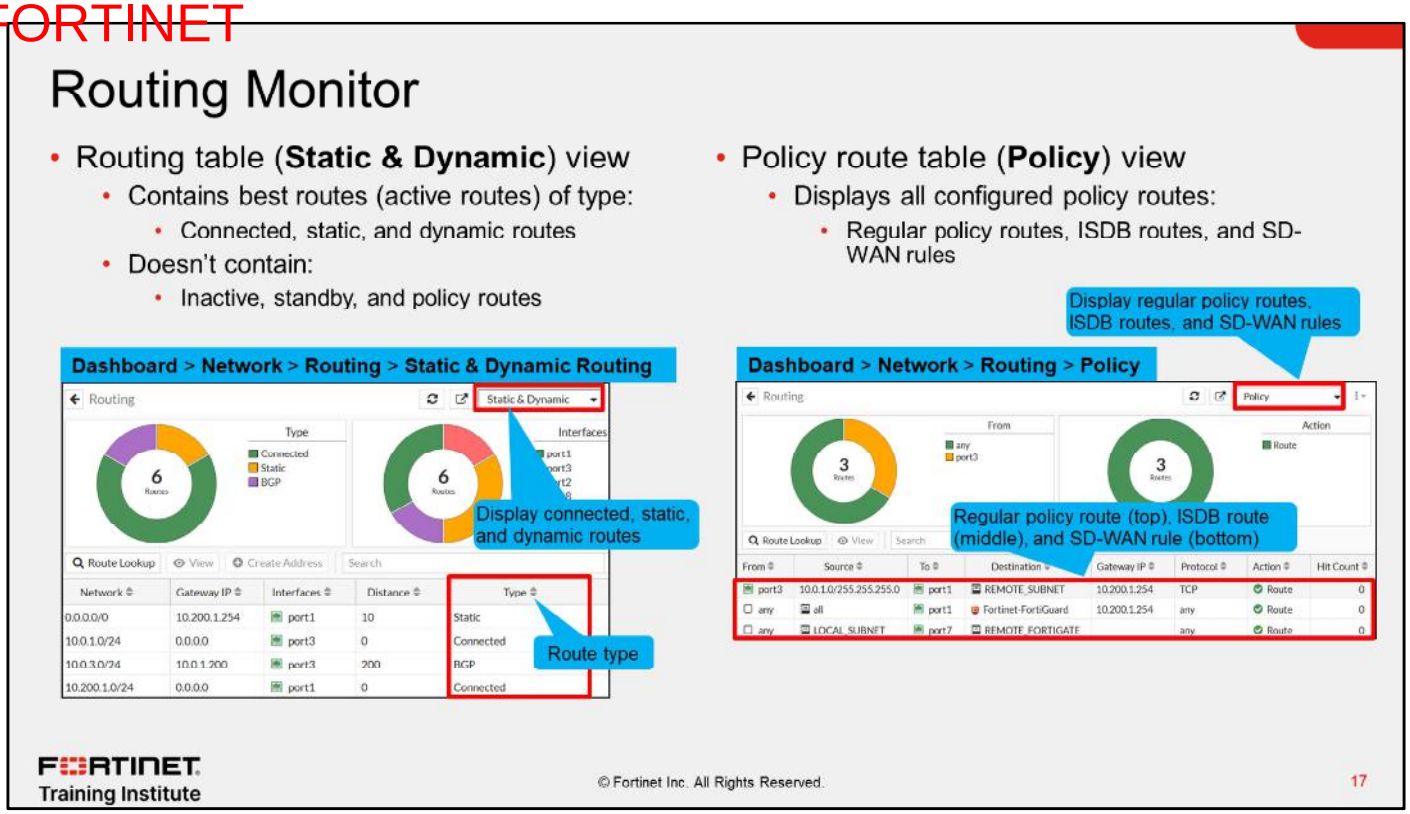
Good job! You now understand routing on FortiGate.

Now, you will learn about routing monitor and route attributes.



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

By demonstrating competence in understanding the routing monitor and route attributes, you should be able to interpret the routing table, identify which routes are installed in the routing table, and identify how FortiGate chooses the best route using route attributes.



The routing monitor widget on the dashboard page enables you to view the routing table and policy route table entries. The routing table contains *the best routes* (or active routes) of the following type:

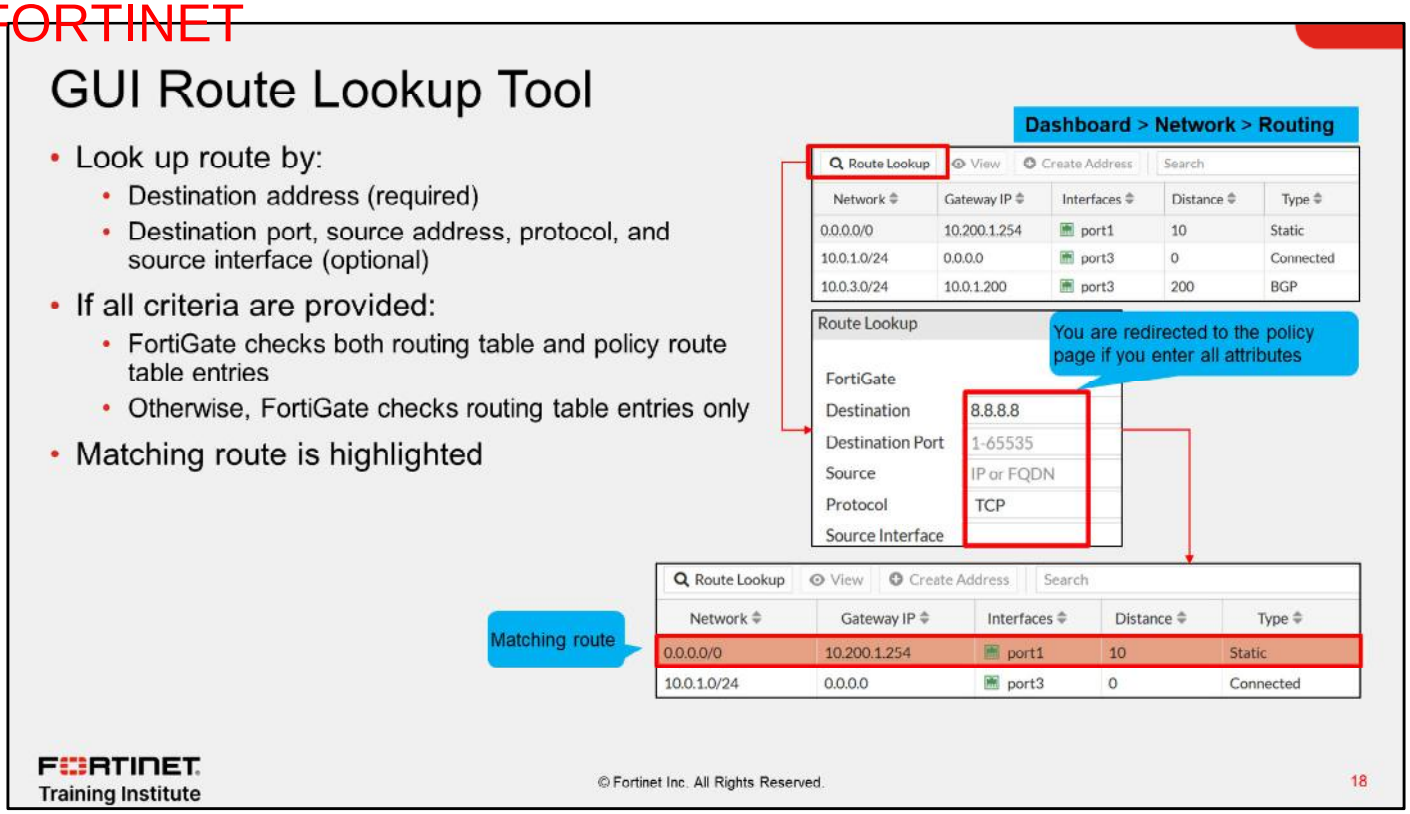
- Static: manual routes that are configured by the administrator.
- Connected: automatic routes added by FortiOS after an interface is assigned an IP address. A connected route references the interface IP address subnet.
- Dynamic: routes learned using a dynamic routing protocol such as BGP or OSPF. FortiGate installs these routes automatically in the routing table and indicates the dynamic routing protocol used.

To view the routing table entries, select **Static & Dynamic**, as shown on this slide. However, keep in mind that the routing table doesn't contain the following routes:

- Inactive routes: static and connected routes whose interfaces are administratively down or whose links are down. Static routes are also marked inactive when their gateway is detected as dead by the link health monitor.

- Standby routes: These are active routes that are removed from the routing table because they are duplicate and have higher distances. For instance:
  - A second static default route with a higher distance than another static default route.
  - A dynamic route such as BGP or OSPF, to the same destination as another static route. However, the dynamic route is not displayed in the routing table because the static route has a lower distance.

- Policy routes: These include regular policy routes, ISDB routes, and SD-WAN rules. Policy routes are viewed in a separate table—the policy route table. To view the policy route table entries, select **Policy**.

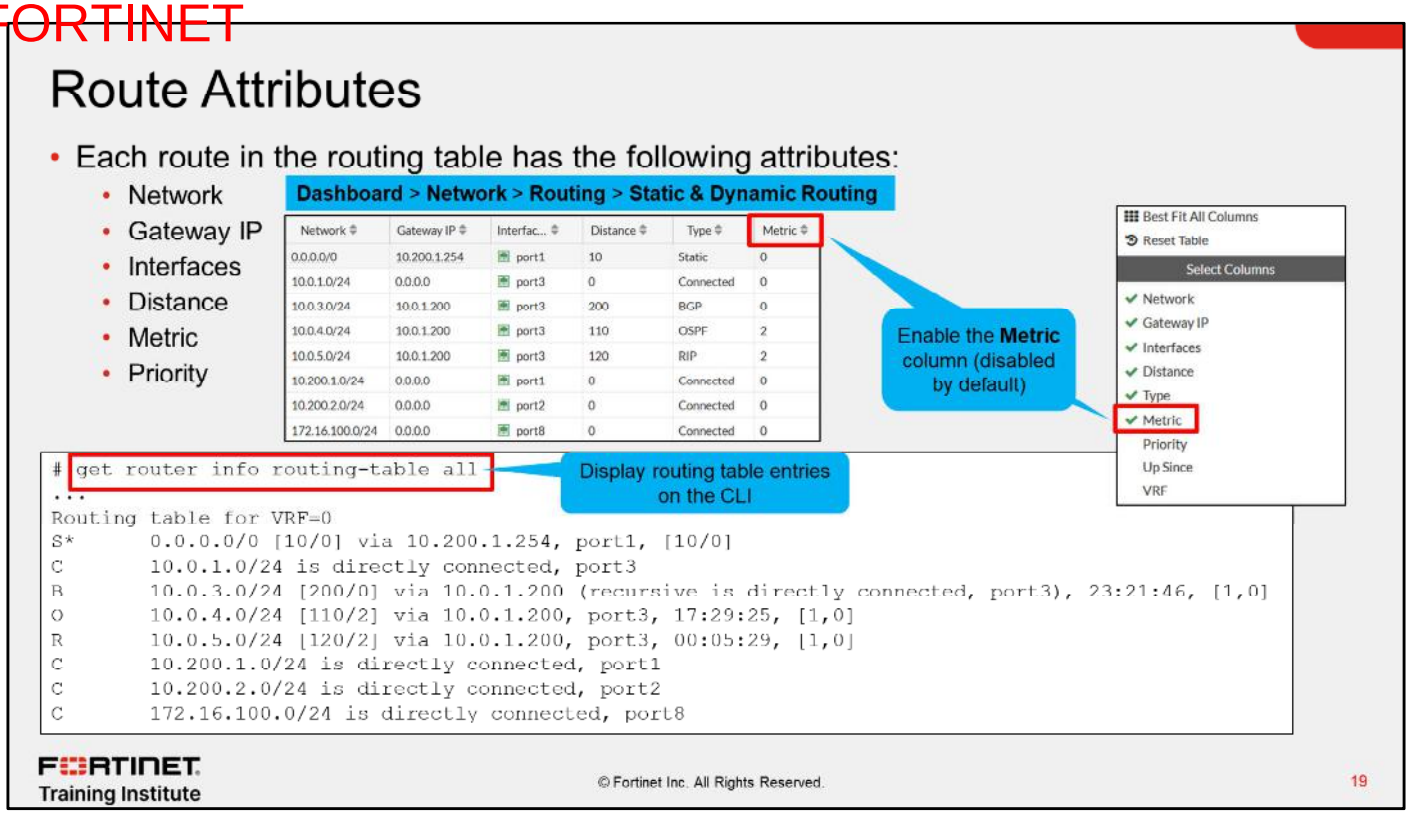


You can perform a route lookup on the routing monitor widget by clicking **Route Lookup**. Then, you must indicate at least the destination address to look up for, and optionally, the destination port, source address, protocol, and source interface.

The way the route lookup works is as follows:

- If you don't provide all lookup criteria, FortiGate considers only the routing table entries. FortiGate then highlights the matching route, if any.
- If you provide all lookup criteria, FortiGate considers both routing table and policy table entries. If the lookup matches a policy route, the GUI redirects you to the policy route page, and then highlights the corresponding matching policy route.

The example on this slide shows a route lookup tool for `8.8.8.8` and TCP as destination address and protocol, respectively. Because the administrator doesn't provide all criteria, FortiGate considers the routing table entries only. Then, the route lookup highlights the static default route as the matching route.



Each of the routes listed in the routing table includes several attributes with associated values.

The **Network** column lists the destination IP address and subnet mask to match. The **Interfaces** column lists the interface to use to deliver the packet.

The **Distance**, **Metric**, and **Priority** attributes are used by FortiGate to make various route selection decisions. You will learn about each of these in this lesson.

This slide also shows the command you can run to display the routing table on the FortiGate CLI. The `get router info routing-table all` command displays the same route entries as the routing monitor widget on the FortiGate GUI.

Distance

- First tiebreaker for duplicate routes (best route selection)
  - The lower the distance, the higher the preference
  - Set by the administrator (except connected routes)
- Best route selection:
  - Route with lowest distance is installed in the RIB
  - Standby routes (higher distance) are not installed in the RIB
    - They are installed in the routing table database
  - Multiple equal-distance duplicate routes but different protocol:
    - FortiGate keeps the route that was learned last (*avoid*)
- Default distance per route type:

Dashboard > Network > Routing > Static & Dynamic

Network	Gateway IP	Interfac...	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
10.200.1.0/24	0.0.0.0	port1	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0

Connected*	Static (SD-WAN zone)	Static (DHCP)	Static (Manual)	Static (IKE)	EBGP	OSPF	IS-IS*	RIP	IBGP
0	1	5	10	15	20	110	115	120	200

* Hardcoded

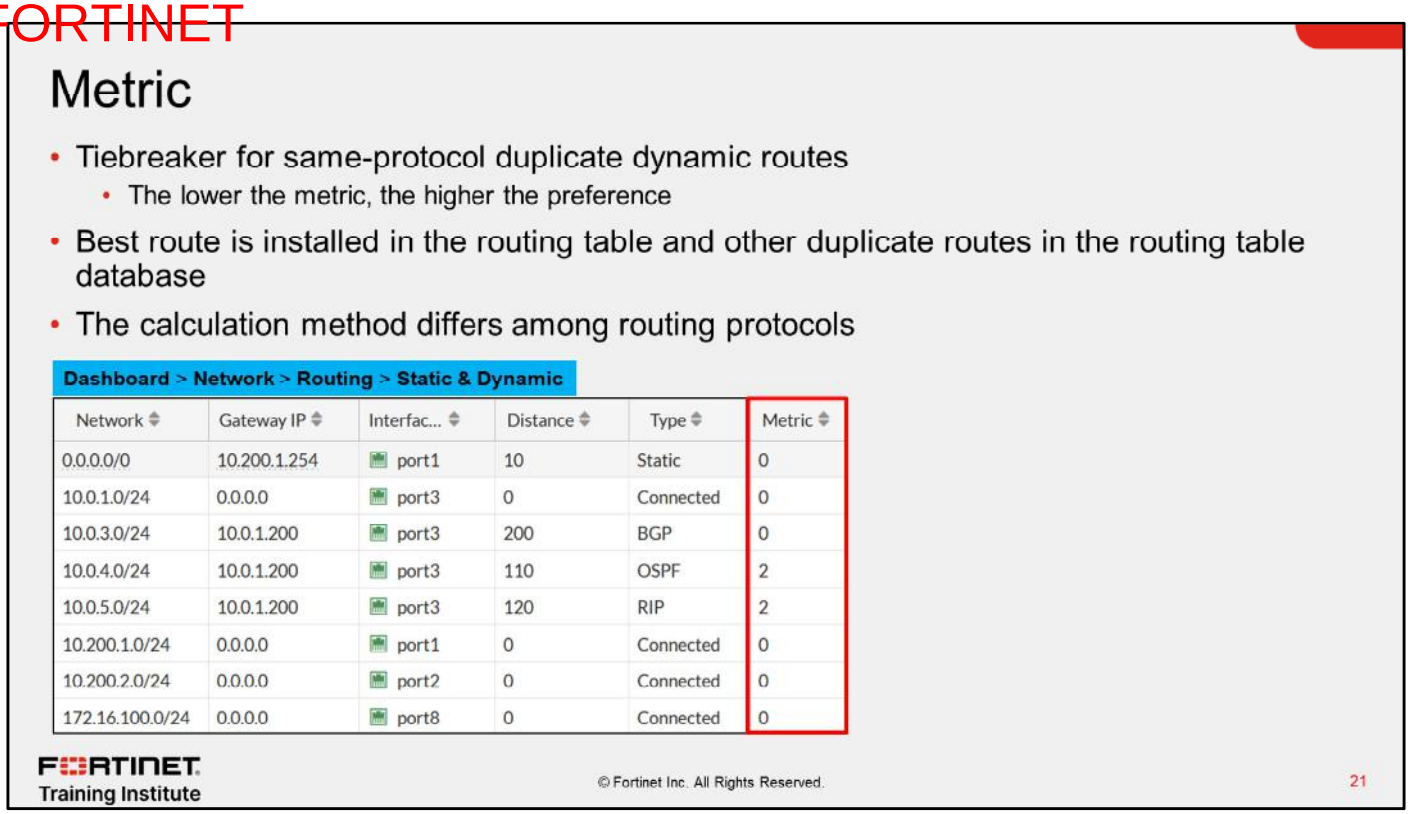
FORTINET Training Institute

20

Distance, or administrative distance, is the first tiebreaker that routers use to determine the best route for a particular destination. If there are two or more routes to the same destination (duplicate routes), the lowest-distance route is considered the best route and, as a result, is installed in the routing table. Other lower-distance routes to the same destination are standby routes and, as a result, are not installed in the routing table. Instead, they are installed in the routing table database. You will learn more about the routing table database in this lesson.

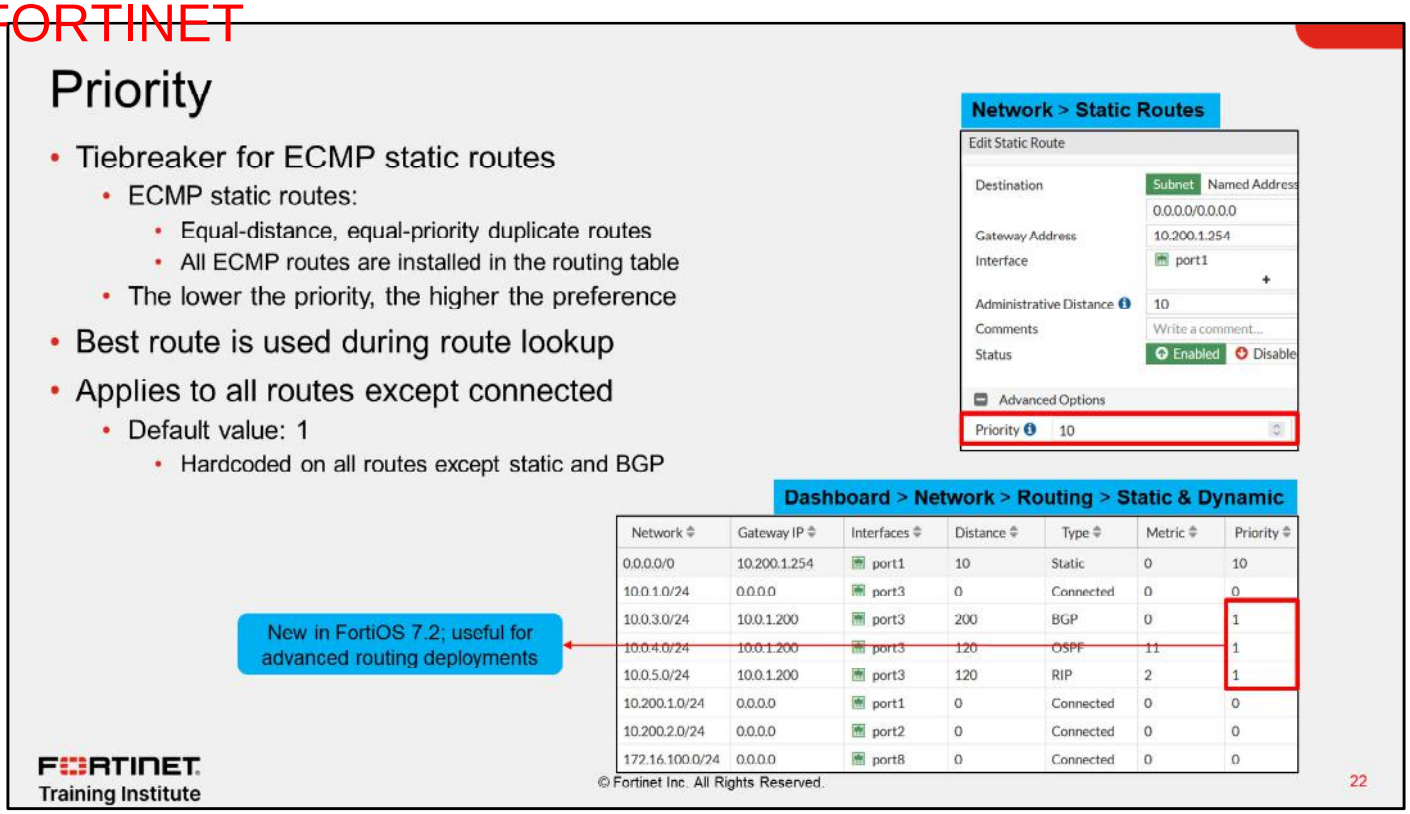
You can set the distance for all route types except connected and IS-IS routes. This slide shows the default values per type of route.

In case FortiGate learns two equal-distance routes to the same destination but that are sourced from different protocols, then FortiGate installs in the routing table the route that was learned *last*. For example, if you set the distance of BGP routes to 110, and there is another OSPF route to the same destination using the default administrative distance (110), then FortiGate keeps whichever route was learned last in the routing table. Because this behavior can lead to different results based on the timing of events, then it's not recommended to configure different-protocol routes with the same distance.



When a dynamic route protocol learns two or more routes to the same destination, it uses the metric as a tiebreaker to identify the best route. The lower the metric, the higher the preference. The dynamic routing protocol then installs the best route in the routing table and the higher-metric routes in the routing table database. Note that the metric is used as tiebreaker for same-protocol dynamic routes, and *not* between different-protocol dynamic routes.

The metric calculation differs among routing protocols, and the details are not covered in this course. For example, RIP uses the hop count, which is the number of routers the packet must pass through to reach the destination. OSPF uses cost, which is determined by the link bandwidth.



When there are two or more duplicate static routes that have the same distance, FortiGate installs all of them in the routing table. If they also have the same priority, then the routes are known as ECMP static routes, and you will learn more about them in this lesson.

The priority setting enables administrators to break the tie among ECMP *static* routes. The result is that, during the route lookup process, FortiGate selects as the best route the static route with the lowest priority among all the equal-distance duplicate static routes. The lower the priority value, the higher the preference.

Starting FortiOS 7.2, the priority attribute applies to all routes except connected routes and is set to 1 by default. Before FortiOS 7.2, the attribute applied to static routes only and was set to 0 by default. When you upgrade to FortiOS 7.2, FortiOS automatically increases the priority of static routes by 1, and a value of 0 is not longer valid.

For dynamic routes, you can change the priority of BGP routes only. The priority of other dynamic routes is hardcoded to 1. The use of the priority value in dynamic routes is useful for advanced routing deployments involving SD-WAN and multiple virtual routing and forwarding (VRF) IDs. The details on how the priority attribute is beneficial for such cases is outside the scope of this course.

For static routes, you can configure the priority setting under the **Advanced Options** on the FortiGate GUI, as shown on this slide.

To view the priority in the routing monitor widget, you must enable the priority column (disabled by default). You can also view the priority on the routing table on the FortiGate CLI, which you will learn about later in this lesson.

Knowledge Check

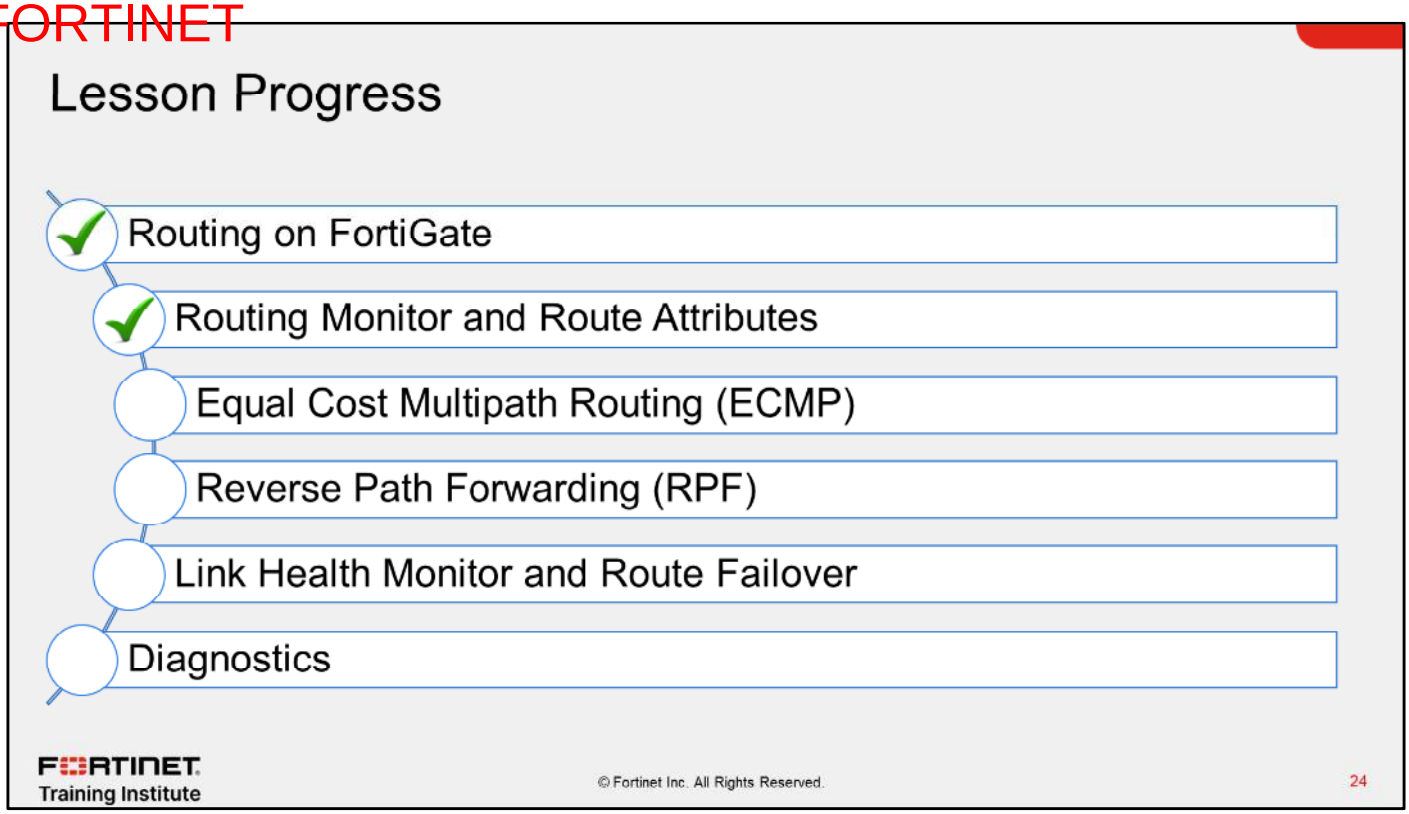
1. The priority attribute applies to which type of routes?
   - ✓ A. Static
   - B. Connected

2. Which attribute does FortiGate use to determine the *best* route for same-protocol duplicate dynamic routes?
   - A. Priority
   - ✓ B. Metric

3. Which routes are installed in the routing table?
   - ✓ A. Best active routes
   - B. Policy routes

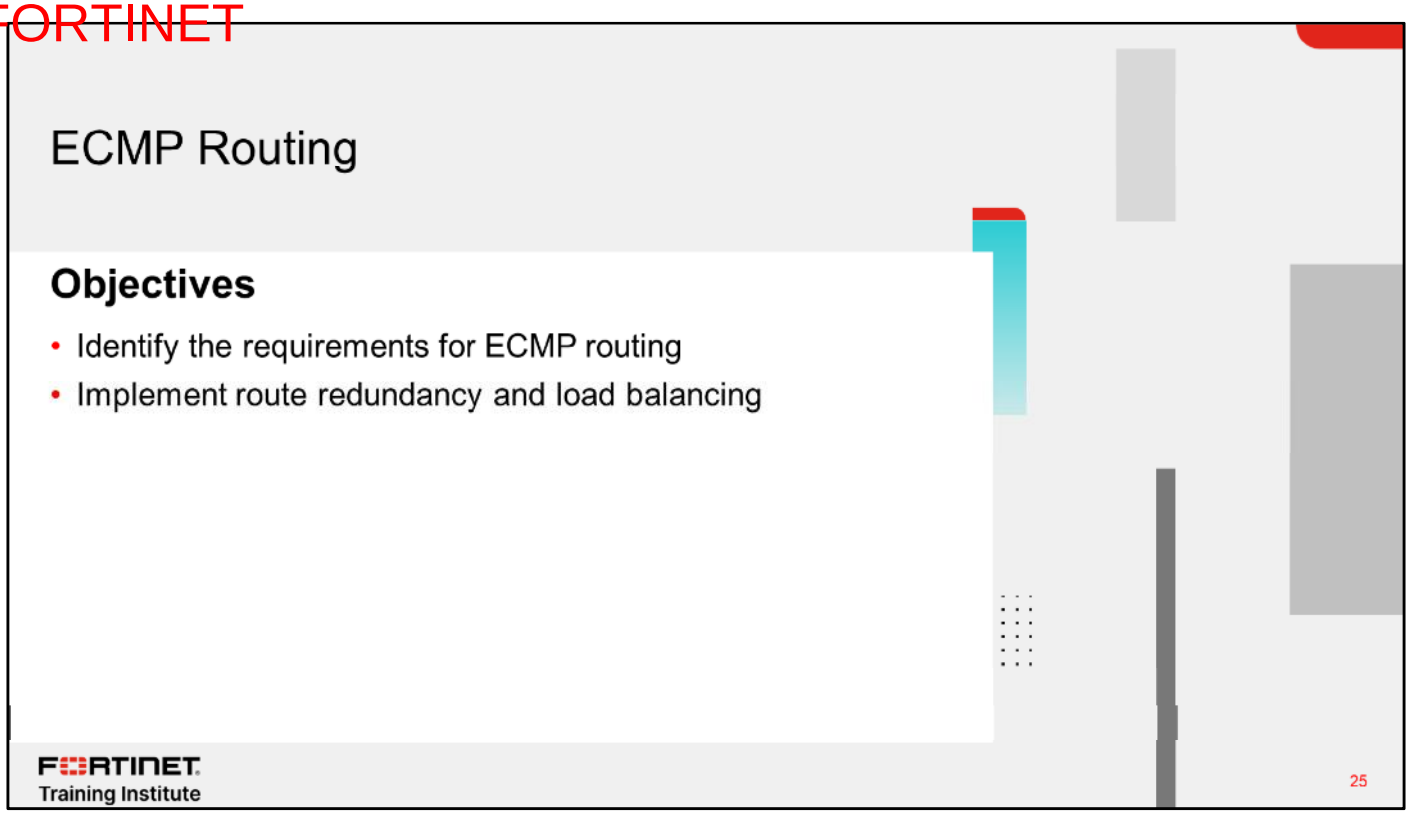
FORTINET Training Institute

23



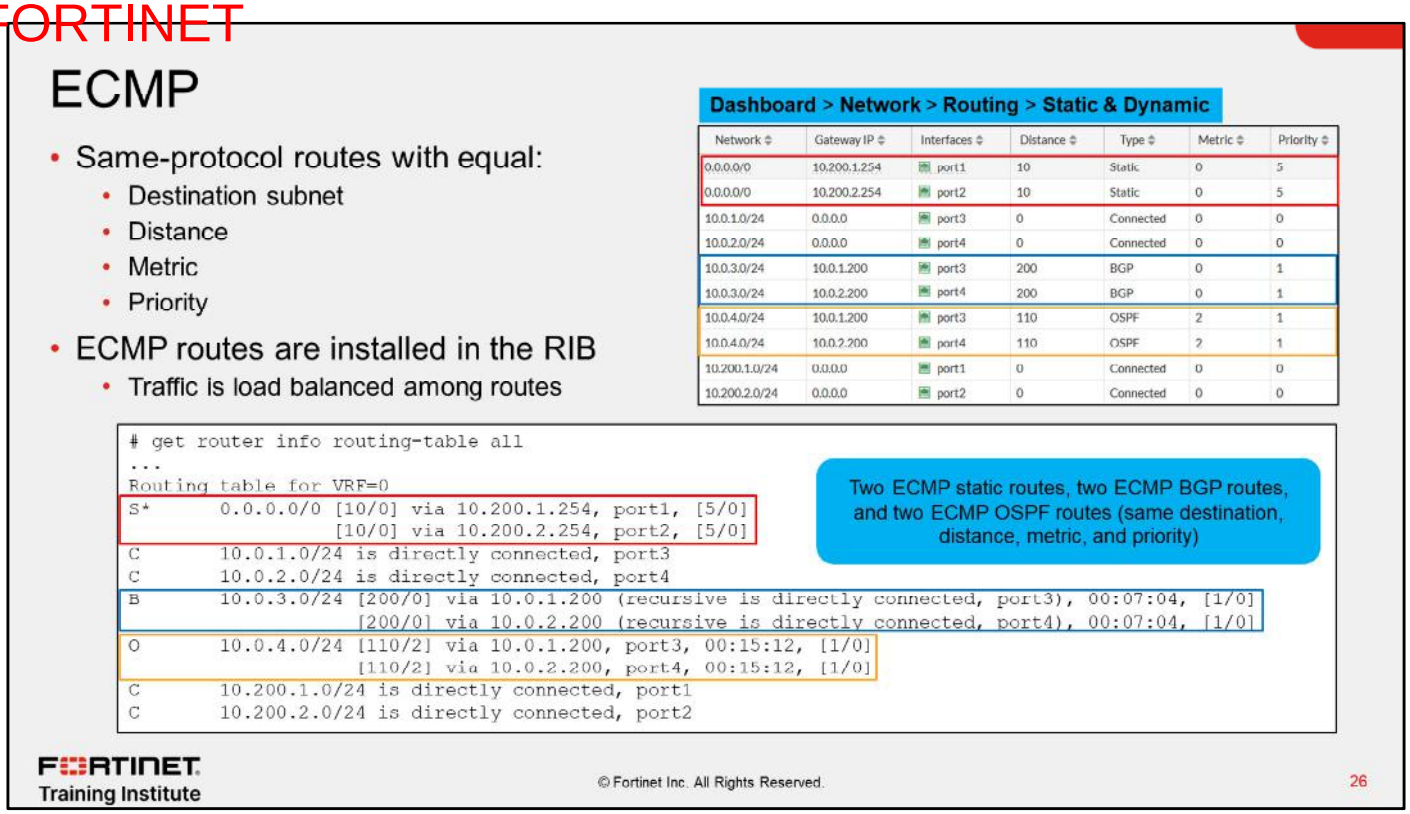
Good job! You now understand the routing monitor and route attributes.

Now, you will learn about ECMP routing.



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

By demonstrating competence in ECMP, you should be able to identify the requirements for implementing ECMP and ECMP load balancing.

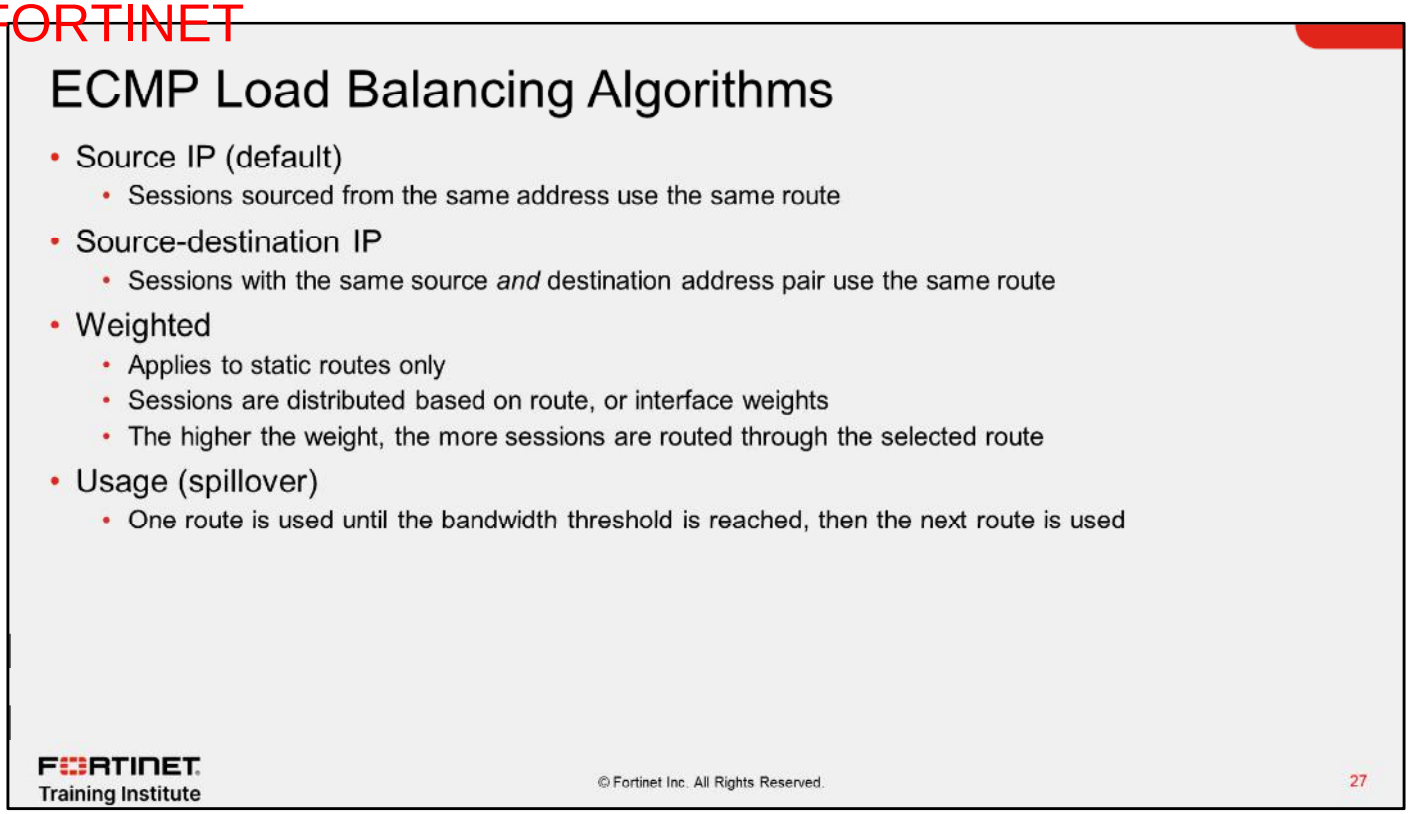


So far, you've learned about the different route attributes that FortiGate looks at to identify the best route to a destination.

But what happens when two or more routes of the same type have the same destination, distance, metric, and priority? These routes are called equal cost multipath (ECMP) routes, and FortiGate installs all of them in the routing table. FortiGate also load balances the traffic among the ECMP routes.

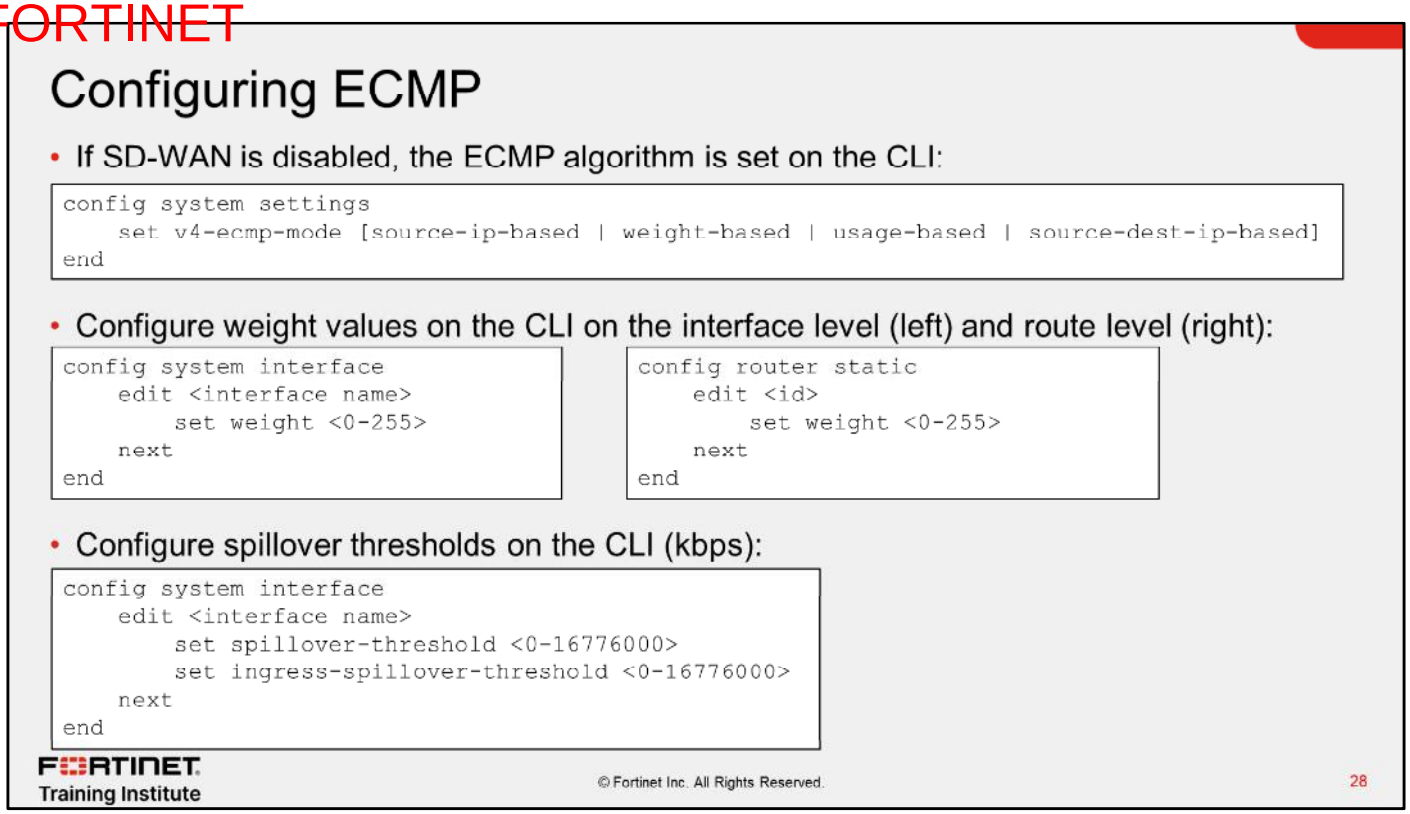
The example on this slide shows two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes. For each ECMP group, the destination subnet, distance, metric, and priority are the same.

The result is that FortiGate installs both routes of each ECMP group in the routing table. This lesson, however, focuses on ECMP static routes only.



ECMP can load balance sessions using one of the following four algorithms:

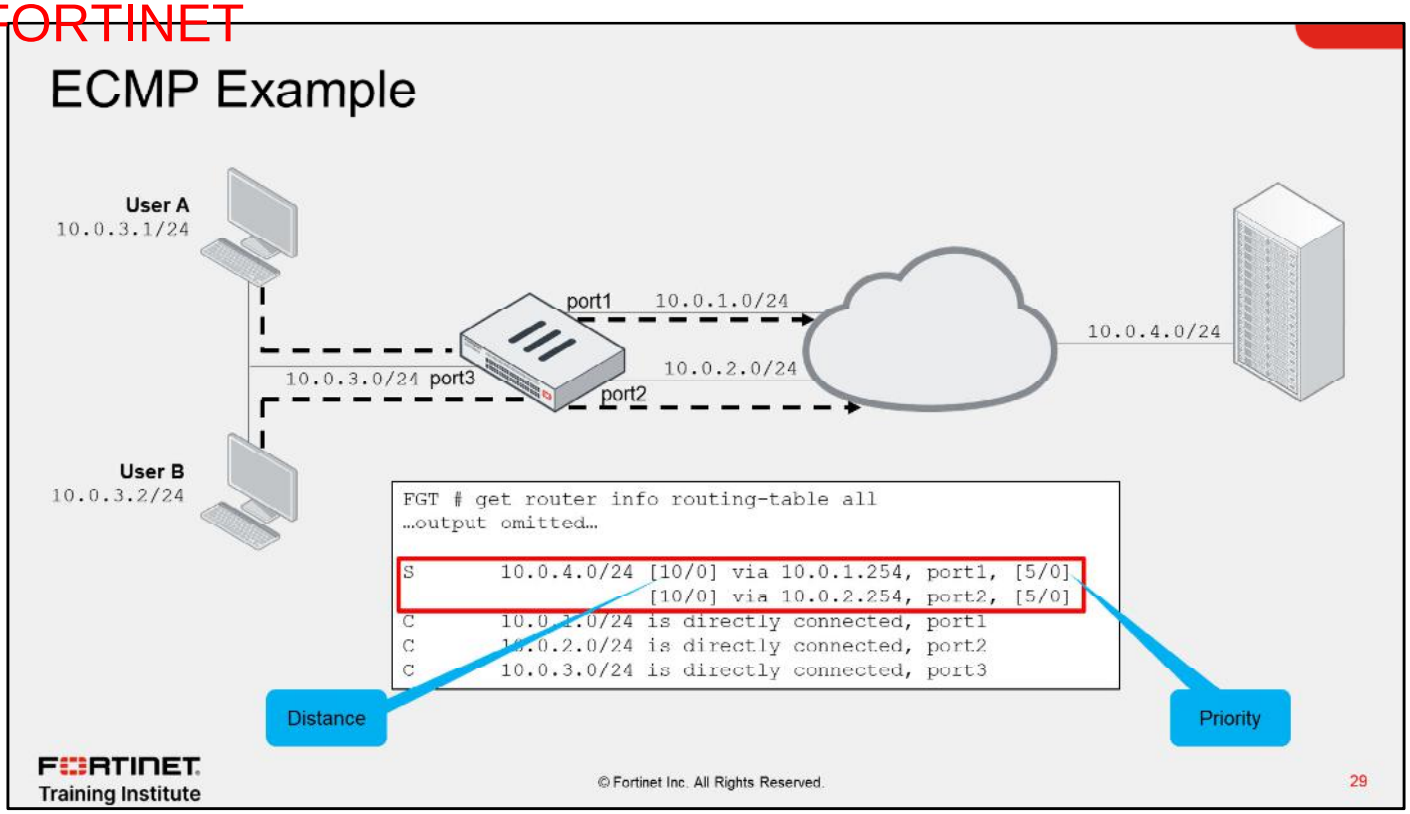
- Source IP: This is the default algorithm. FortiGate uses the same ECMP route to route sessions sourced from the same address.
- Source-destination IP: FortiGate uses the same ECMP route to route sessions with the same source-destination IP address pair.
- Weighted: Applies to static routes only. FortiGate load balances sessions based on the route weight or the respective interface weight. The higher the weight, the more sessions FortiGate routes through the selected route.
- Usage (spillover): FortiGate sends sessions to the interface of the first ECMP route until the bandwidth of the interface reaches the configured spillover limit. After the spillover limit is reached, FortiGate uses the interface of the next ECMP route.



If SD-WAN is disabled, you can change the ECMP load balancing algorithm on the FortiGate CLI using the commands shown on this slide.

When SD-WAN is enabled, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, when you enable SD-WAN, you control the ECMP algorithm with the `load-balance-mode` setting.

For spillover to work, you must also configure the egress and ingress spillover thresholds, as shown on this slide. The thresholds are set to `0` by default, which disables spillover check. For weighted algorithm, you must configure the weights on the interface level or route level, as shown on this slide.

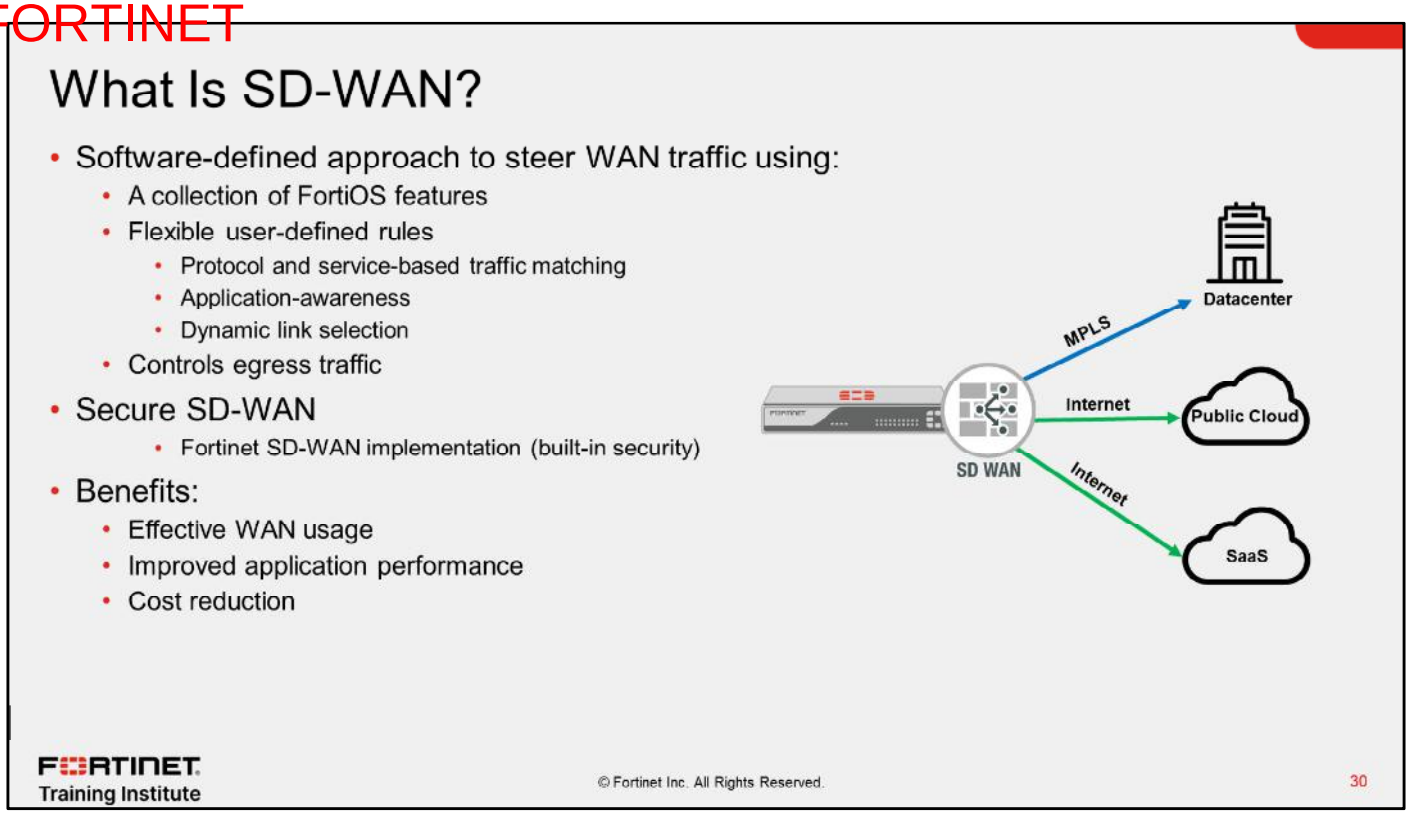


In the scenario shown on this slide, FortiGate has ECMP routes for the `10.0.4.0/24` subnet on port1 and port2. Using the default ECMP algorithm (source IP based), FortiGate may use any of the two routes to route traffic from user A and user B.

In the example shown on this slide, FortiGate selects the route over port1 for user A, and the route over port2 for user B. FortiGate continues to use the same selected routes for the same traffic. In the route over port1 is removed from the routing table, FortiGate automatically starts to forward the traffic sourced from both users and destined to `10.0.4.0/24` through port2.

ECMP enables you to use multiple paths for the same destination, as well as provide built-in failover. Usually, you want to use ECMP for mission-critical services that require high availability. Another reason to use ECMP is for bandwidth aggregation. That is, you can leverage the bandwidth of multiple links by load balancing sessions across them.

While ECMP enables you to leverage multiple WAN links on FortiGate, you may want to use SD-WAN because of the additional benefits.



According to Gartner, software-defined WAN (SD-WAN) provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls. Fortinet implementation of SD-WAN is called secure SD-WAN because it also provides security by leveraging the built-in security features available in FortiOS.

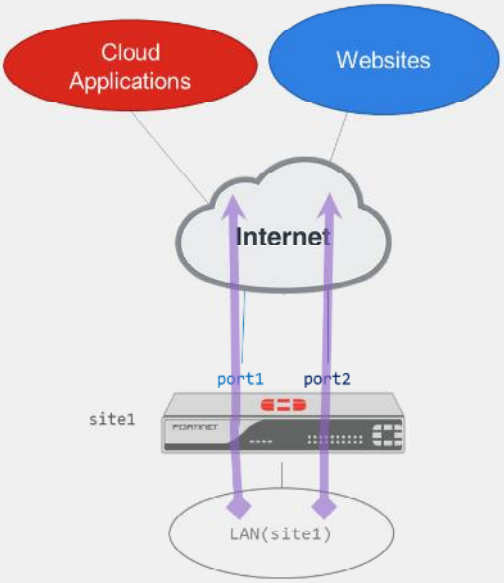
Secure SD-WAN relies on well-known FortiOS features such as IPsec, auto-discovery VPN (ADVPN), link monitoring, advanced routing, internet services database (ISDB), traffic shaping, UTM inspection, and load balancing. The administrator can then combine these features and set rules that define how FortiGate steers traffic across the WAN based on multiple factors such as the protocol, service, or application identified for the traffic, and the quality of the links. Note that SD-WAN controls egress traffic, not ingress traffic. This means that the return traffic may use a different link from the one SD-WAN chose for egress.

One benefit of SD-WAN is effective WAN usage. That is, you can use public (for example, broadband, LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of links to connect sites to private and public networks is known as hybrid WAN. A hybrid WAN reduces costs mainly because administrators usually steer more traffic over low-cost fast internet links than high-cost slow private links. The result is that private links, such as MPLS links, are often used to steer critical traffic only, or as failover links for high availability.

Another benefit of SD-WAN is an improved application performance because you can steer traffic through the best link that meets the application requirements. During congestion, you can leverage traffic shaping to prioritize sensitive and critical applications over less important ones. Also, the support of ADVPN shortcuts enables SD-WAN to use direct IPsec tunnels between sites to steer traffic, resulting in lower latency for traffic between the sites (spokes), and less load on the central locations (hubs).

Direct Internet Access With SD-WAN

- Traffic steered across multiple internet links
- Typical operation:
  - Critical/sensitive traffic expedited and steered over best performing links
  - Costly links used for critical traffic or failover
  - Static default routing



FORTINET Training Institute

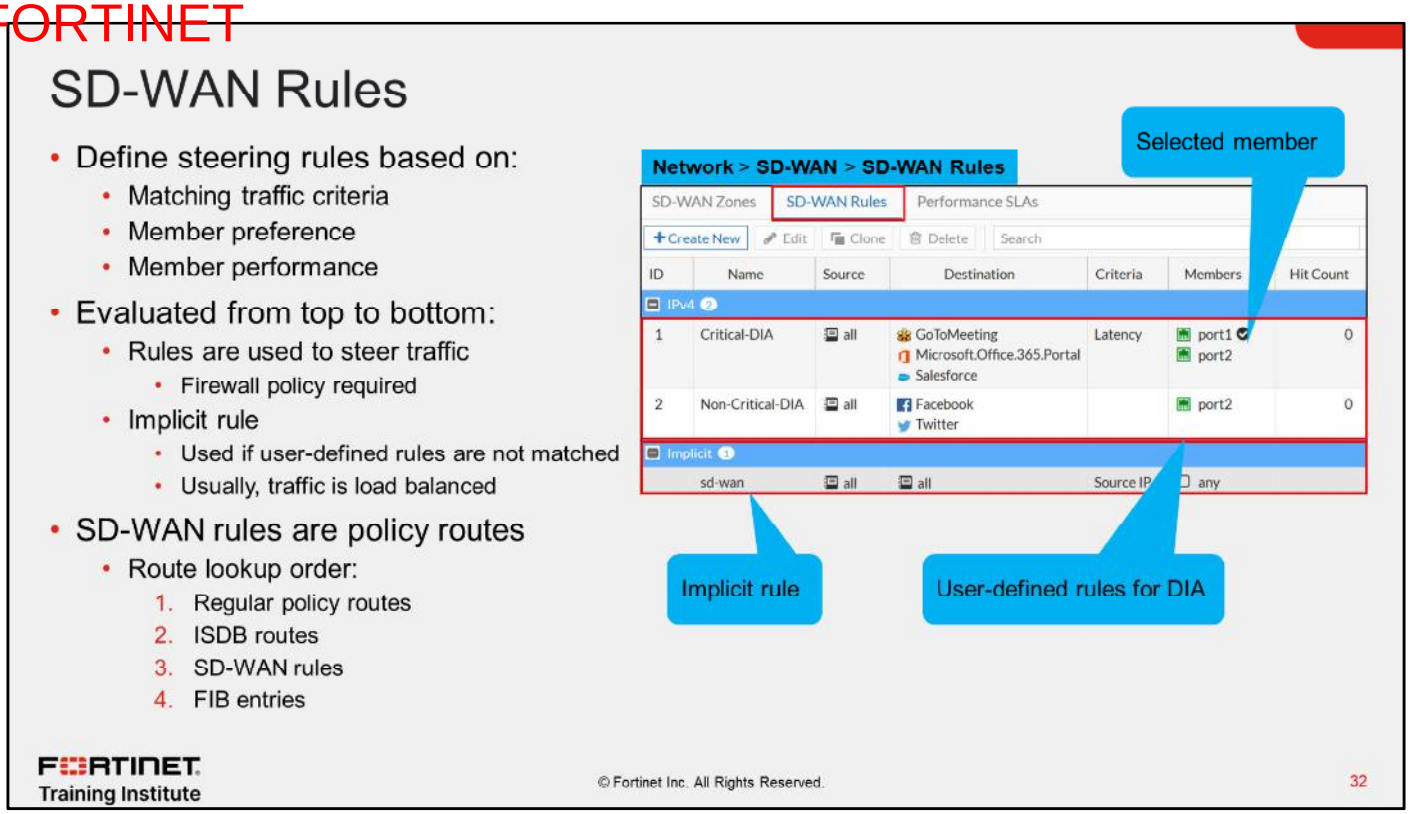
31

Direct internet access (DIA), also known as local breakout, is arguably the most common use case for SD-WAN. A site has multiple internet links (also known as underlay links), and the administrator wants FortiGate to steer internet traffic across the links (also known as members). The links are connected to FortiGate using different types of physical interfaces: physical port, VLAN, link aggregation (LAG), USB modem, or through FortiExtender.

Usually, sensitive traffic is expedited and steered over the best performing links, while non-critical traffic is distributed across one or more links using a best effort approach. Costly internet links are commonly used as backup links, or to steer critical traffic only.

For routing, a typical configuration makes use of static default routes. However, in some cases, BGP is used between the ISP and FortiGate, especially if the site must advertise a public IP prefix.

The example on this slide shows a basic DIA deployment. FortiGate has two internet links. One link is connected to port1 and the other to port2. FortiGate uses both links to steer traffic sourced from the LAN and destined to cloud applications and websites on the internet.

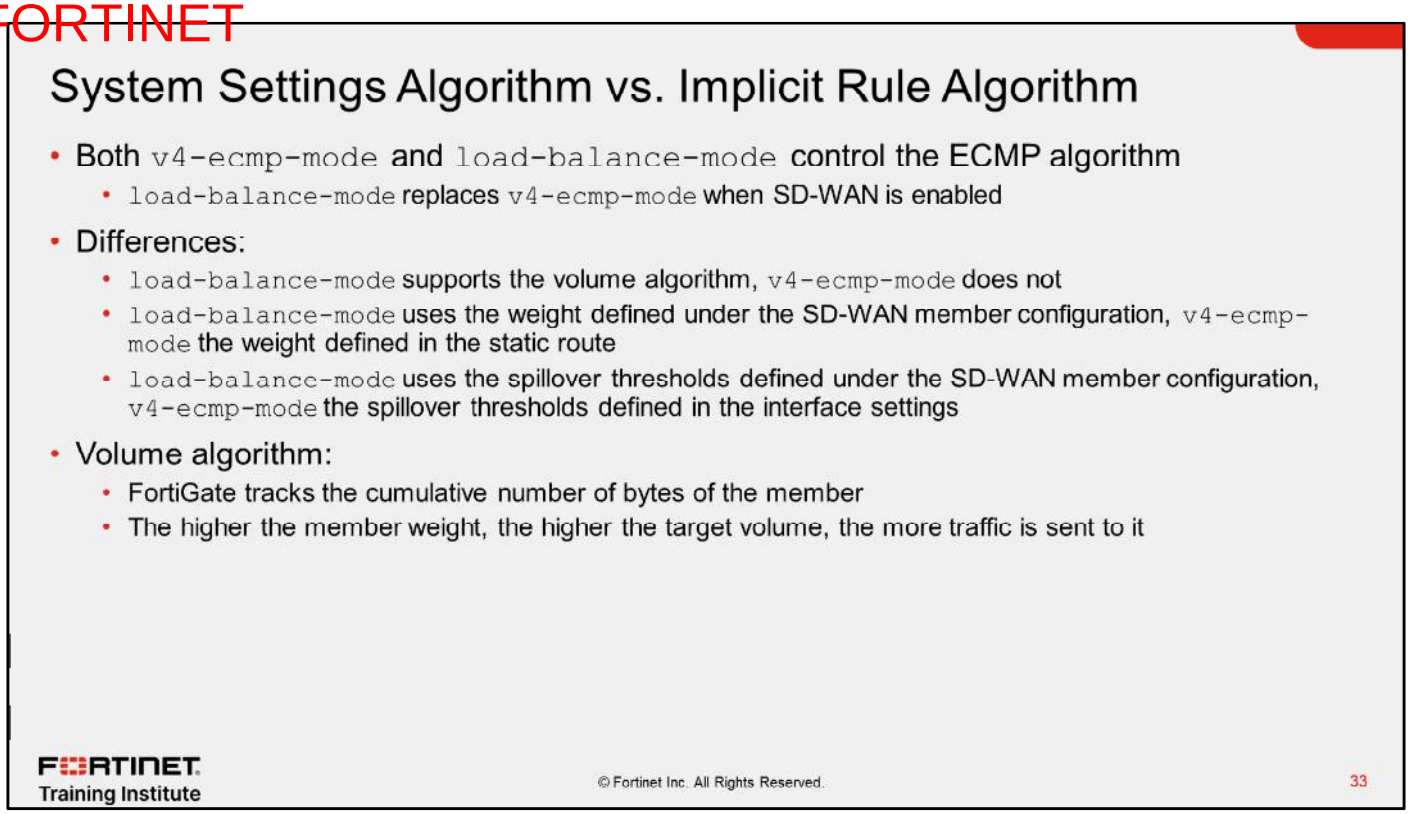


SD-WAN rules represent the intelligence of the SD-WAN solution and the software-defined aspect of it. When you configure an SD-WAN rule, you first define the application or traffic pattern to match. After that, you indicate the preferred members and/or zones to steer the matching traffic to, and in some cases, the performing metrics that the member must meet to be eligible for steering traffic.

SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom, using the first match. However, unlike firewall policies, they are used to steer traffic, and *not* to allow traffic. That is, you must configure corresponding firewall policies to allow the SD-WAN traffic. If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. The implicit rule instructs FortiGate to perform standard routing on traffic. Because SD-WAN deployments usually have multiple routes to the same destination—that is, ECMP routes—then traffic that matches the implicit rule is usually load balanced across multiple SD-WAN members.

SD-WAN rules are essentially policy routes. Like regular policy routes, SD-WAN rules route traffic based on multiple criteria. That is, when you configure an SD-WAN rule, the kernel installs a corresponding policy route that reflects the source, destination, service, and outgoing interfaces configured in the SD-WAN rule. When FortiGate performs a route lookup, it checks the routes in the order of sequence shown on this slide. For example, SD-WAN rules have precedence over FIB entries, but not over regular policy routes.

The example on this slide shows two user-defined rules named **Critical-DIA** and **Non-Critical-DIA**, which are used to steer traffic in our basic DIA setup. The **Critical-DIA** steers **GoToMeeting**, **Microsoft.Office.365.Portal**, and **Salesforce** traffic to the member with the lowest latency, between **port1** and **port2**. The example shows that **port1** is selected because it is the member with the check mark beside it. The **Non-Critical-DIA** rule steers Facebook and Twitter traffic to **port2**. The implicit rule, located at the bottom of the list, is used if none of the two user-defined rules are matched.



When you enable SD-WAN, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, after you enable SD-WAN, you now control the ECMP algorithm with the `load-balance-mode` setting.

There are some differences between the two settings. The main difference is that `load-balance-mode` supports the volume algorithm, and `v4-ecmp-mode` does not. In addition, the related settings such as weight and spillover thresholds are configured differently. That is, when you enable SD-WAN, the weight and spillover thresholds are defined on the SD-WAN member configuration. When you disable SD-WAN, the weight and spillover thresholds are defined on the static route and interface settings, respectively.

When you set the ECMP algorithm to volume, FortiGate load balances sessions across members based on the measured interface volume and the member weight. That is, the volume algorithm instructs FortiGate to track the cumulative number of bytes of each member and to distribute sessions based on the weight. The higher the weight, the higher the target volume of the interface and, as a result, the more traffic FortiGate sends to it.

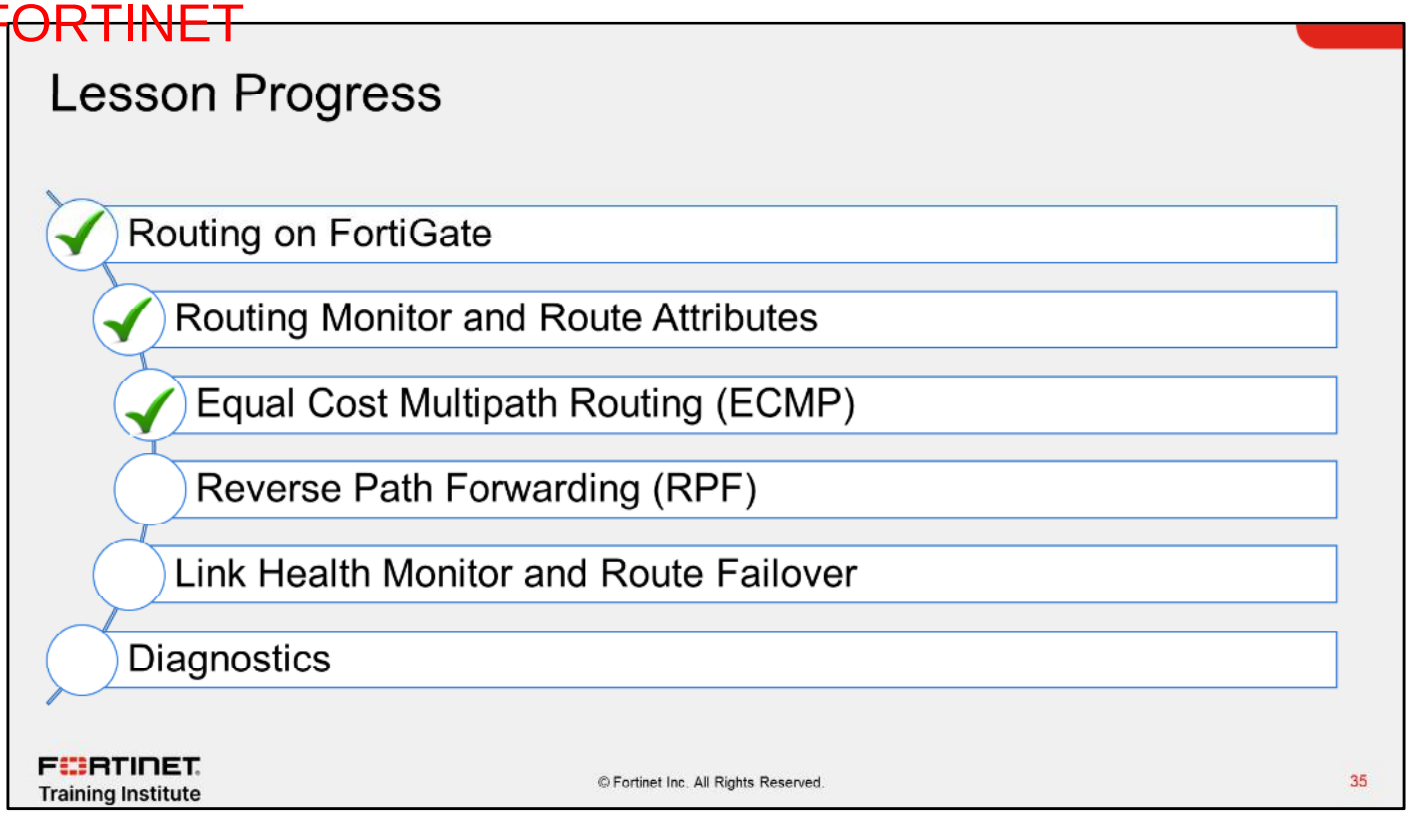
Knowledge Check

1. What is the default ECMP algorithm on FortiGate?
   - A. Weighted
   - ✓ B. Source IP

2. How does FortiGate load balance traffic when using the spillover algorithm in ECMP routing?
   - ✓ A. Sessions are distributed based on interface threshold.
   - B. Sessions are distributed based on route weight.

FORTINET Training Institute

34

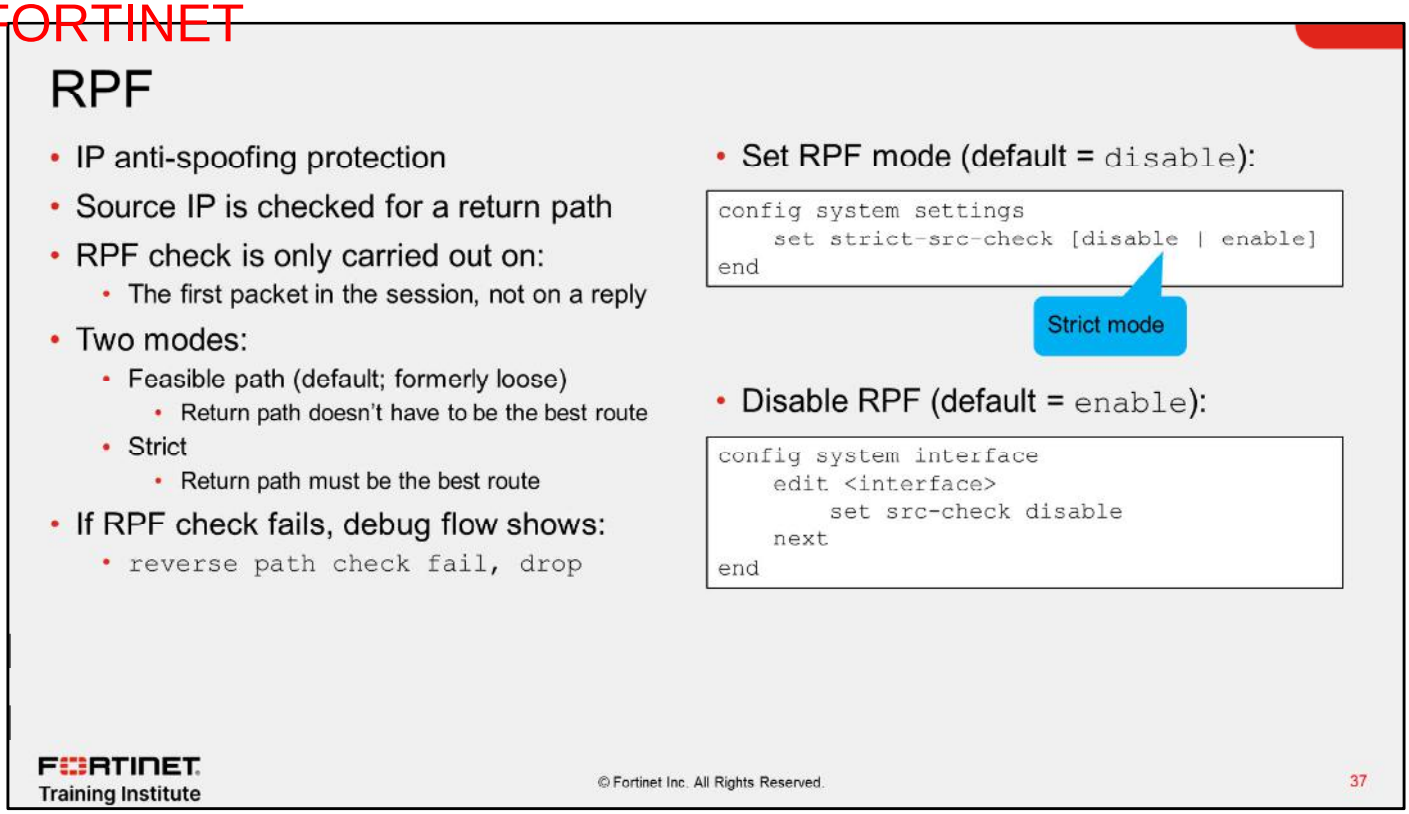


Good job! You now understand ECMP routing.

Now, you will learn about reverse path forwarding.

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

By demonstrating competence in RPF, you should be able to identify and block IP spoofing attacks in your network.



The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table.

The premise behind the RPF check is that if FortiGate receives a packet on an interface, and FortiGate doesn't have a route to the packet source address through the incoming interface, then the source address of the packet could have been forged, or the packet was routed incorrectly. In either case, you want to drop that unexpected packet, so it doesn't enter your network.

FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session.

There are two RPF check modes:

- Feasible path: Formerly known as loose, it's the default mode. In this mode, FortiGate verifies that the routing table contains a route that matches the source address of the packet and the incoming interface. The matching route doesn't have to be the best route in the routing table for that source address. It just has to match the source address and the incoming interface of the packet.

- Strict: In this mode, FortiGate also verifies that the matching route is the best route in the routing table. That is, if the routing table contains a matching route for the source address and incoming interface, but there is a better route for the source address through another interface, then, the RPF check fails.

This slide also shows how to change the RPF check mode on the FortiGate CLI, as well as how to disable the RPF check on the interface level.