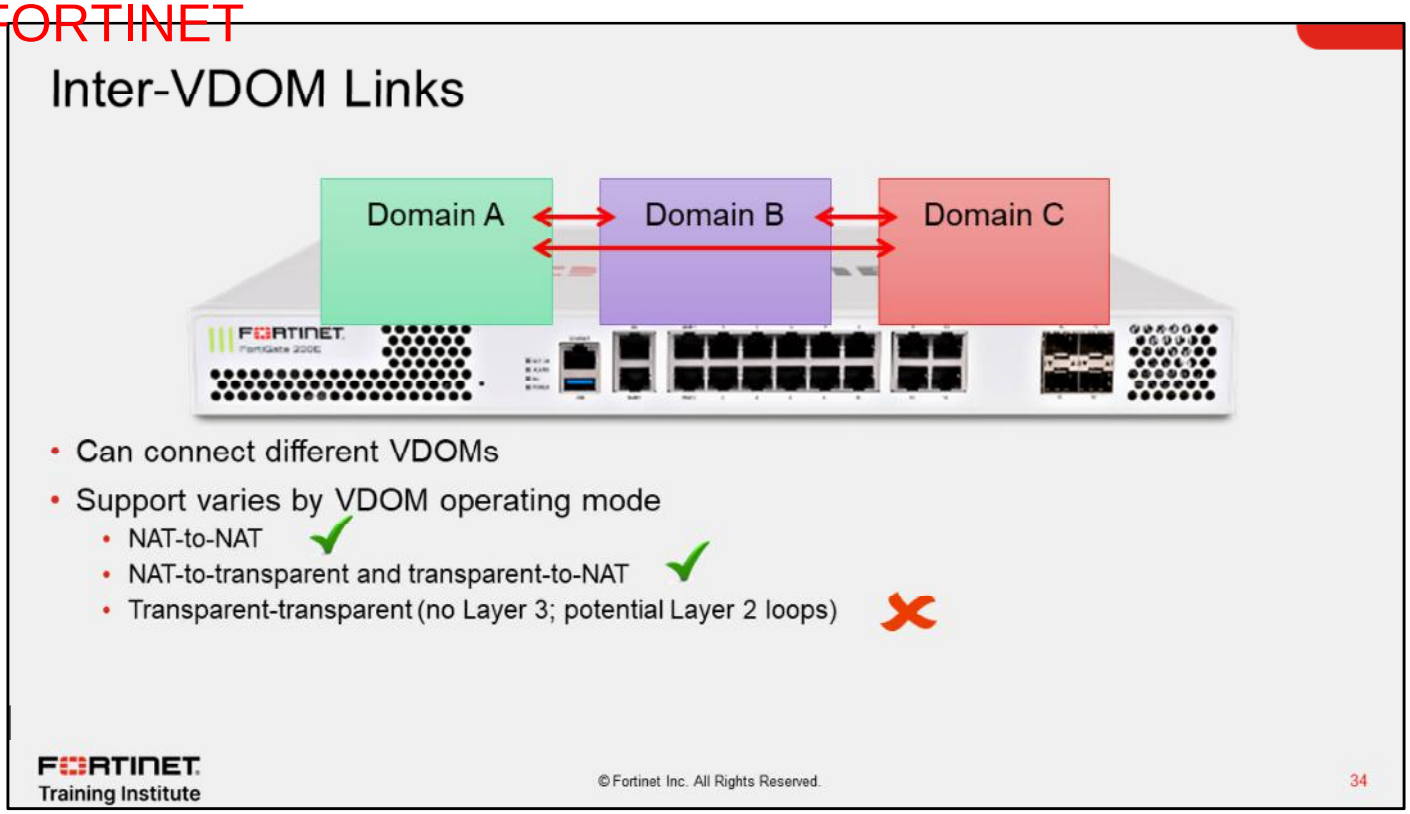
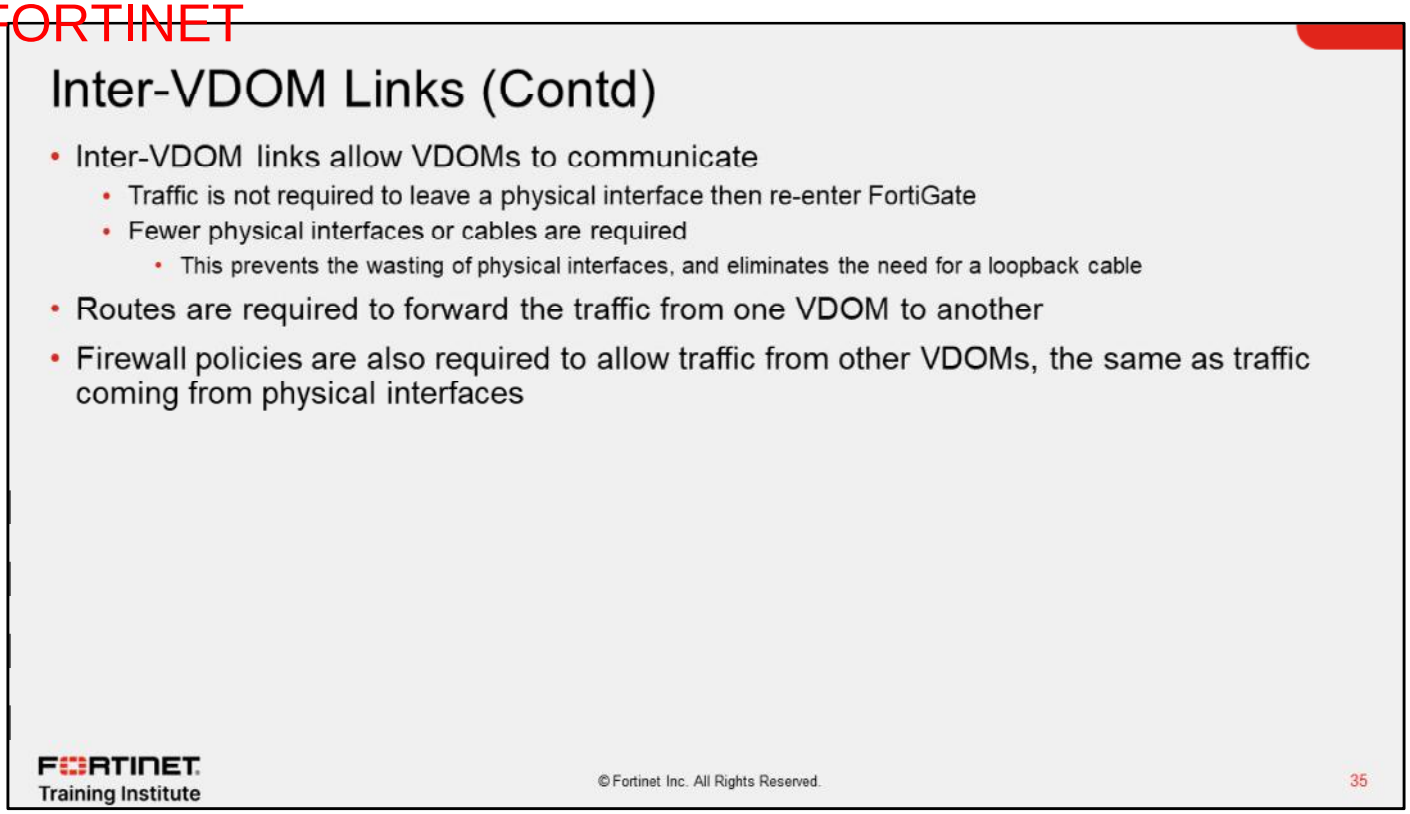


To review, each VDOM behaves like it is on a separate FortiGate device. With separate FortiGate devices, you would normally connect a network cable and configure routing and policies between them. But VDOMs are on the same FortiGate. So, how should you route traffic between them?
The solution is inter-VDOM links. Inter-VDOM links are a type of virtual interface that route traffic between VDOMs. This removes the need to loop a physical cable between two VDOMs.

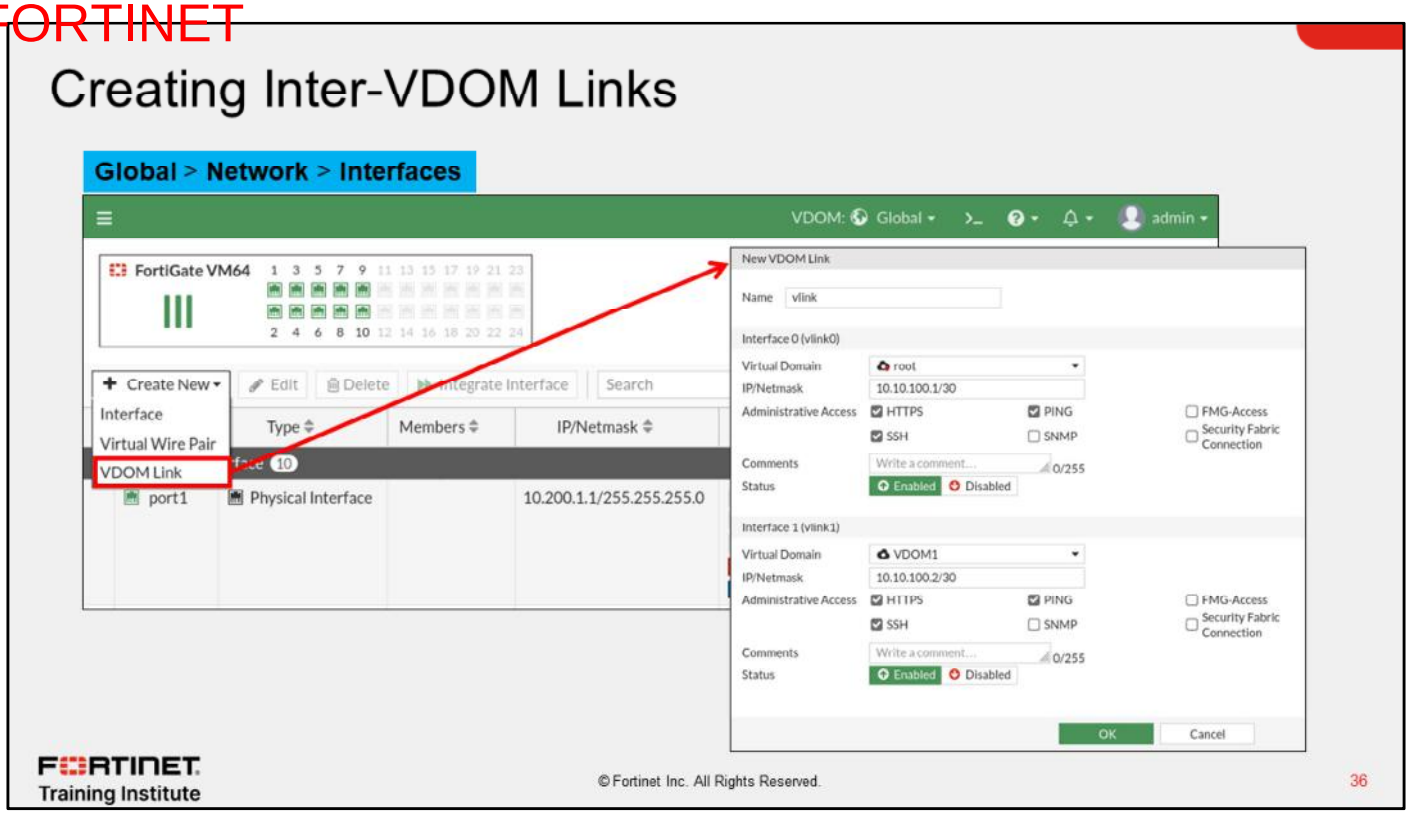
In the case of a NAT-to-NAT inter-VDOM link, both sides of the link must be on the same IP subnet, because you are creating a point-to-point network connection.

Note that like using inter-VLAN routing, Layer 3 must be involved—you cannot create an inter-VDOM link between Layer 2 transparent mode VDOMs. At least one of the VDOMs must be operating in NAT mode. This, among other benefits, prevents potential Layer 2 loops.

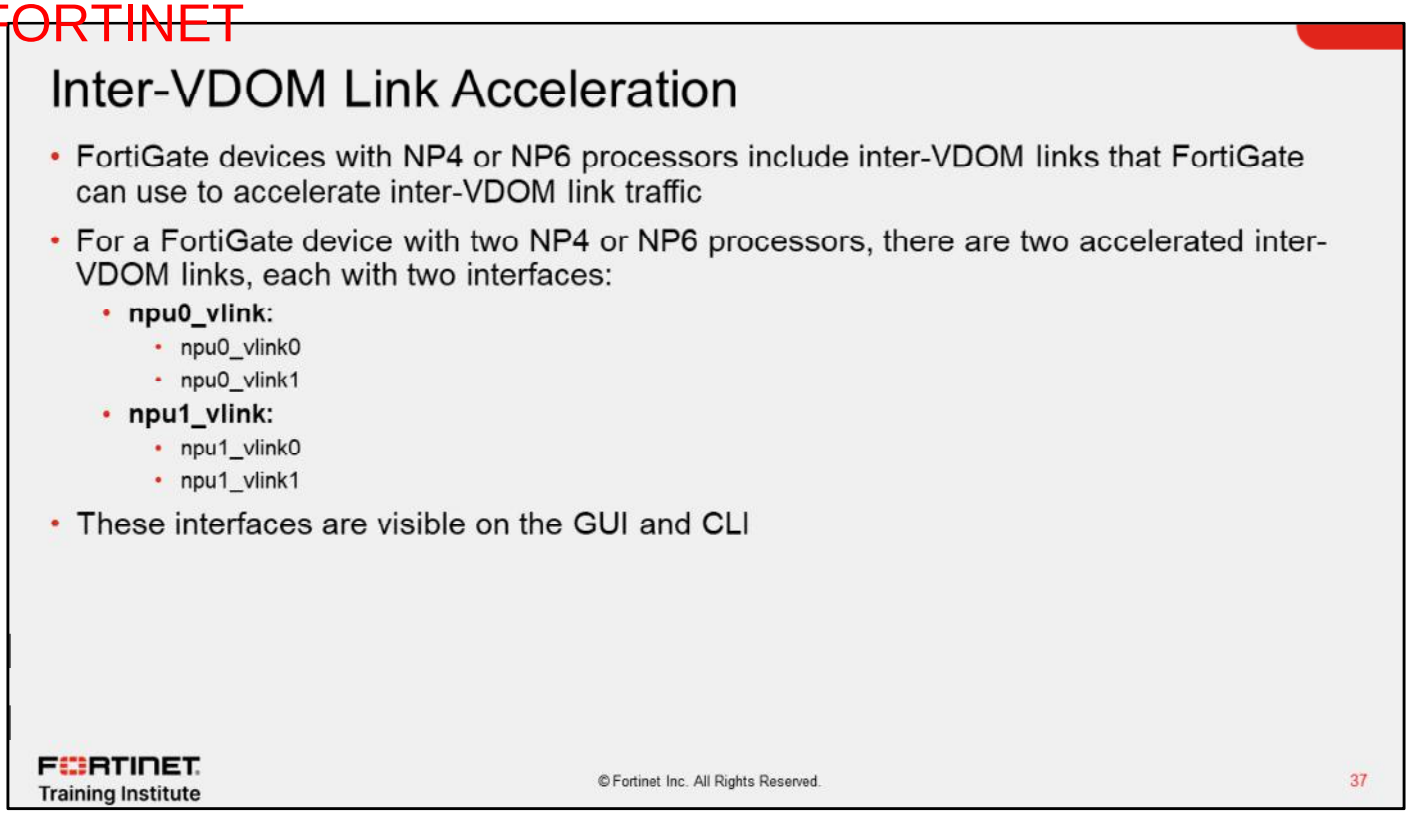


When creating inter-VDOM links, you must create the virtual interfaces. You must also create the appropriate firewall policies in each VDOM, just as you would if the traffic were arriving on a network cable, otherwise, FortiGate will block it.

Additionally, routes are required to correctly route packets between two VDOMs.



On the GUI, you create a network interface in the **Global** settings. To create the virtual interface, click **Create New**, and then select **VDOM Link**.



FortiGate devices with NP4 or NP6 processors include inter-VDOM links that FortiGate can use to accelerate inter-VDOM link traffic. For a FortiGate with two NP4 or NP6 processors, there are two accelerated inter-VDOM links, each with two interfaces:

- **npu0_vlink:**
  - npu0_vlink0
  - npu0_vlink1
- **npu1_vlink:**
  - npu1_vlink0
  - npu1_vlink1

These interfaces are visible on the GUI and CLI. By default, the interfaces in each inter-VDOM link are assigned to the root VDOM. To use these interfaces to accelerate inter-VDOM link traffic, assign each interface in the pair to the VDOMs that you want to offload traffic between. For example, if you have added a VDOM named *New-VDOM* to a FortiGate with NP4 processors, you can click **System** > **Network** > **Interfaces** and edit the **npu0-vlink1** interface and set the VDOM to *New-VDOM***.** This results in an accelerated inter-VDOM link between *root* and *New-VDOM.*

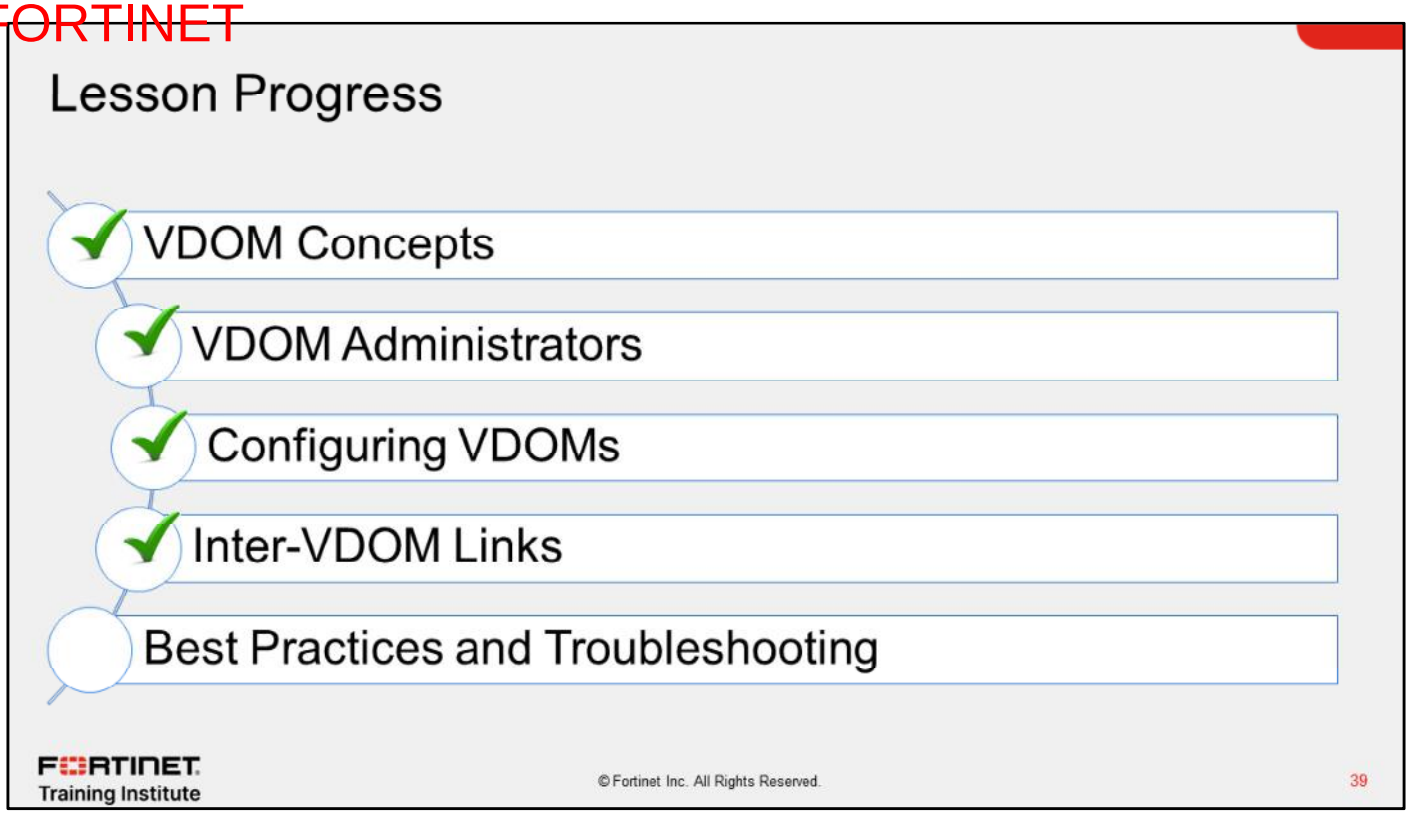
Knowledge Check

1. What is a requirement for creating an inter-VDOM link between two VDOMs?
   - A. The NGFW mode of at least one VDOM must be profile based.
   - ✓ B. At least one of the VDOMs must be operating in NAT mode.

2. Which type of VDOM link requires that both sides of the link be assigned an IP address within the same subnet?
   - A. NAT-to-transparent
   - ✓ B. NAT-to-NAT

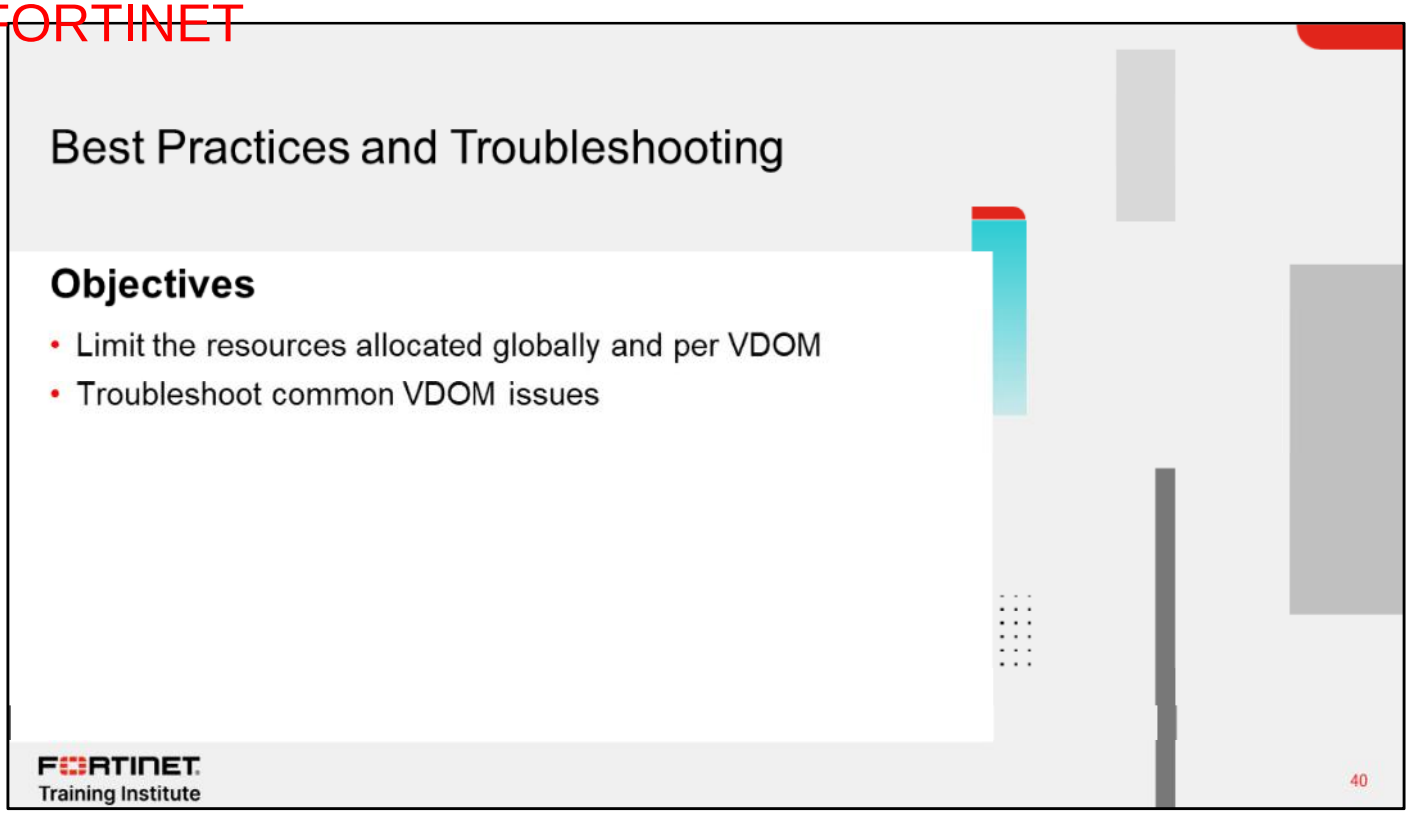
FORTINET Training Institute

38



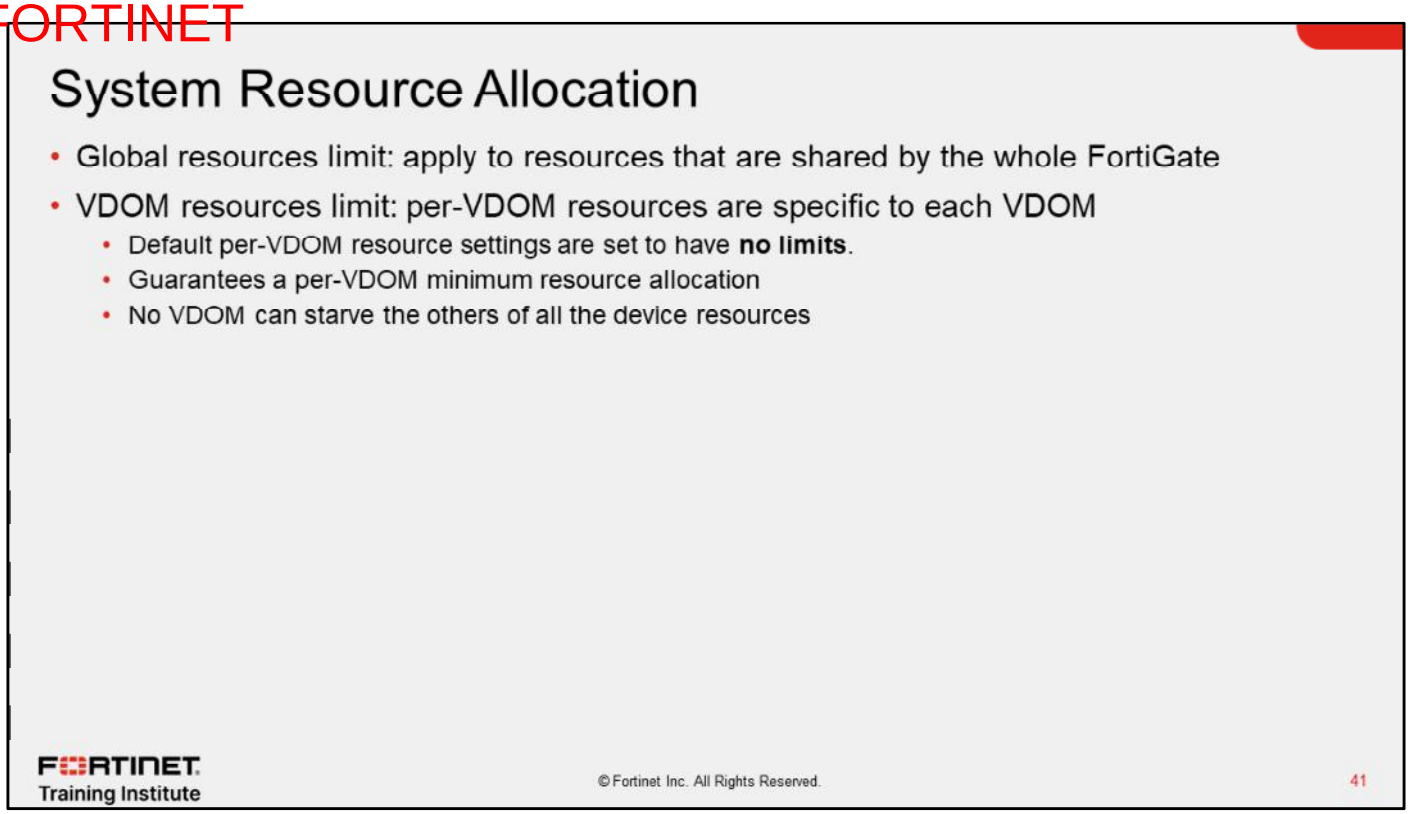
Good job! You now understand inter-VDOM Links.

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



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

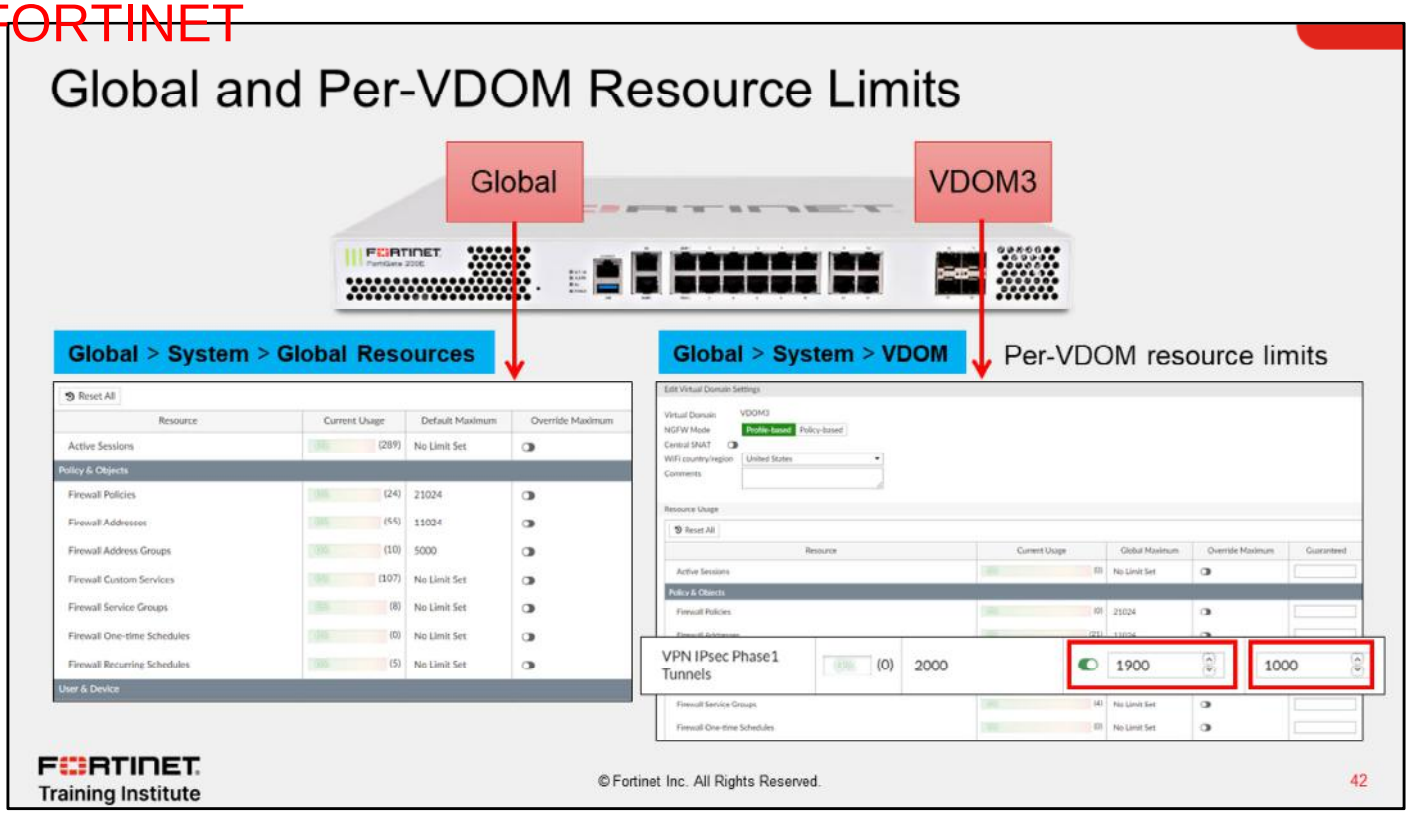
By demonstrating competence in VDOM best practices and troubleshooting, you will be able to prevent, identify, and solve common VDOM issues.



Remember, VDOMs are only a *logical* separation—each VDOM shares physical resources with the others.

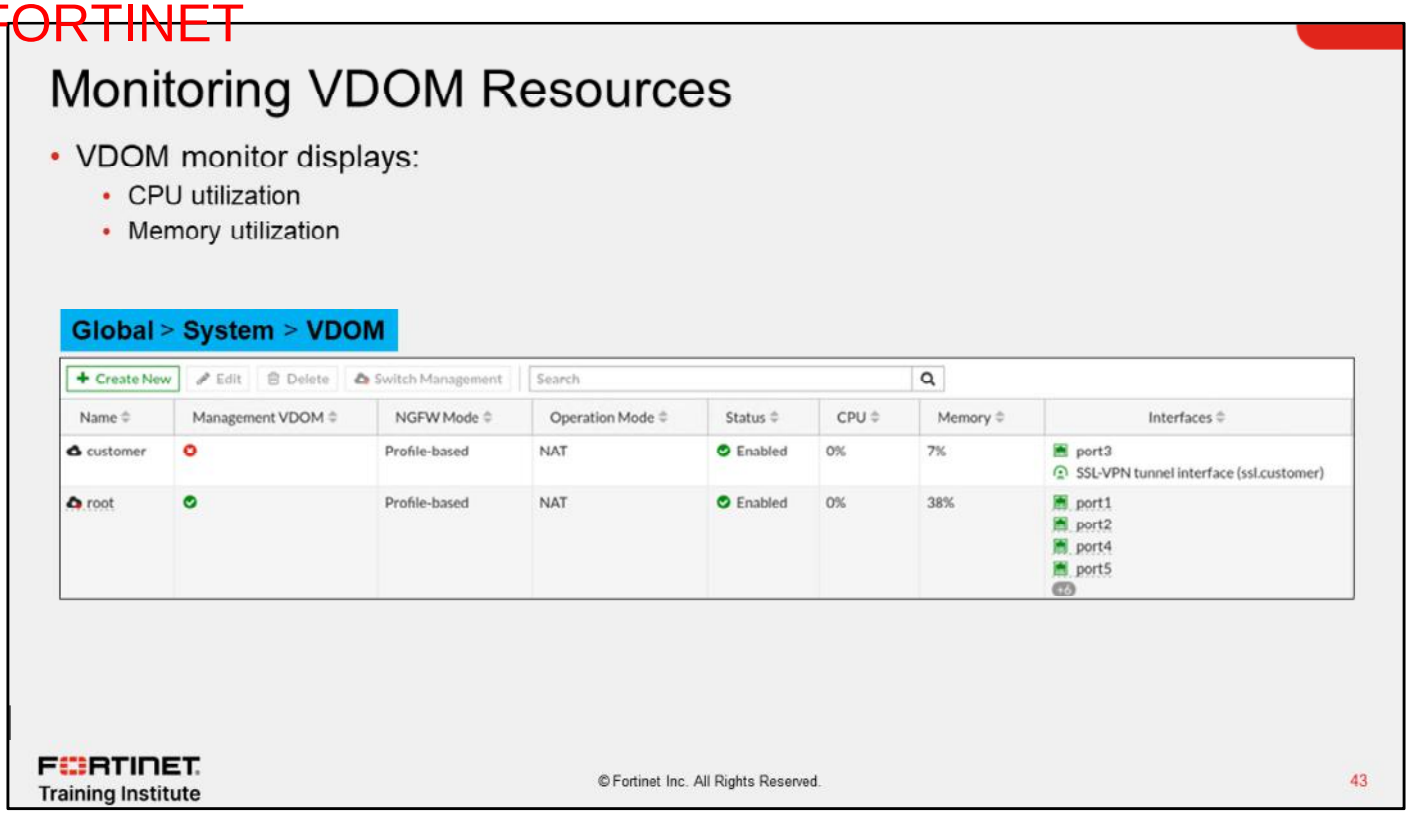
By default, all per-VDOM resource settings are set to have no limits. This means that any single VDOM can use all of the FortiGate device's resources. This could deprive other VDOMs of the resources that they require, to the point that could be unable to function.

Unlike FortiGate-VM, VDOMs are not allocated and balanced with weighted vCPU cores, vRAM, and other virtualized hardware.
To fine-tune performance, you can configure resource limits for each feature—IPsec tunnels, address objects, and so on—at the global level and at each VDOM level. This controls the ratio of the system resource usage of each VDOM to the total available resources.

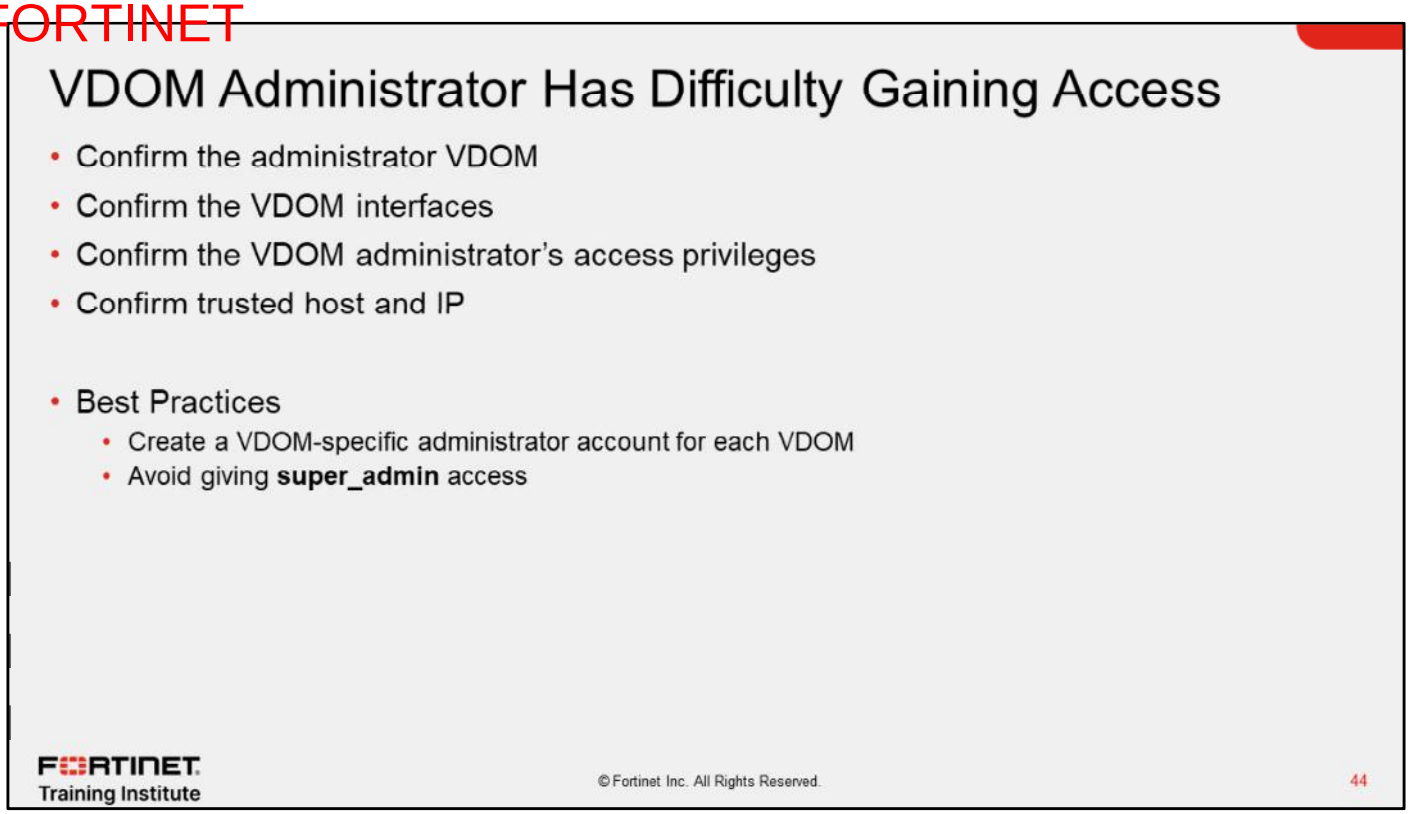


For example, a FortiGate with hardware powerful enough to handle up to 2000 IPsec VPN tunnels and configured with three VDOMs, could be configured as follows to meet specific criteria: VDOM1 and VDOM2 don't use IPsec VPN tunnels often. So, they are allowed to have up to 50 tunnels each. VDOM3, however, uses VPN extensively. Therefore, this FortiGate device is configured to allow VDOM3 to have up to 1900 tunnels, with 1000 guaranteed.

Configure your FortiGate device with global limits for critical features, such as sessions, policies, and so on. Then, configure each VDOM with its own quotas and minimums, within the global limits.



On the GUI, you can click **Global** > **System** > **VDOM** to see the VDOM monitor. It displays the CPU and memory usage for each VDOM.



With VDOMs configured, administrators have an extra layer of permissions and may have problems accessing the desired information. If an administrator cannot gain access, check the following:

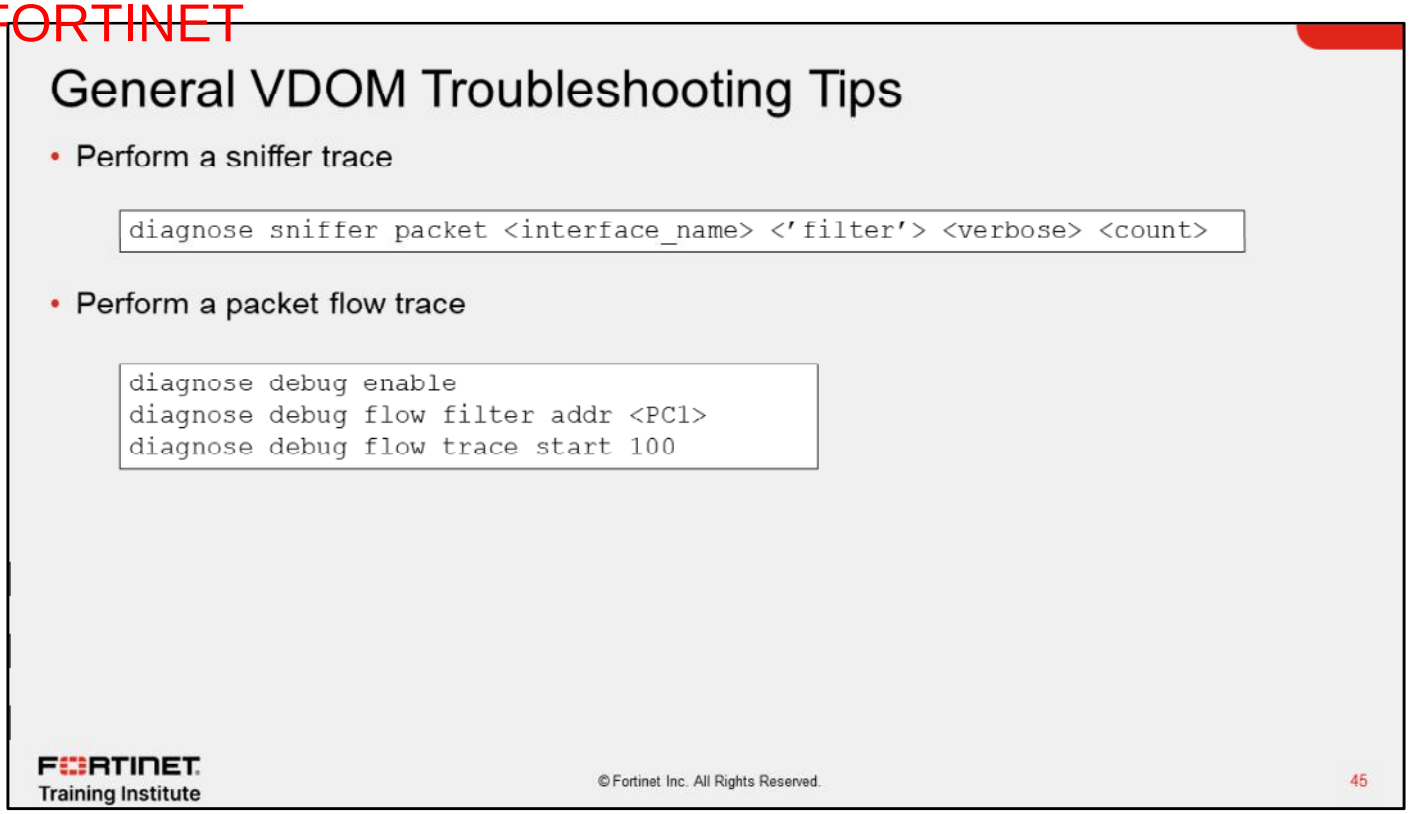
- Confirm the administrator's VDOM: each administrator account, other than the **super_admin** account, is tied to one or more specific VDOMs. That administrator is not able to access any other VDOM. It may be possible they are trying to access the wrong VDOM (one that they do not have permissions for).

- Confirm the VDOM interfaces: an administrator can access their VDOM only through interfaces that are assigned to that VDOM. If interfaces on that VDOM are disabled or unavailable, there will be no method of accessing that VDOM by its local administrator. The **super_admin** is required to either bring up the interfaces, fix the interfaces, or move another interface to that VDOM to restore access.

- Confirm the VDOM admin access: as with all FortiGate devices, administration access on the VDOM's interfaces must be enabled for the administrators of that VDOM to gain access. For example, if SSH is not enabled, that is not available to administrators. To enable admin access, the **super_admin** clicks **Global** > **Network** > **Interfaces** and enables administrator access for the interface in question.

- Confirm trusted host and IP: if trusted hosts are enabled on the administrator account, ensure the user is connecting from the correct, specified host address, and that no intermediate devices are performing NAT functions on the connection.

Best practice dictates that you should usually avoid unnecessary security holes. Do not provide **super_admin** access, if possible. Instead, restrict each administrator to their relevant domain. That way, they cannot accidentally or maliciously impact other VDOMs, and any damage or mistakes will be limited in scope.



Besides ping and traceroute, there are additional tools for troubleshooting your VDOM configurations. The primary tools for VDOM troubleshooting include packet sniffing and debugging the packet flow.

- Perform a sniffer trace: when troubleshooting networks, it helps to look inside the headers of packets to determine if they are traveling along the expected route. Packet sniffing can also be called a network tap, packet capture, or logic analyzing. The sniffer also indicates what traffic is entering or leaving the egress and ingress interfaces in all VDOMS. This makes it extremely useful for troubleshooting inter-VDOM routing issues.

- Debug the packet flow: traffic should enter and leave the VDOM. If you have identified that network traffic is not entering and leaving the VDOM as expected, debug the packet flow. You can debug only using CLI commands. This tool provides more granular details for help in troubleshooting inter-VDOM traffic because it gives details of routing selection, NAT, and policy selection.

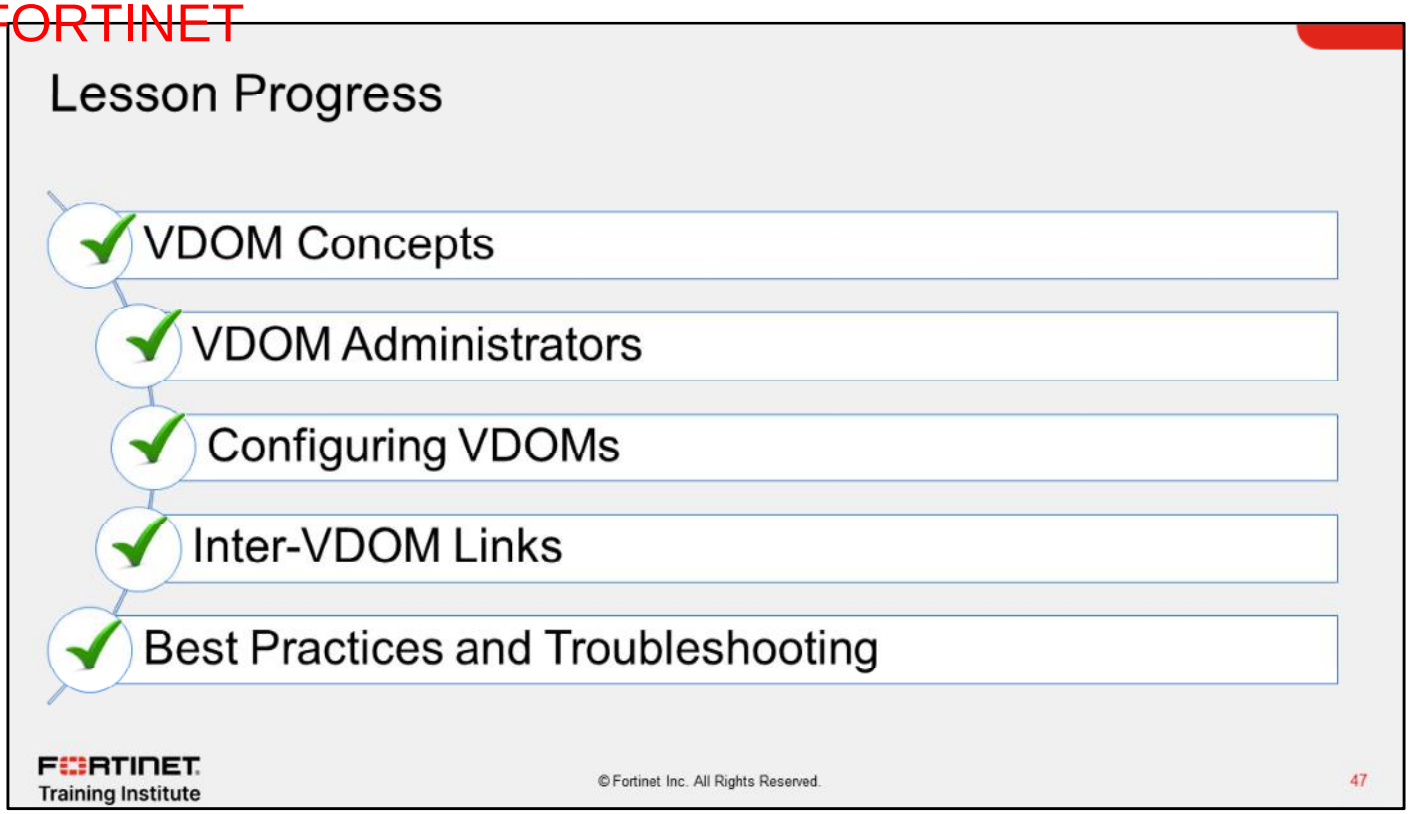
Knowledge Check

1. Of these options, what is a possible reason why an administrator might not be able to gain access to a specific VDOM?
   - ✓ A. The administrator is using an IP address that is not specified as a trusted host.
   - B. The administrator is using the super_admin profile.

2. Which troubleshooting tool is most suitable when trying to verify the firewall policy used by an inter-VDOM link?
   - A. Sniffer trace
   - ✓ B. Packet flow trace

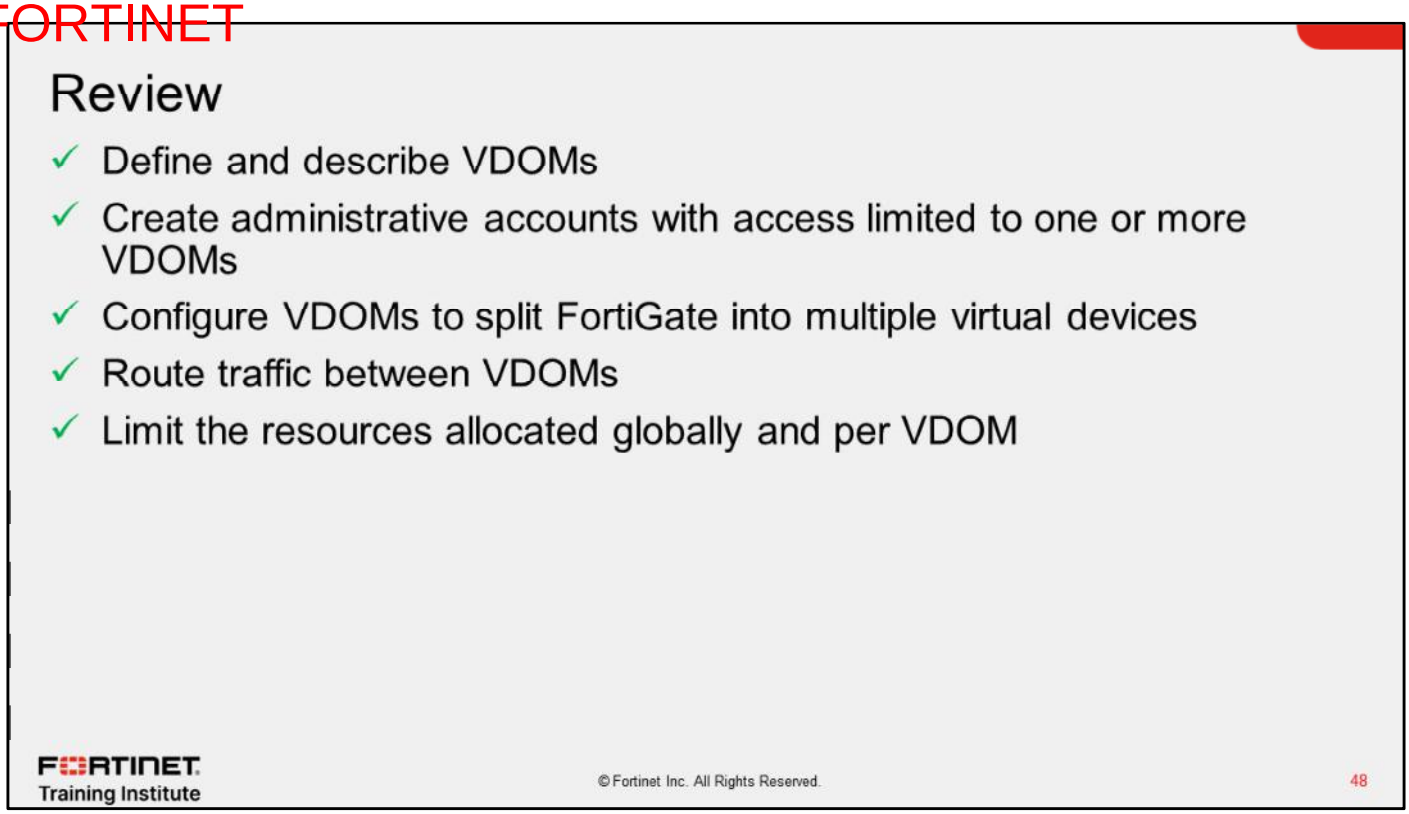
FORTINET Training Institute

46



Congratulations! You have completed this lesson.

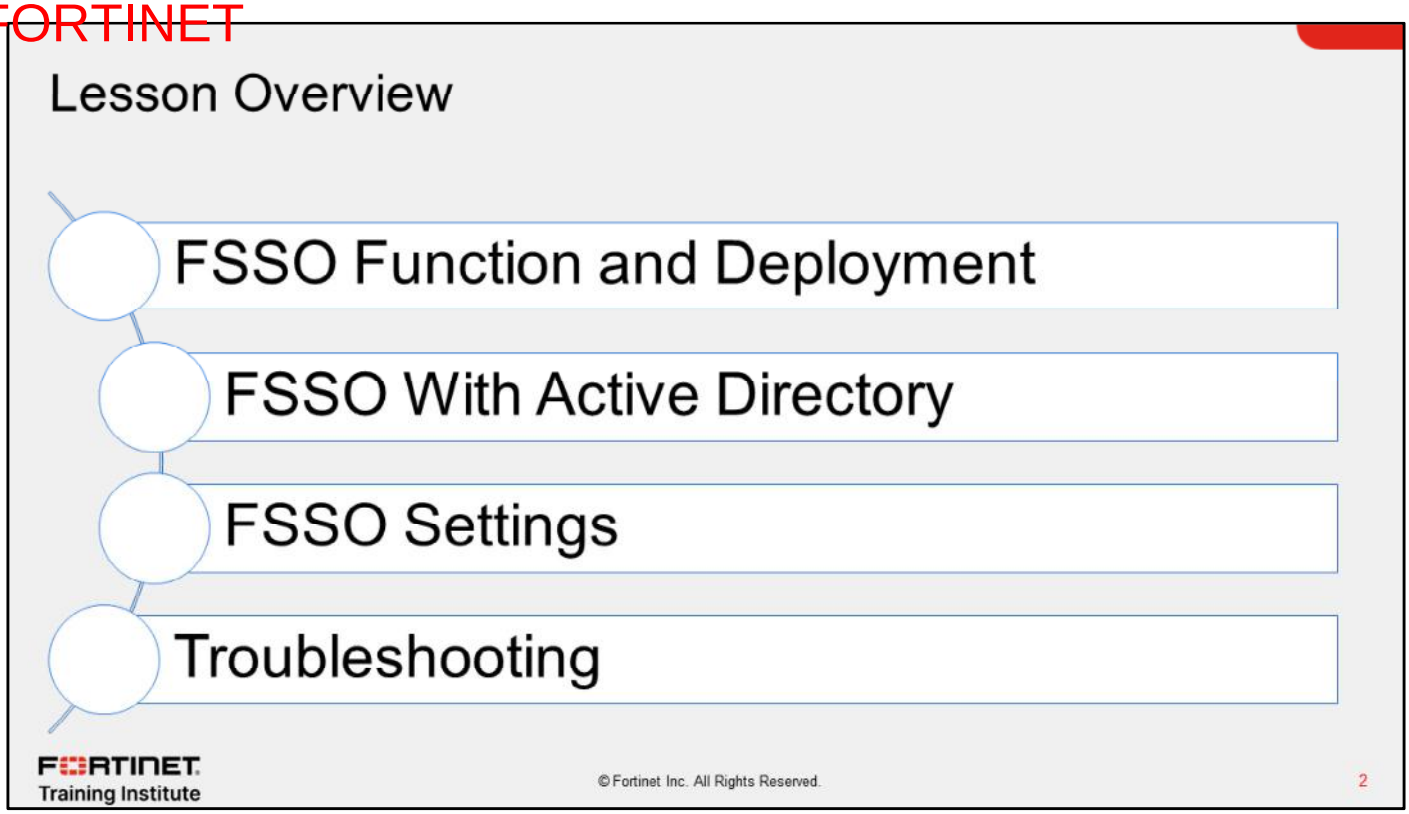
Now, you will review the objectives that you covered in this lesson.



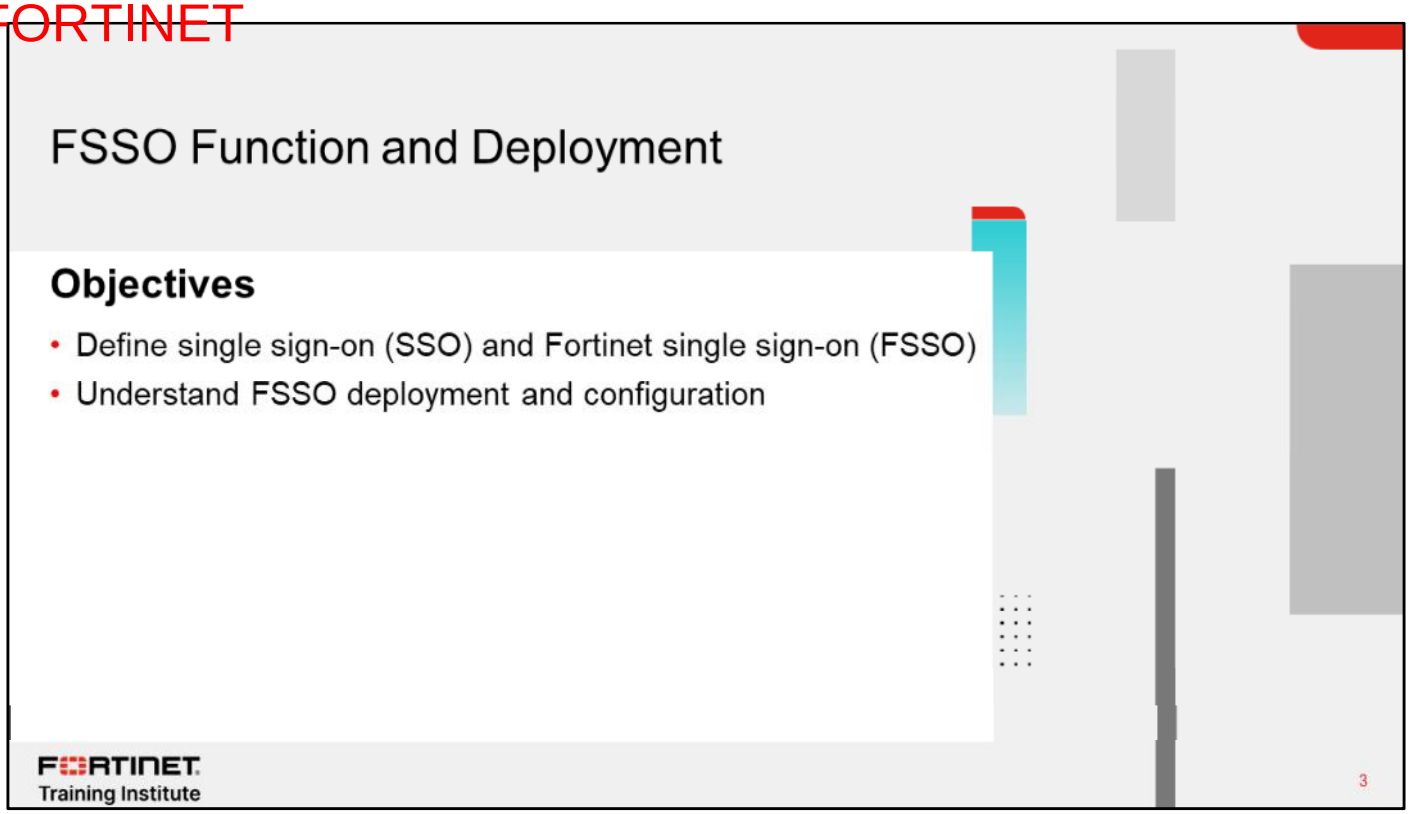
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure VDOMs, and examined examples of common use.

In this lesson, you will learn about Fortinet single sign-on (FSSO). When you use this feature, your users don't need to log on each time they access a different network resource.

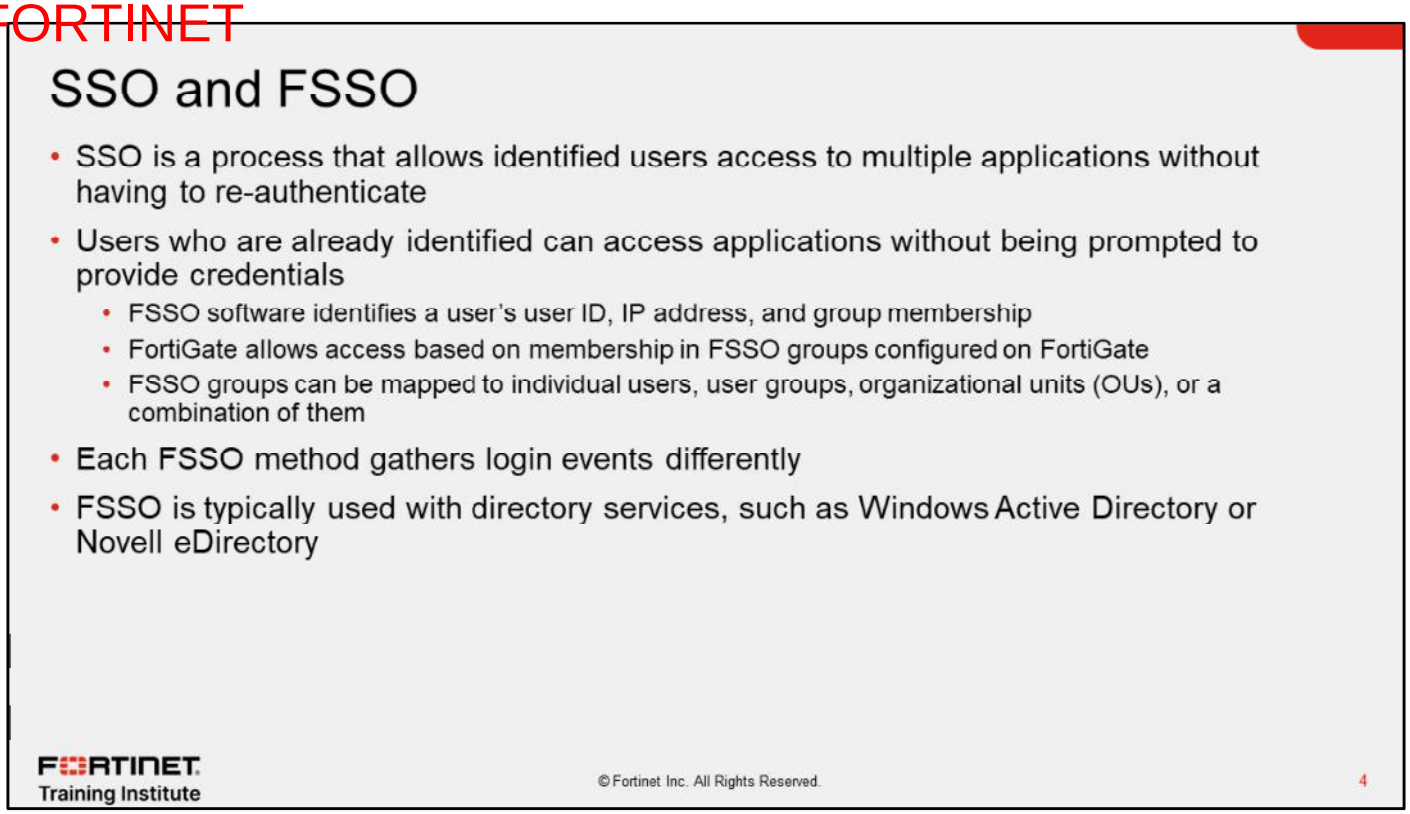


In this lesson, you will learn about the topics shown on this slide.



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

By demonstrating competence in understanding SSO concepts, you will be able to more effectively understand FSSO methods.

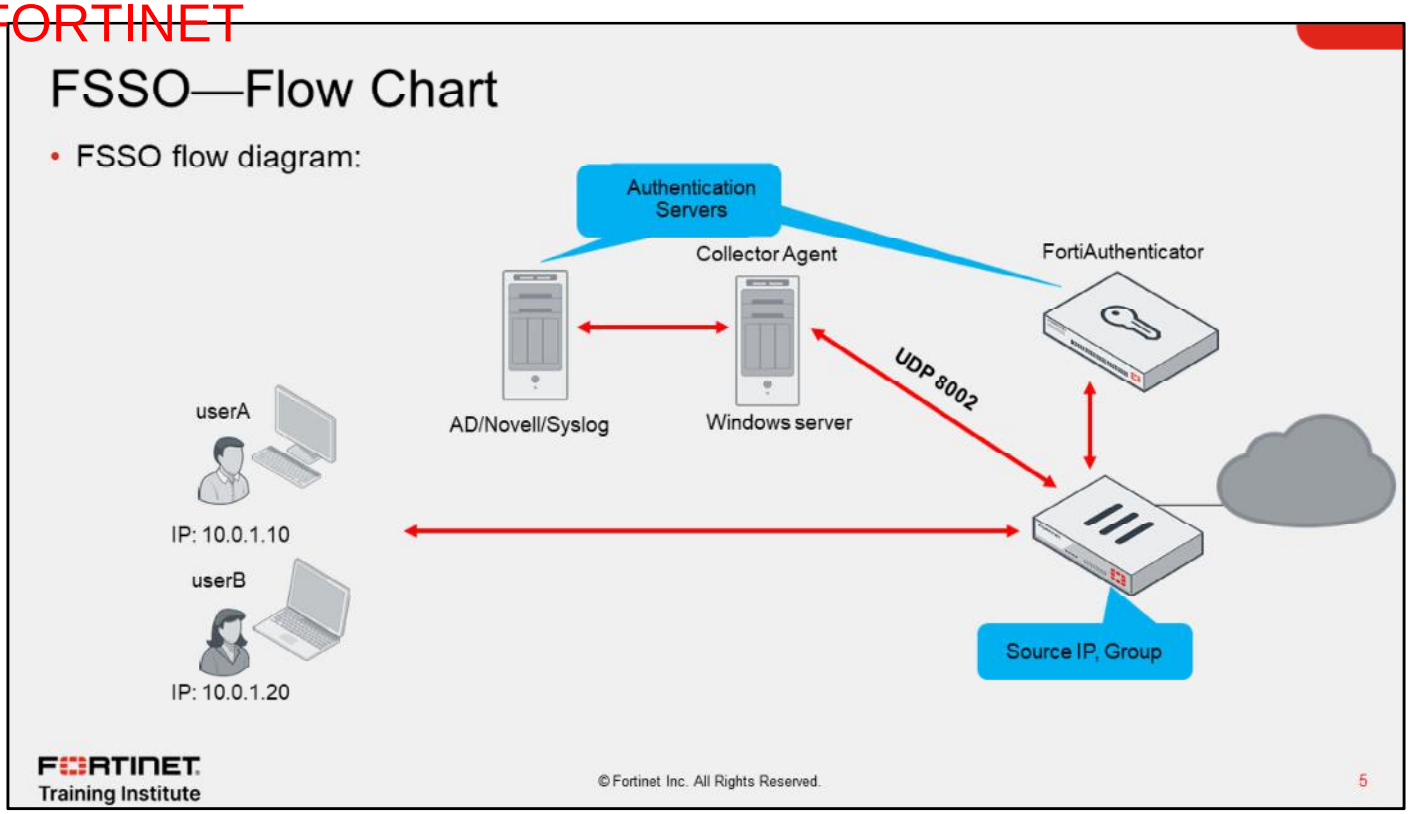


SSO is a process that allows users to be automatically logged in to every application after being identified, regardless of platform, technology, and domain.

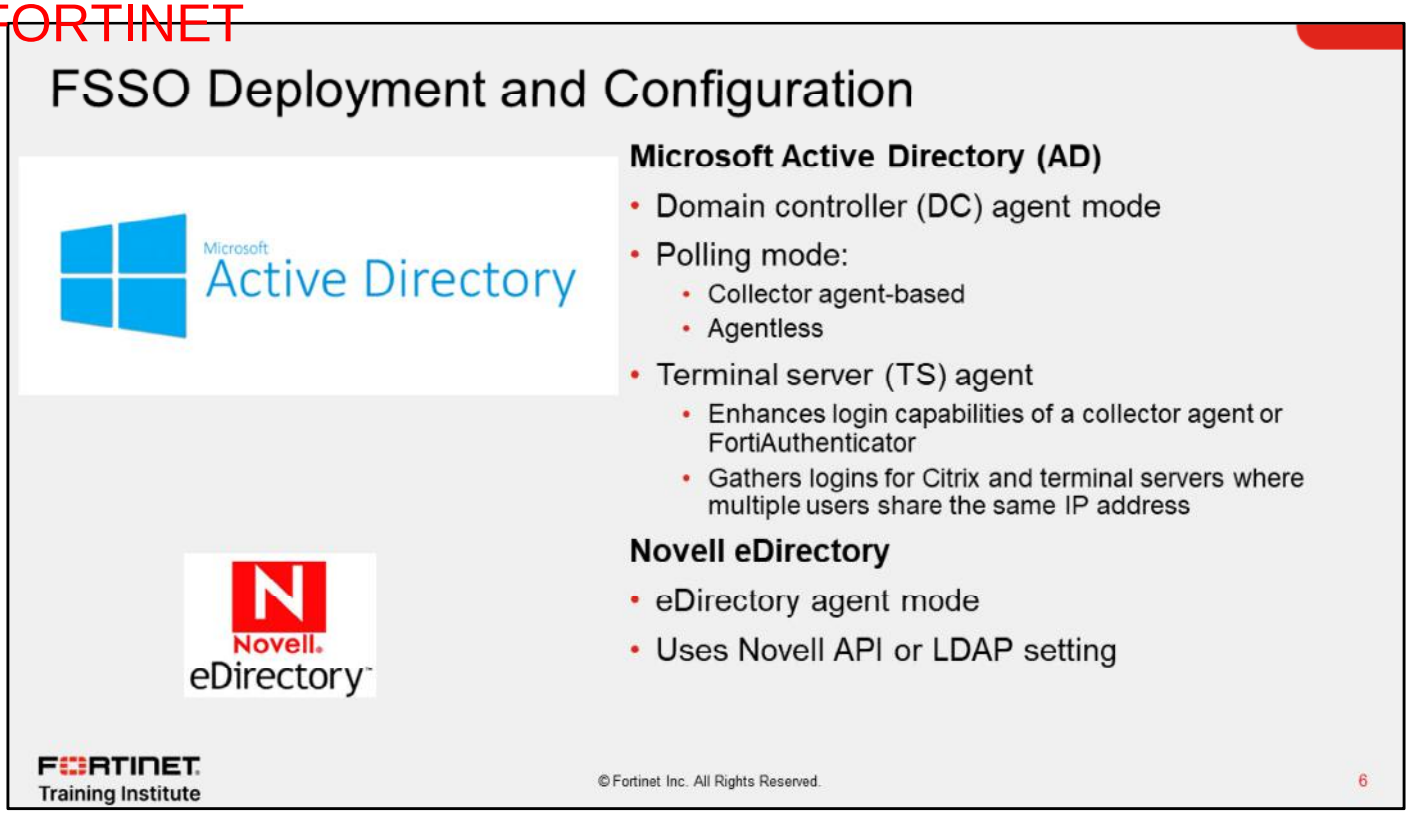
FSSO is a software agent that enables FortiGate to identify network users for security policies or for VPN access, in advanced deployments with FortiAuthenticator, without asking for their username and password. When a user logs in to a directory service, the FSSO agent sends FortiGate the username, the IP address, and the list of groups that the user belongs to. FortiGate uses this information to maintain a local database of usernames, IP addresses, and group mappings.

Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSSO is typically used with directory service networks such as Windows Active Directory or Novell eDirectory.



This slide shows the FSSO flow we discussed in the previous slide.

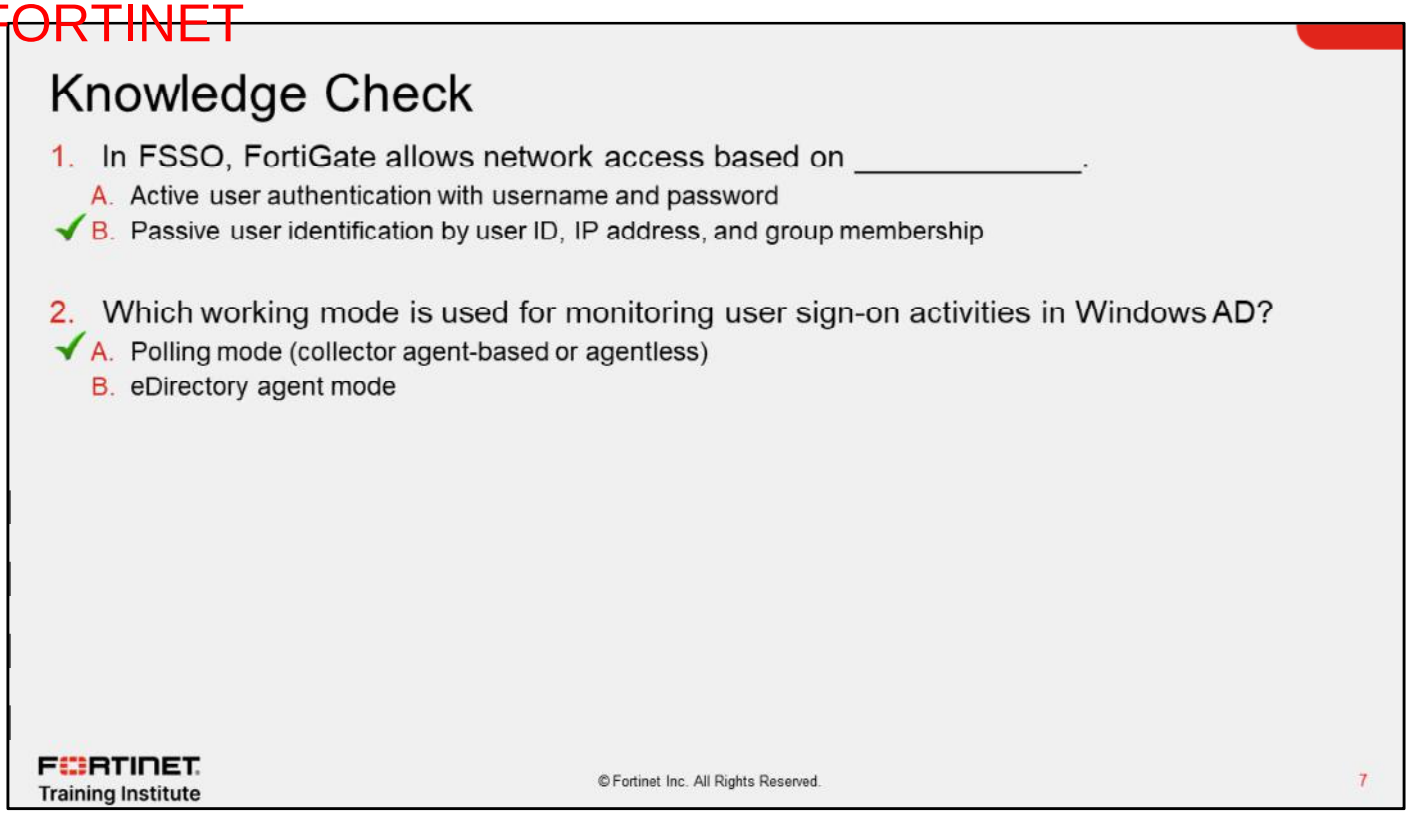


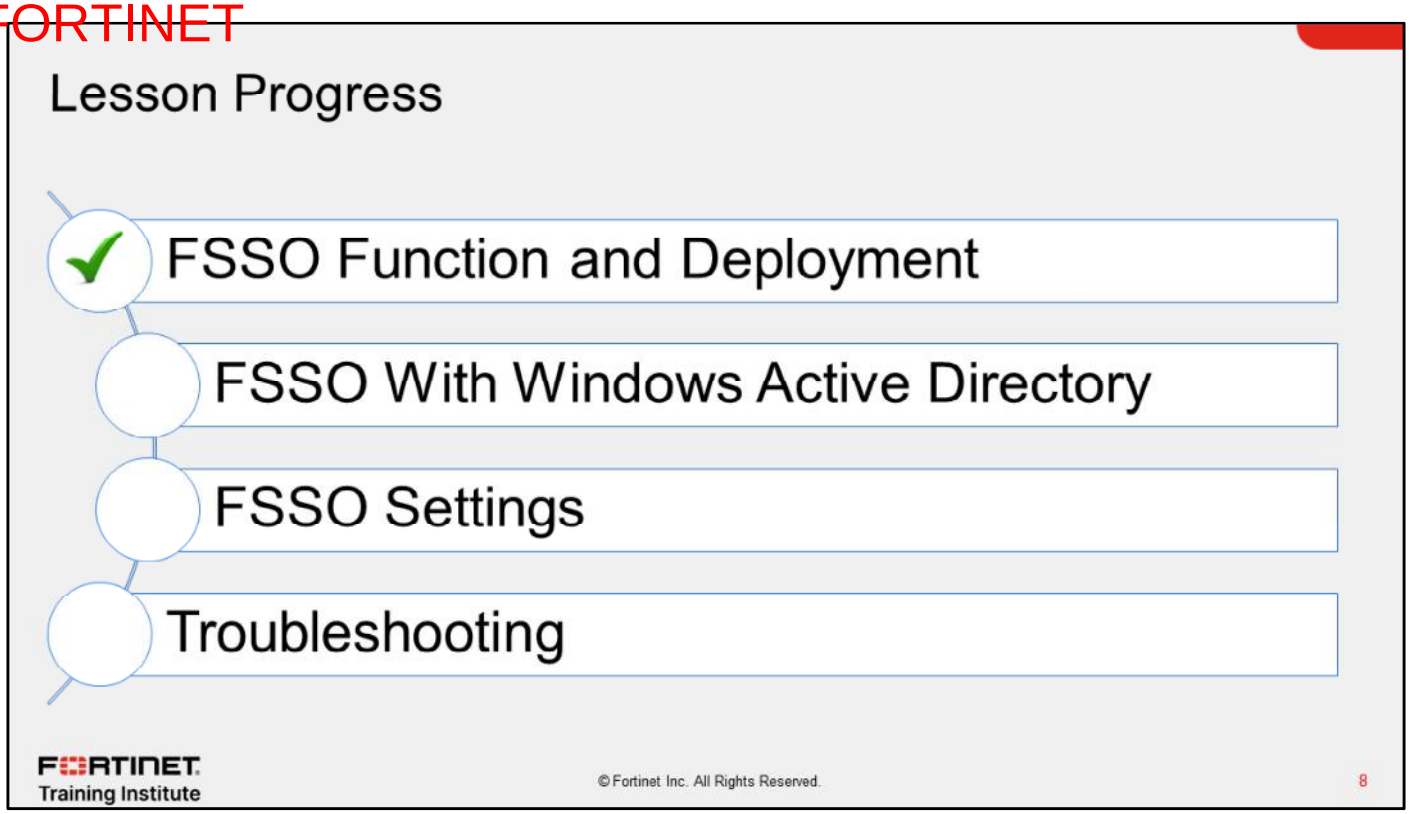
How you deploy and configure FSSO depends on the server that provides your directory services.

FSSO for Windows Active Directory (AD) uses a collector agent. Domain controller (DC) agents may also be required, depending on the collector agent working mode. There are two working modes that monitor user sign-on activities in Windows: DC agent mode and polling mode. FortiGate also offers a polling mode that does not require a collector agent, which is intended for simple networks with a minimal number of users.

There is another kind of DC agent that is used exclusively for Citrix and terminal services environments: terminal server (TS) agents. TS agents require the Windows Active Directory collector agent or FortiAuthenticator to collect and send the login events to FortiGate.

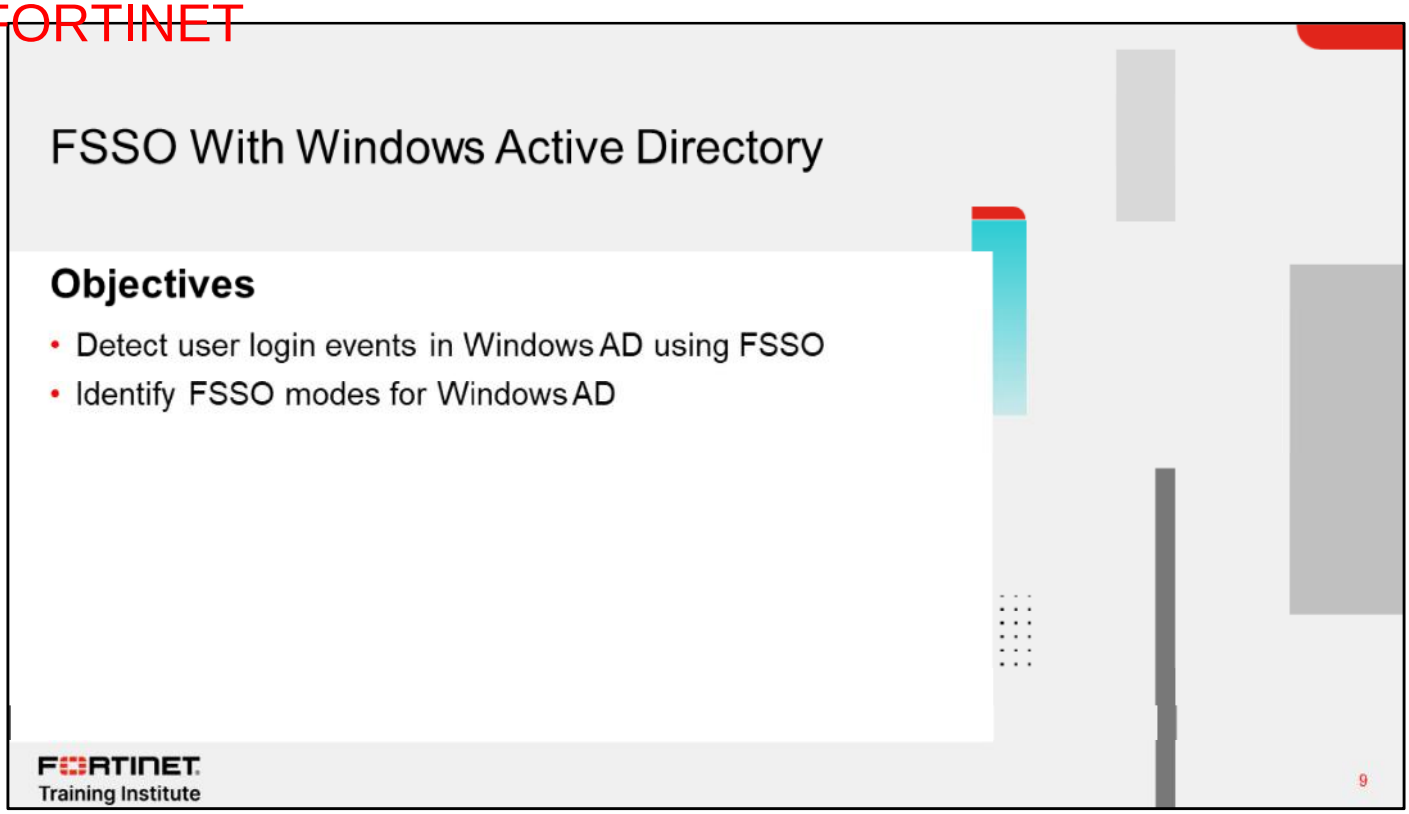
The eDirectory agent is installed on a Novell network to monitor user sign-ons and send the required information to FortiGate. It functions much like the collector agent on a Windows AD domain controller. The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.





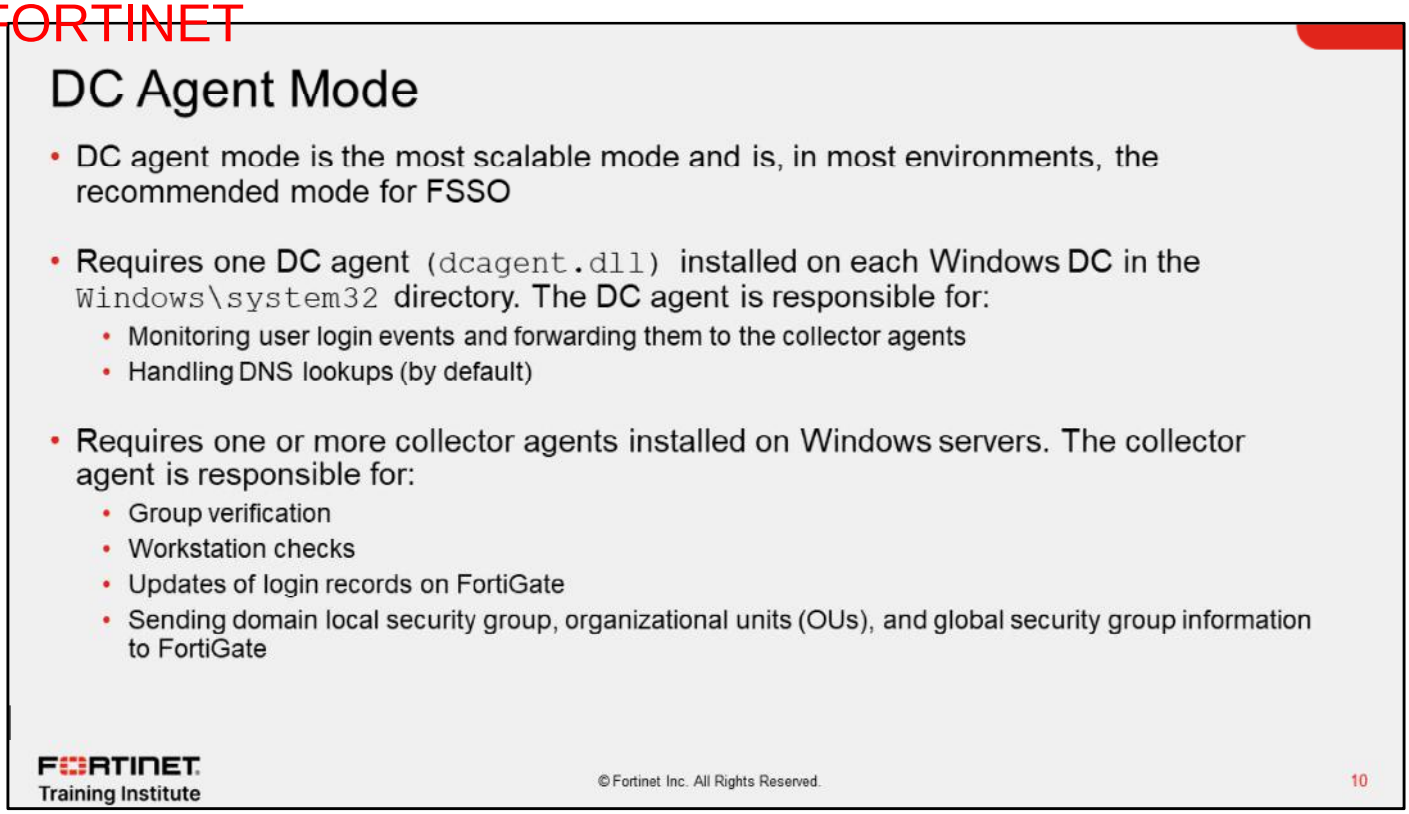
Good job! You now understand basic concepts about the function of FSSO and how it is deployed.

Now, you'll learn about user login events in Windows Active Directory using FSSO.



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

By demonstrating competence in understanding the different ways you can configure FSSO for Windows AD, you will be better able to design the architecture of your SSO system.



DC agent mode is considered the recommended mode for FSSO.

DC agent mode requires:

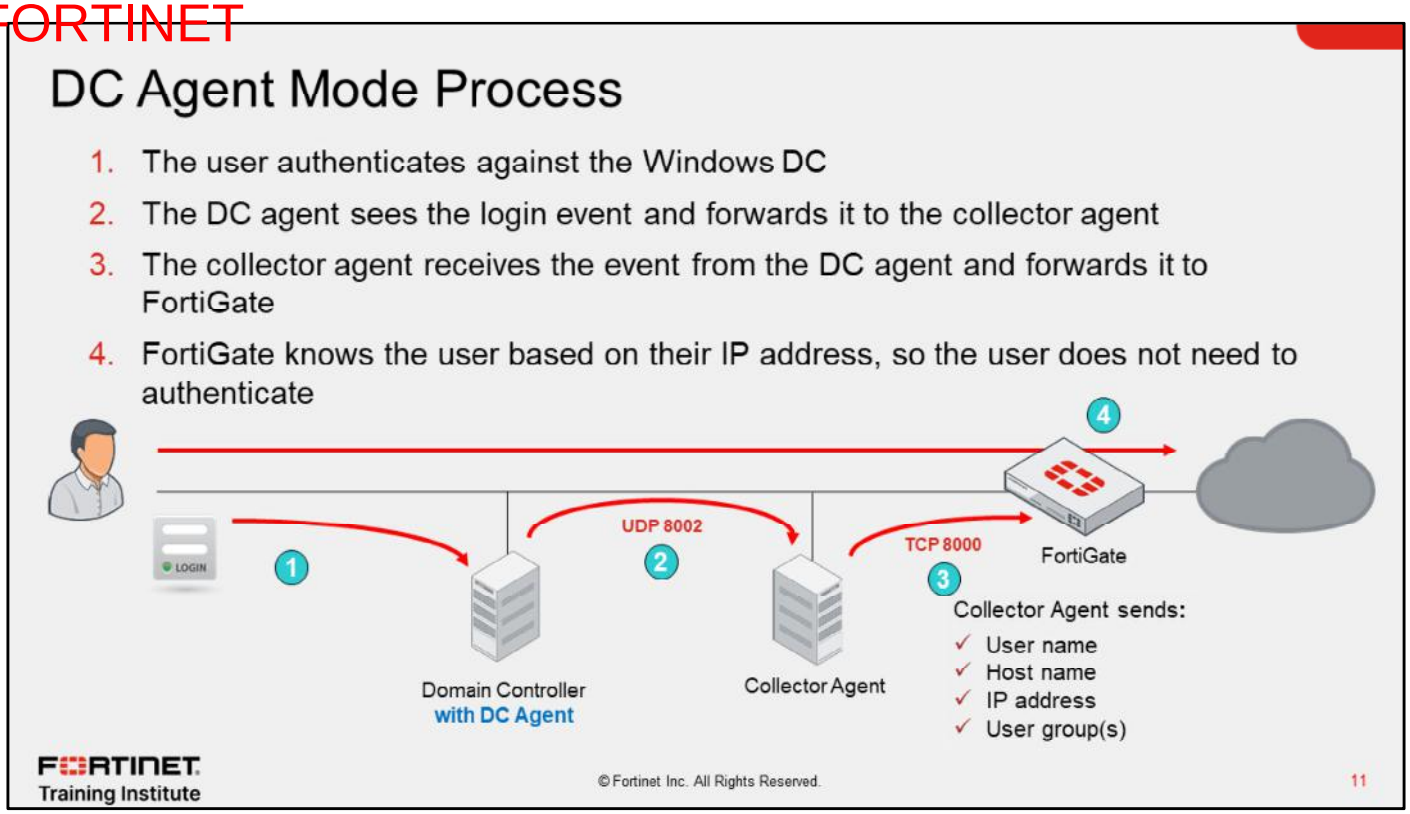
- One DC agent installed on each Windows DC
  If you have multiple DCs, this means that you need multiple DC agents. DC agents monitor and forward user login events to the collector agents.

- A collector agent, which is another FSSO component
  The collector agent is installed on a Windows server that is a member of the domain you are trying to monitor. It consolidates events received from the DC agents, then forwards them to FortiGate. The collector agent is responsible for group verification, workstation checks, and FortiGate updates of login records. The FSSO collector agent can send domain local security group, organizational units (OUs), and global security group information to FortiGate devices. It can also be customized for DNS lookups.

  When the user logs on, the DC agent intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

  The collector agent receives it and then performs a DNS resolution in order to check if the IP of the user has changed.

  In some configurations, double DNS resolution is a problem. In this case, you may configure a registry key on the domain controller that hosts the DC agent in order not to resolve the DNS:
  `donot_resolve = (DWORD) 1 at HKLM/Software/Fortinet/FSAE/dcagent`



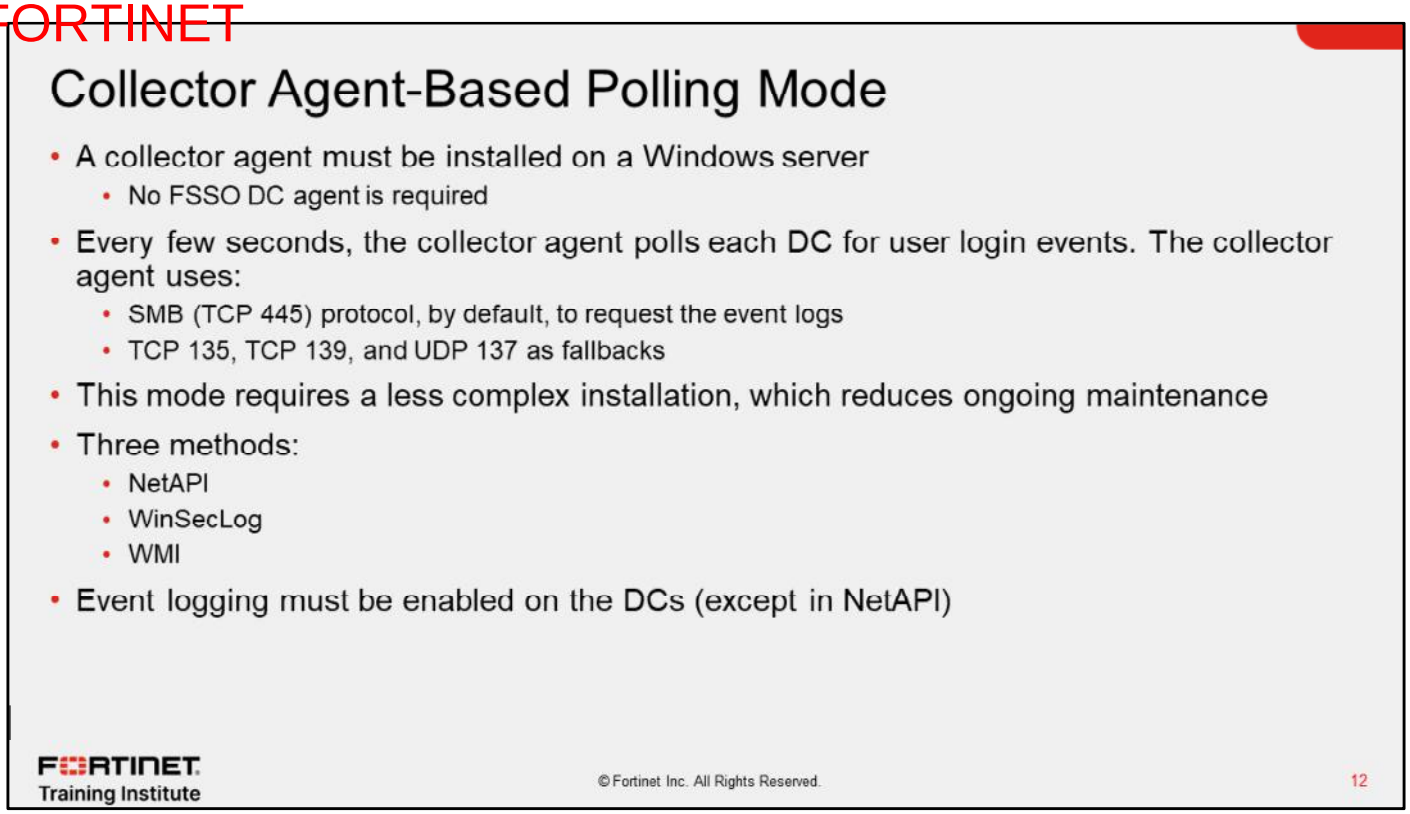
This slide shows the process of information passing between DC agents, the collector agent, and a FortiGate configured for FSSO authentication.

1. When users authenticate with the DC, they provide their credentials.

2. The DC agent sees the login event, and forwards it to the collector agent.

3. The collector agent aggregates all login events and forwards that information to FortiGate. The information sent by the collector agent contains the user name, host name, IP address, and user group(s). The collector agent communicates with FortiGate over TCP port 8000 (default) and it listens on UDP port 8002 (default), for updates from the DC agents. The ports are customizable.

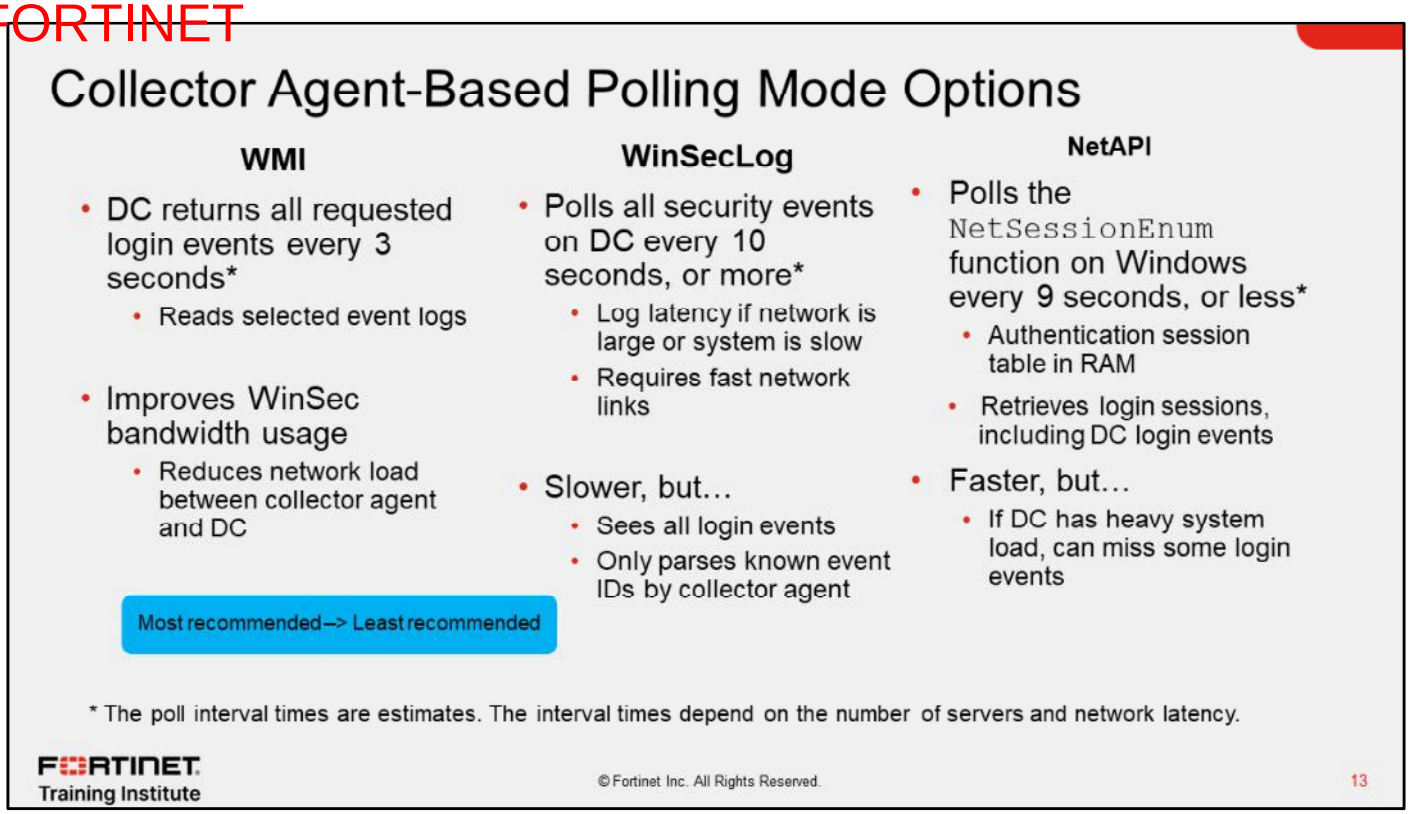
4. FortiGate learns from the collector agent who the user is, their IP address, and some of the AD groups that the user is a member of. When a user tries to access the internet, FortiGate compares the source IP address to its list of active FSSO users. Because the user in this case has already logged in to the domain, and FortiGate already has their information, FortiGate doesn't prompt the user to authenticate again. Rather it allows or denies the traffic based on the matching firewall policy.



Polling mode can be collector agent-based or agentless.

First, you'll look at the collector agent-based polling mode. Like DC agent mode, collector agent-based mode requires a collector agent to be installed on a Windows server, but it *doesn't* require DC agents to be installed on each DC. In collector agent-based polling mode, the collector agent must be more powerful than the collector agent in DC agent mode, and it also generates unnecessary traffic when there have been no login events.

In Windows Event Log Polling, the most commonly deployed polling mode, the collector agent uses the SMB (TCP port 445) protocol to periodically request event logs from the domain controllers. Other methods may gather information differently, but after the login is received by the collector agent, the collector agent parses the data and builds the user login database, which consists of usernames, workstation names/IP addresses, and user group memberships. This information is then ready to be sent to FortiGate.

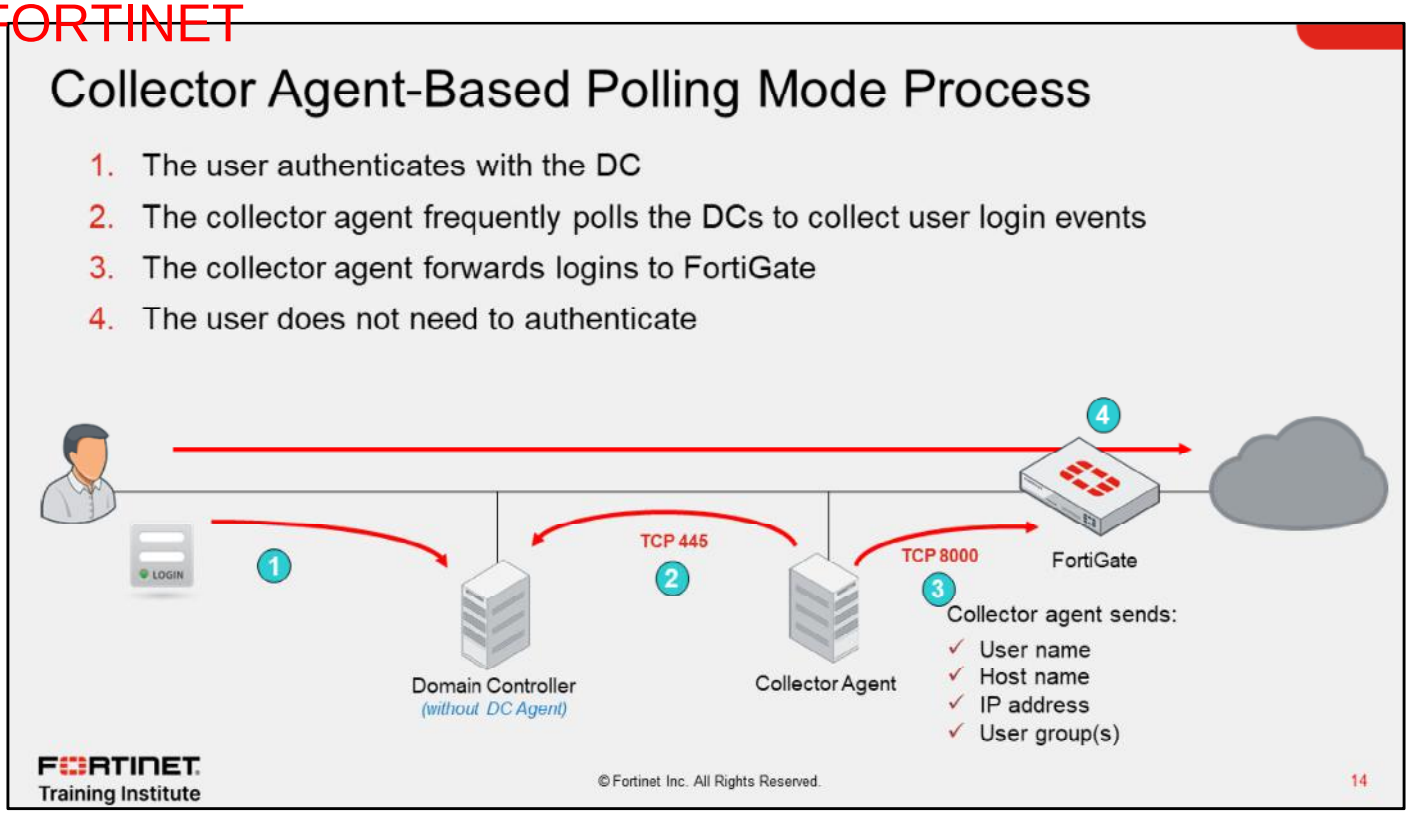


As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **WMI**: is a Windows API that gets system information from a Windows server. The DC returns all requested login events. The collector agent is a WMI client and sends WMI queries for user login events to the DC, which, in this case, is a WMI server. The collector agent doesn't need to search security event logs on the DC for user login events; instead, the DC returns all requested login events. This reduces network load between the collector agent and DC.

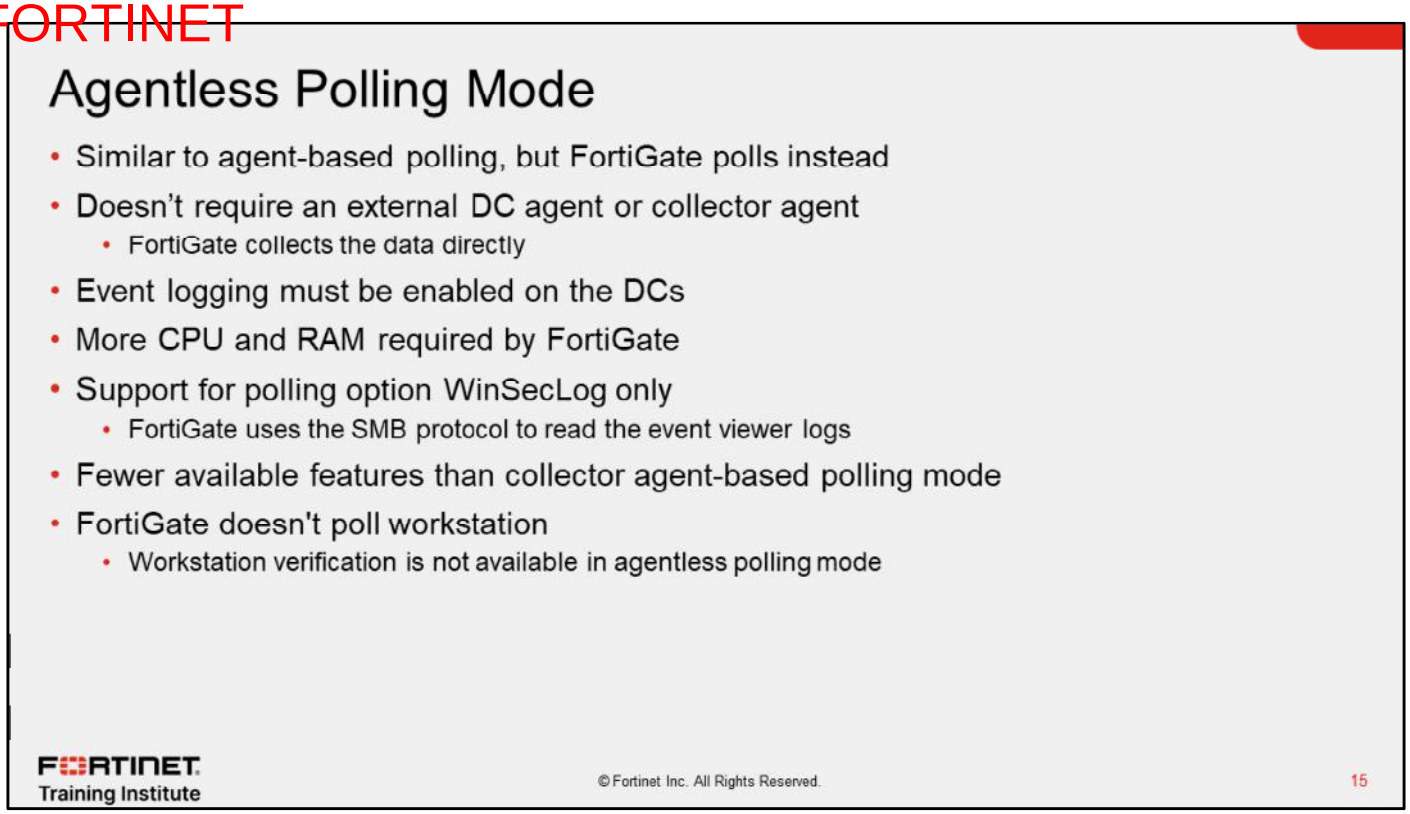
- **WinSecLog**: polls all the security event logs from the DC. It doesn't miss any login events that have been recorded by the DC because events are not normally deleted from the logs. There can be some delay in FortiGate receiving events if the network is large and, therefore, writing to the logs is slow. It also requires that the audit success of specific event IDs is recorded in the Windows security logs. For a full list of supported event IDs, visit the Fortinet Knowledge Base (http://kb.fortinet.com).

- **NetAPI**: polls temporary sessions created on the DC when a user logs in or logs out and calls the `NetSessionEnum` function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some login events if a DC is under heavy system load. This is because sessions can be quickly created and purged from RAM, before the agent has a chance to poll and notify FortiGate.



This slide shows an example of FSSO using the collector agent-based polling mode. This example includes a DC, a collector agent, and FortiGate, but the DC doesn't have the dcagent (or, alternatively, dcagent.dll) installed.

1. The user authenticates with the DC, providing their credentials.
2. The collector agent periodically (every few seconds) polls TCP port 445 of each DC directly, to ask if anyone has logged in.
3. The collector agent sends login information to FortiGate over TCP port 8000. This is the same information that is sent in DC agent mode.
4. When user traffic arrives at FortiGate, FortiGate already knows which users are at which IP addresses, and no repeated authentication is required.

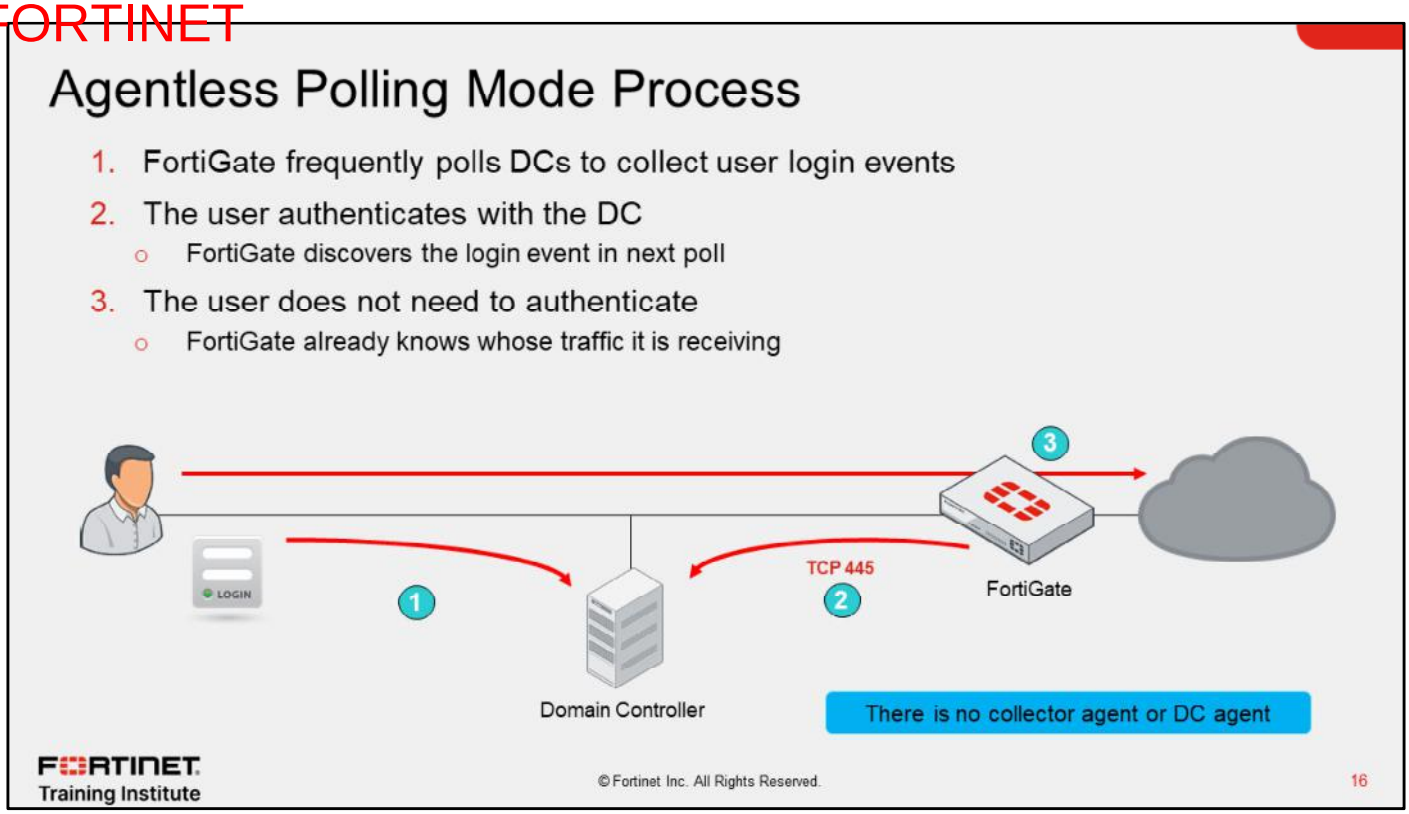


You can deploy FSSO without installing an agent. FortiGate polls the DCs directly, instead of receiving login information indirectly from a collector agent.

Because FortiGate collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

In agentless polling mode, FortiGate acts as a collector. It is responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

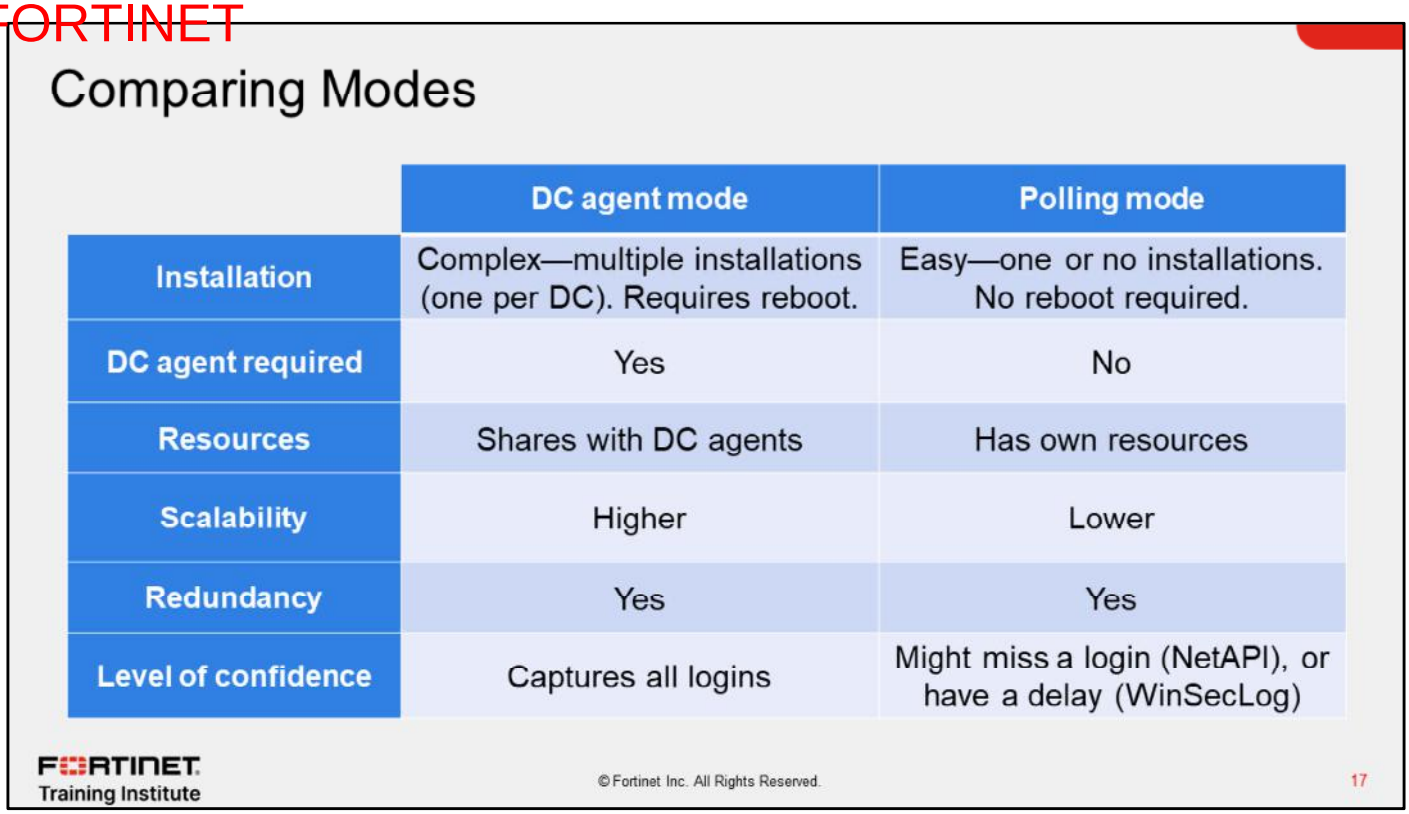


This slide shows how communication is processed without agents. (There is no collector agent or DC agent.)

1. FortiGate polls the DC TCP port 445 to collect user login events.

2. After the user authenticates with the DC, FortiGate registers a login event during its next poll, obtaining the following information: the user name, the host name, and the IP address. FortiGate then queries for the user's user group(s).

3. When the user sends traffic, FortiGate already knows whose traffic it is receiving; therefore, the user does not need to authenticate.



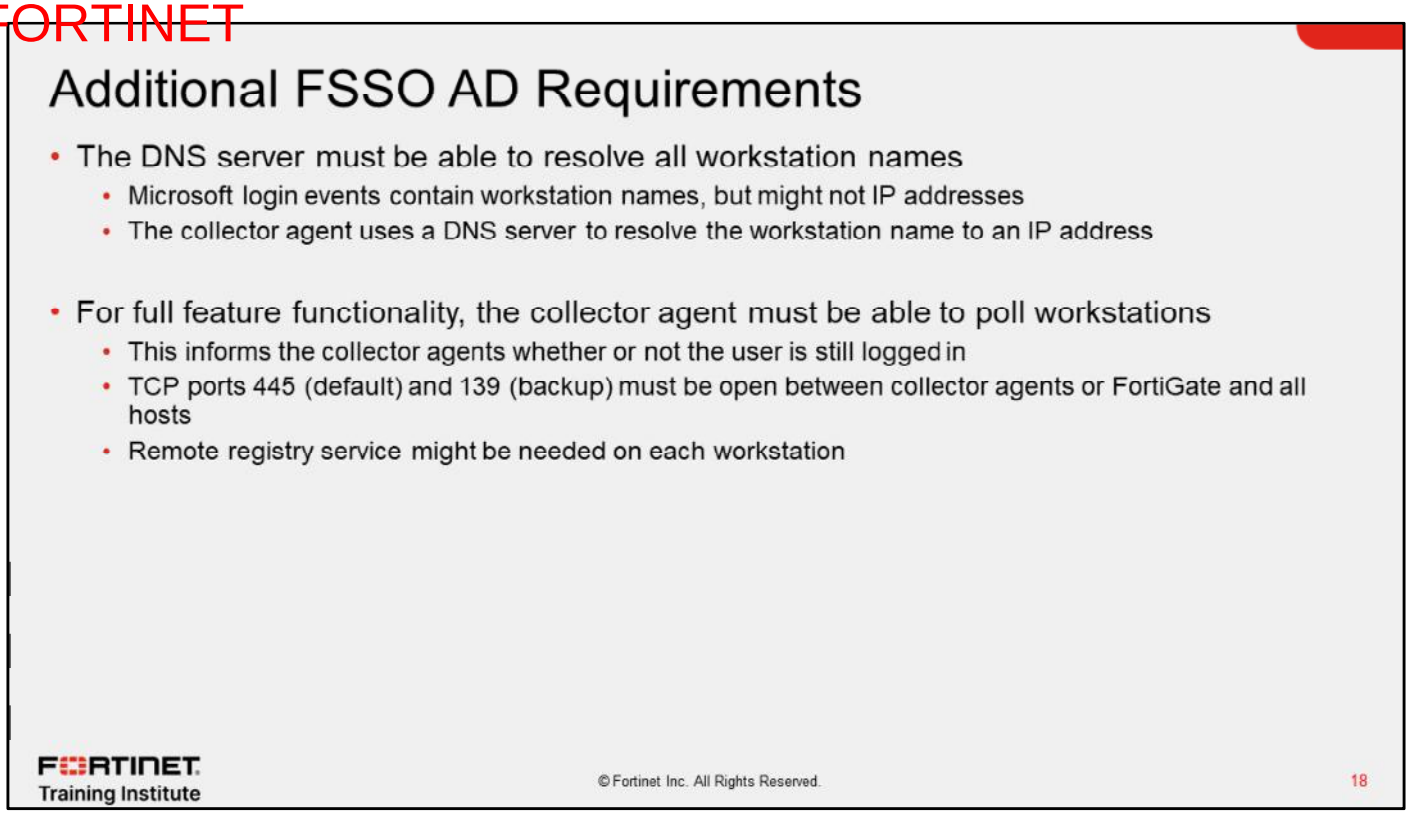
This table summarizes the main differences between DC agent mode and polling mode.

DC agent mode is more complex. It requires not only a collector agent, but also a DC agent for each monitored domain controller. However, it is also more scalable because the work of capturing logins is done by the DC agents who pass their information directly to the collector.

In polling mode, the collector needs to query every domain controller, every few seconds. So, with each DC that is added, the number of queries grows. If you want to add a second collector agent for redundancy in polling mode, both collector agents need to query every DC individually.

In DC agent mode, the DC agent just has to collect the log once, and send a copy of the necessary information to all the collector agents. In comparison, if you use polling mode, some login events might be missed or delayed, depending on the polling option used.

You do not have to install a collector agent on the DC, you can install it on any Windows machine on the network.



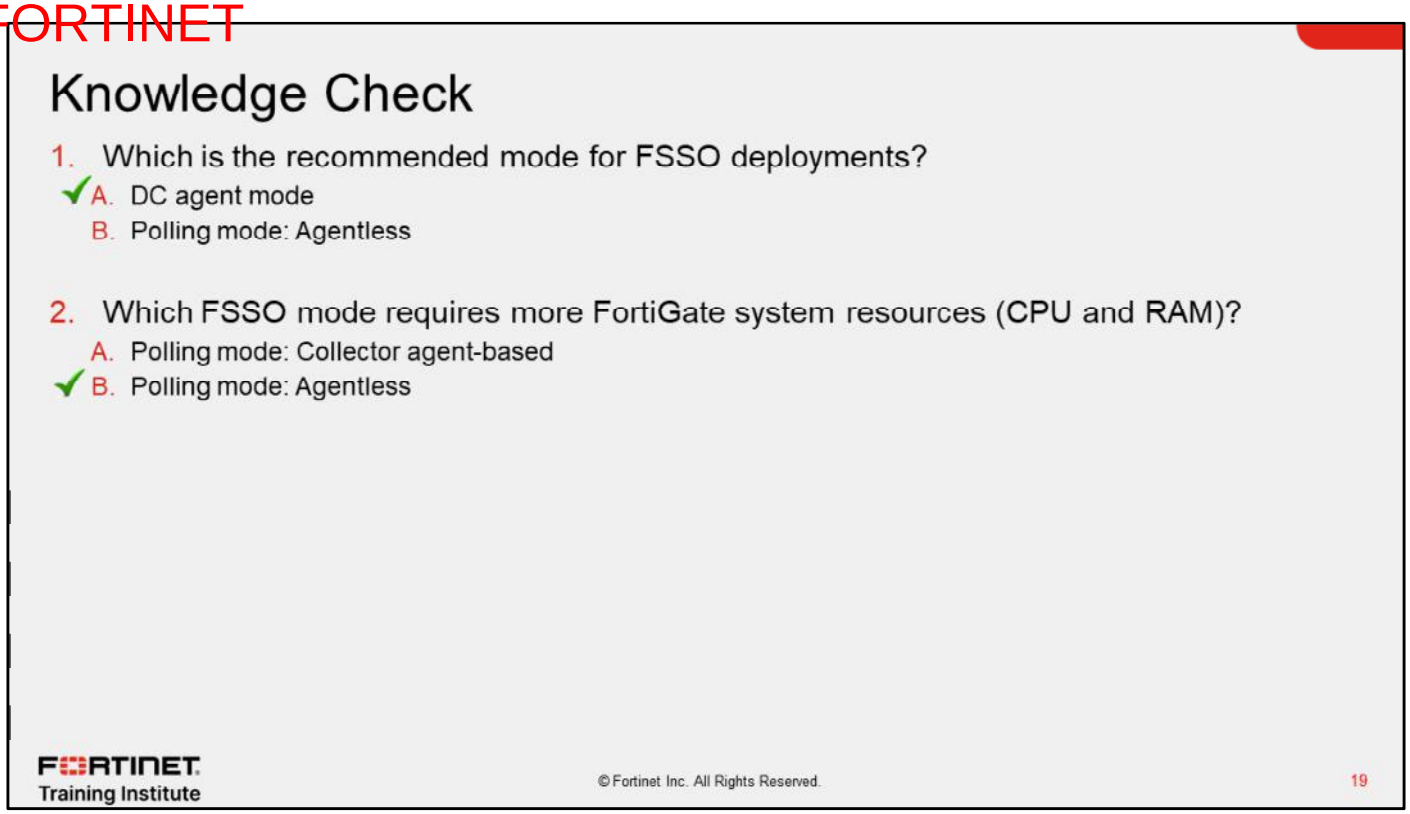
Regardless of the collector method you choose, some FSSO requirements for your AD network are the same:

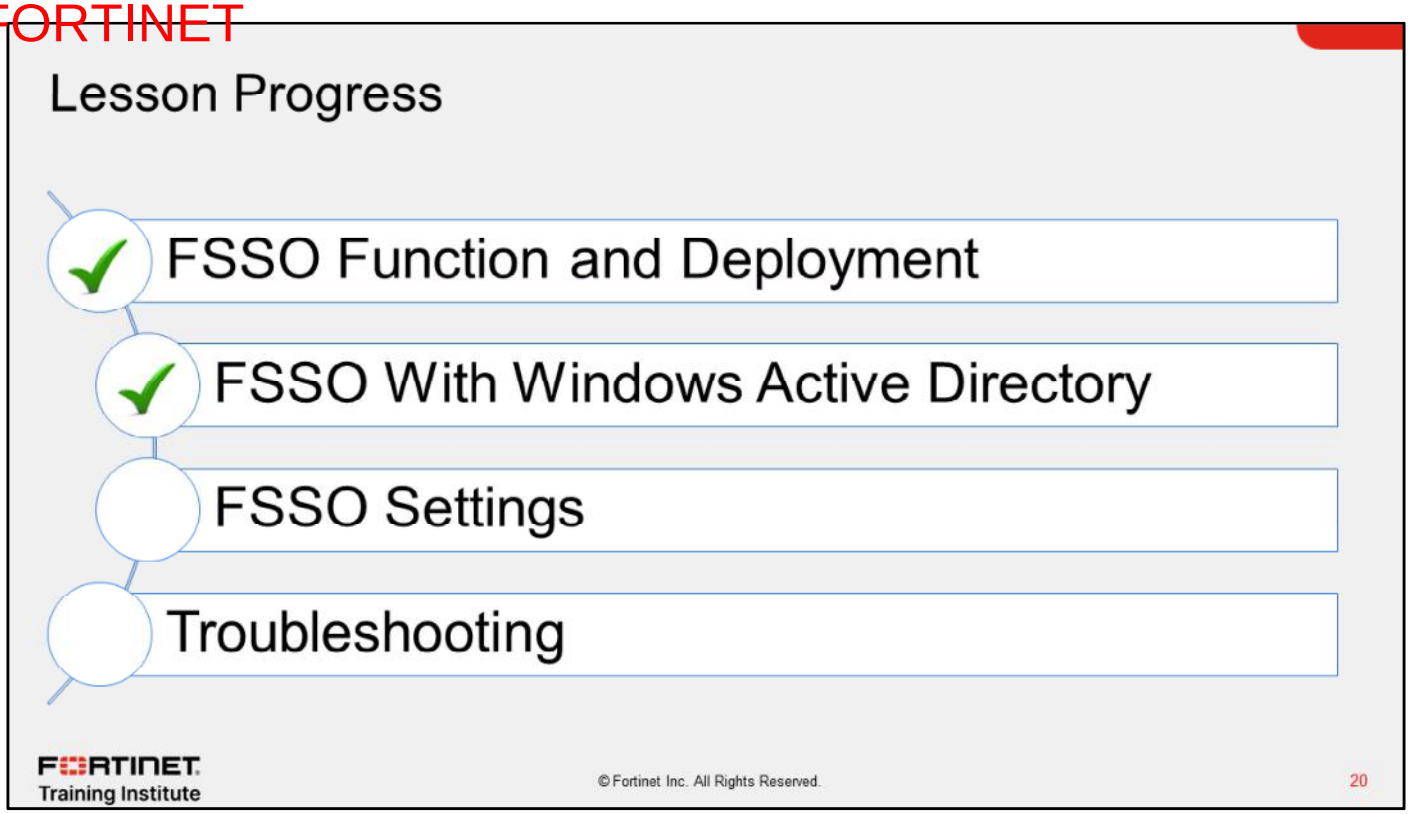
- Microsoft Windows login events have the workstation name and username, but not the workstation IP address. When the collector agent receives a login event, it queries a DNS server to resolve the IP address of the workstation. So, FSSO requires that you have your own DNS server. If a workstation IP address changes, DNS records must be updated immediately in order for the collector agent to be aware of the change and report them to FortiGate.

- For full feature functionality, collector agents need connectivity with all workstations. Since a monitored event log is not generated on logout, the collector agent (depending on the FSSO mode) must use a different method to verify whether users are still logged in. So, each user workstation is polled to see if users are still there.

- The DC agent, when the user logs in, intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

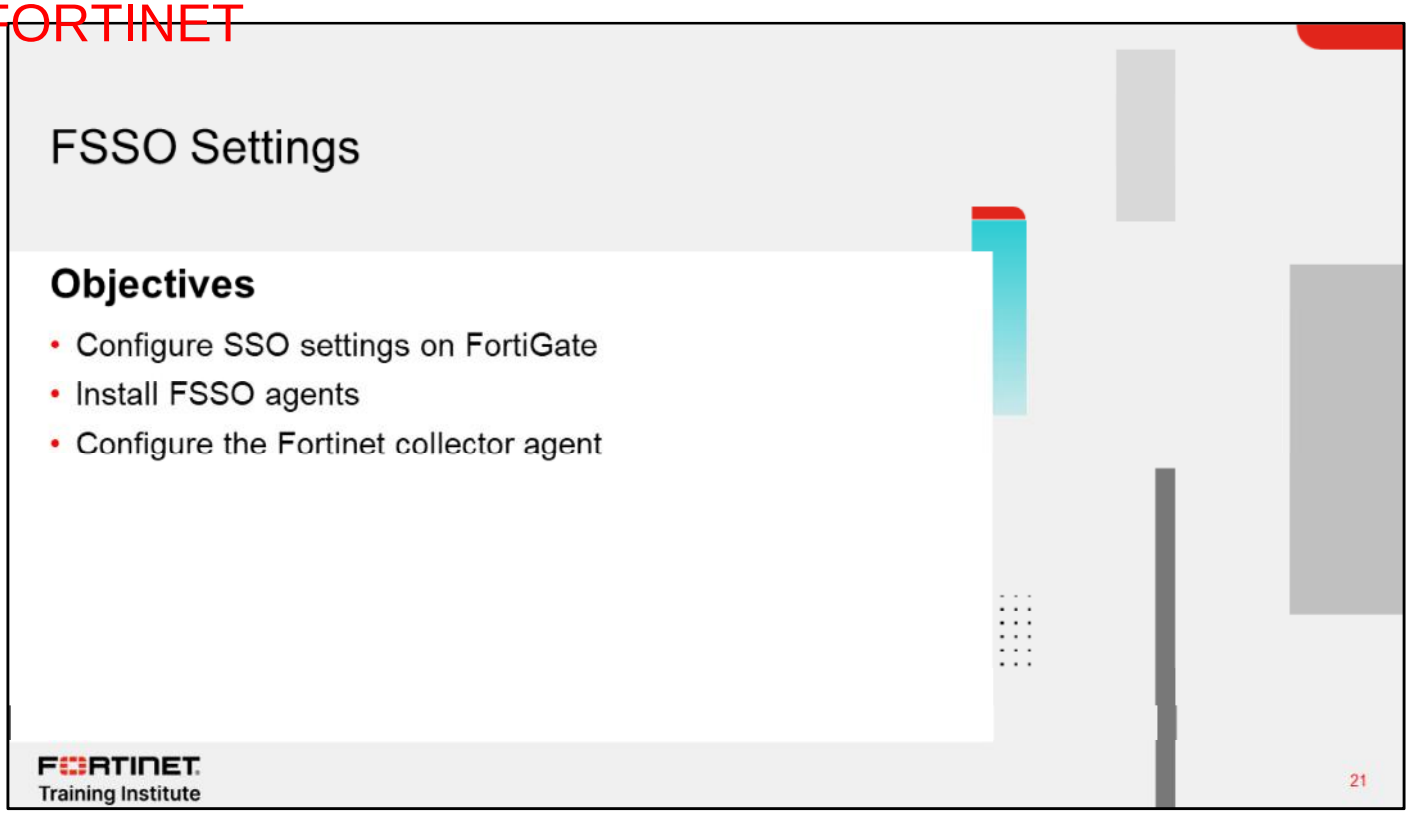
  The collector agent receives the DNS and then performs a DNS resolution in order to check if the IP of the user has changed.





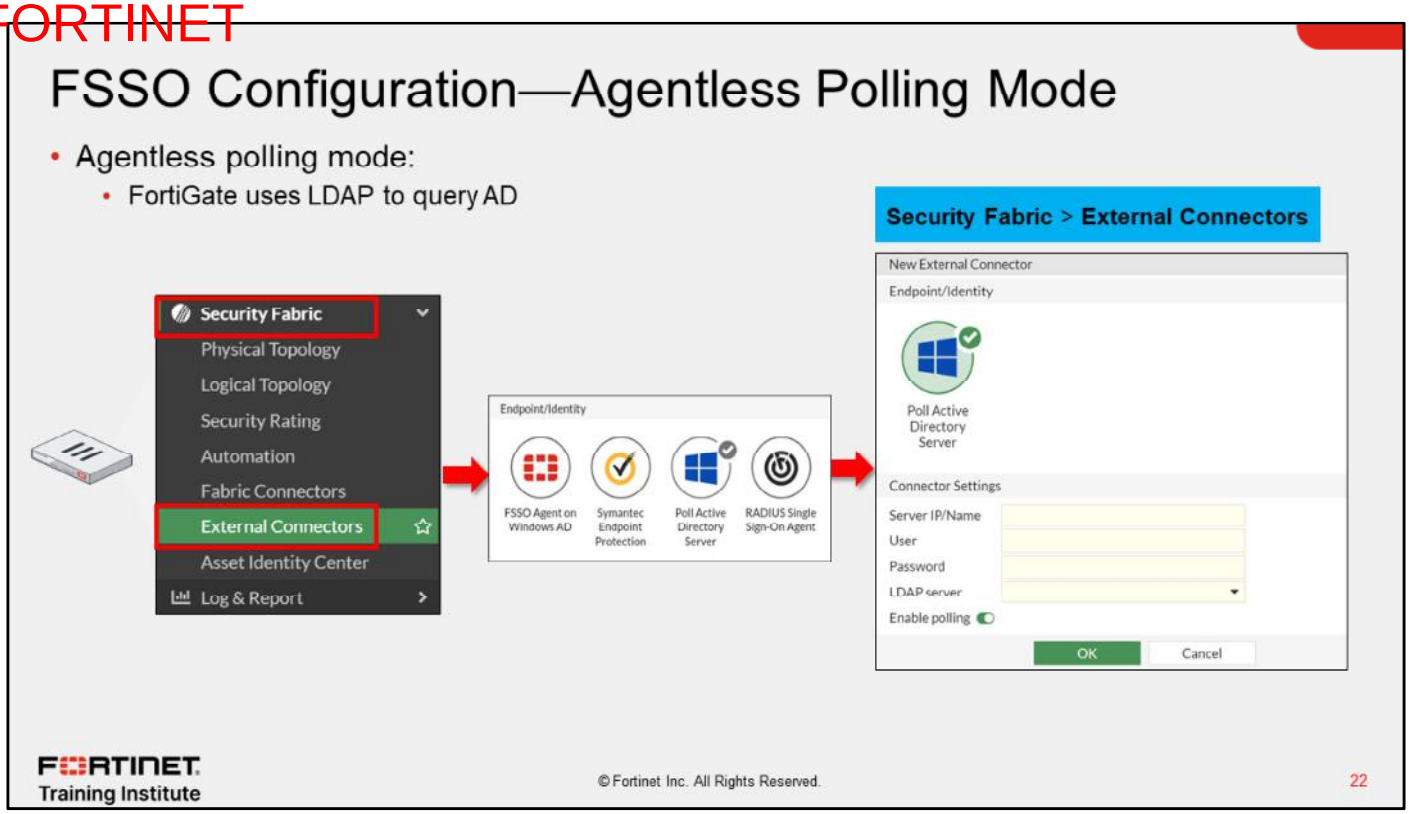
Good job! You now understand how FortiGate detects login events in Windows Active Directory (AD) using FSSO.

Now, you'll lean how to configure FSSO settings.



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

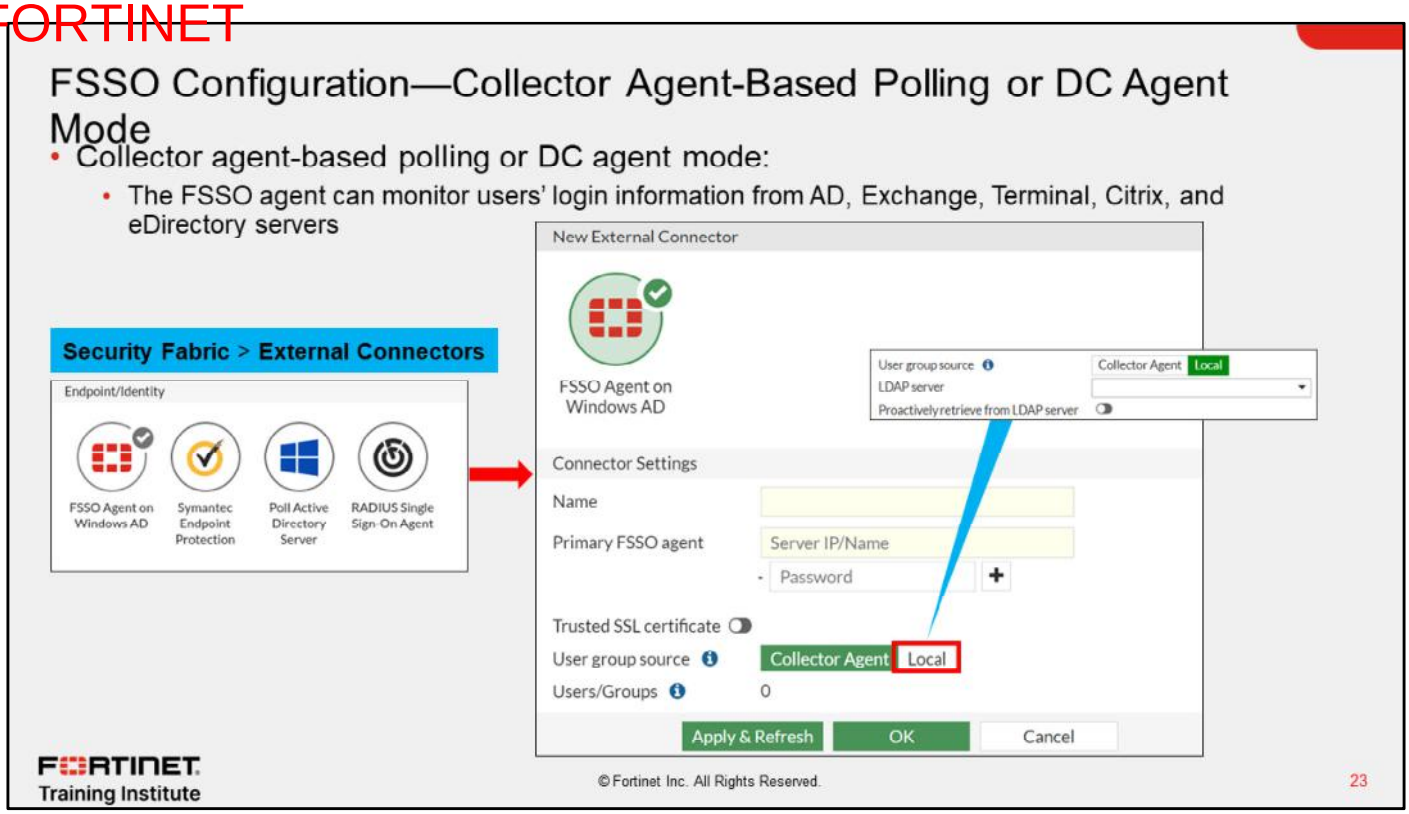
By demonstrating competence in configuring the FSSO settings on FortiGate, and installing and configuring the FSSO agents, you will be able to implement FSSO within your network.



FortiGate FSSO configuration is straightforward.

If FortiGate is acting as a collector for agentless polling mode, you must select **Poll Active Directory Server** and configure the IP addresses and AD administrator credentials for each DC.

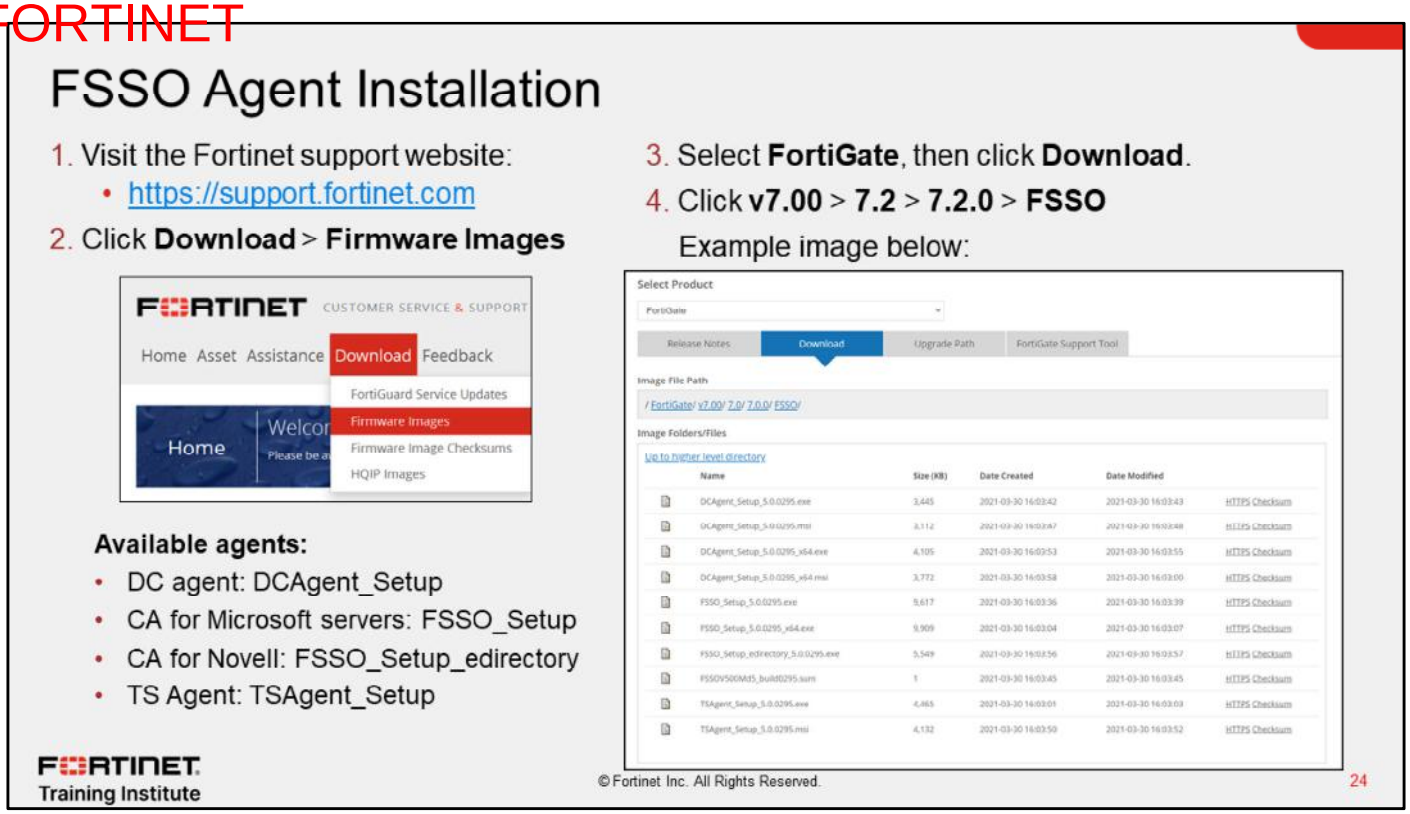
FortiGate uses LDAP to query AD to retrieve user group information. For this to happen, you must add the LDAP server to the **Poll Active Directory Server** configuration.



If you have collector agents, using either the DC agent mode or the collector agent-based polling mode, you must select **Fortinet Single-Sign-On Agent** and configure the IP address and password for each collector agent.

The FSSO collector agent can access Windows AD in one of two modes:

- **Collector Agent**: You create group filters are created on the collector agent. You can set FortiGate to **Collector Agent** mode, and the collector agent can still use **Advanced** mode to access nested groups.
- **Local**: You create group filters on FortiGate, using the LDAP server. If you set FortiGate to **Local** mode, you must set the collector agent to **Advanced** mode, otherwise the collector agent does not recognize the group filter sent by FortiGate and does not pass down any user logins.

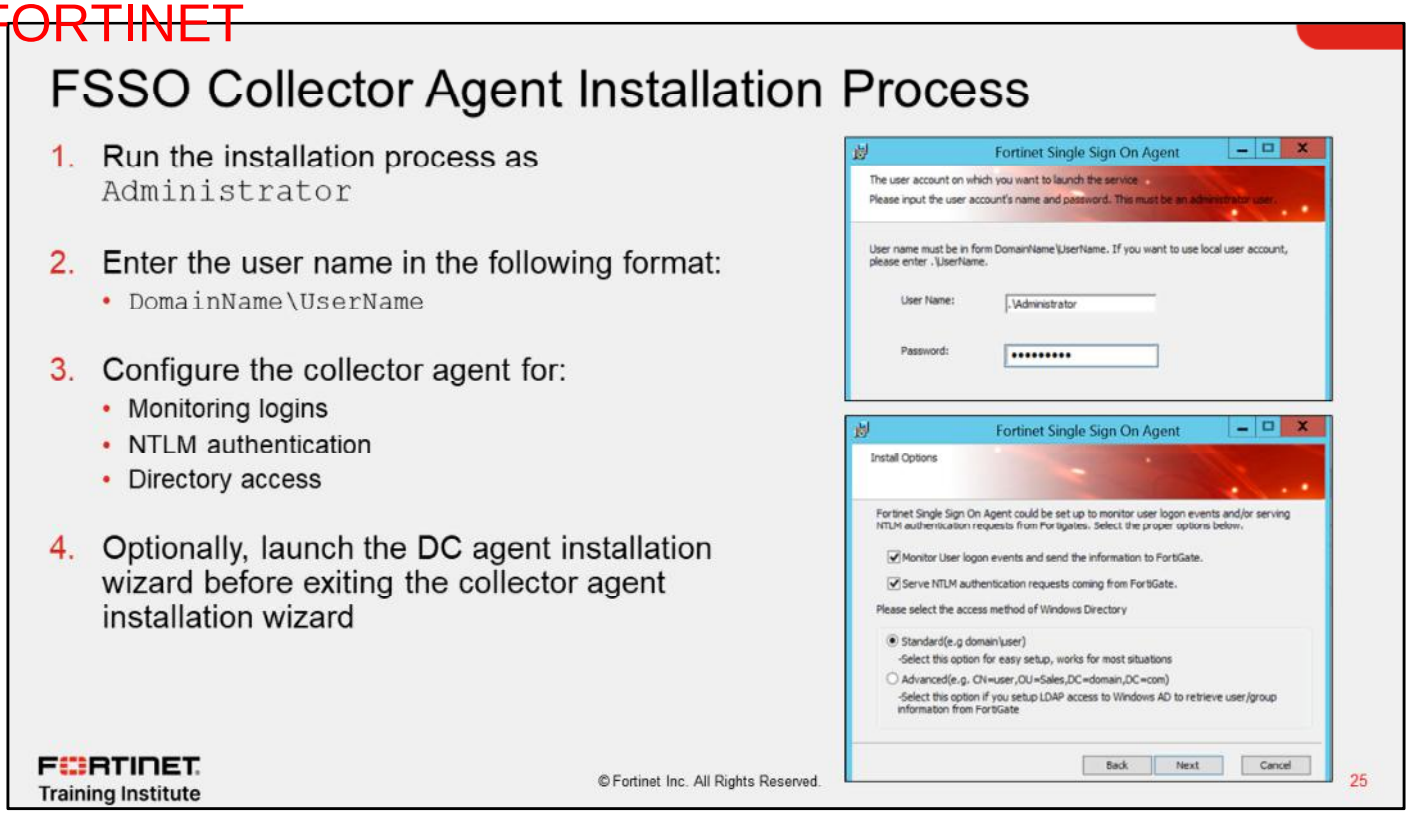


The FSSO agents are available on the Fortinet Support website. There you will find the following:

- The DC agent
- The collector agent for Microsoft servers: FSSO_Setup
- The collector agent for Novell directories: FSSO_Setup_edirectory
- The terminal server agent (TSagent) installer for Citrix and terminal servers: TSAgent_Setup

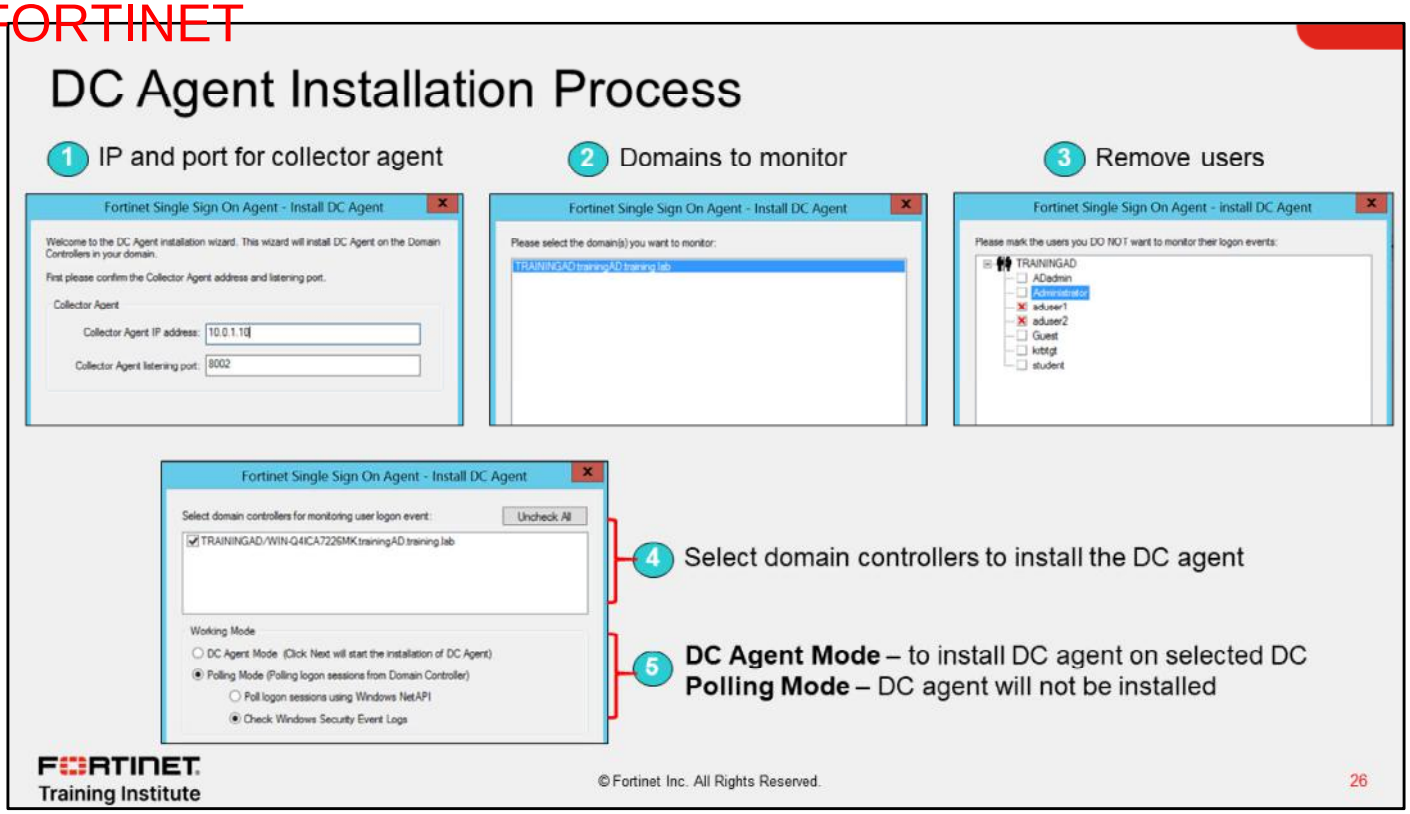
Also, for each agent, there are two versions: the executable (`.exe`) and Microsoft Installer (`.msi`).

Notice that you do not need to match the FSSO version with your exact FortiGate firmware version. When installing FSSO, grab the latest collector agent for your major release. You do however, need to match the DC agent version to the collector agent version.



After you've downloaded the collector agent, run the installation process as Administrator and follow these steps in the installation wizard:

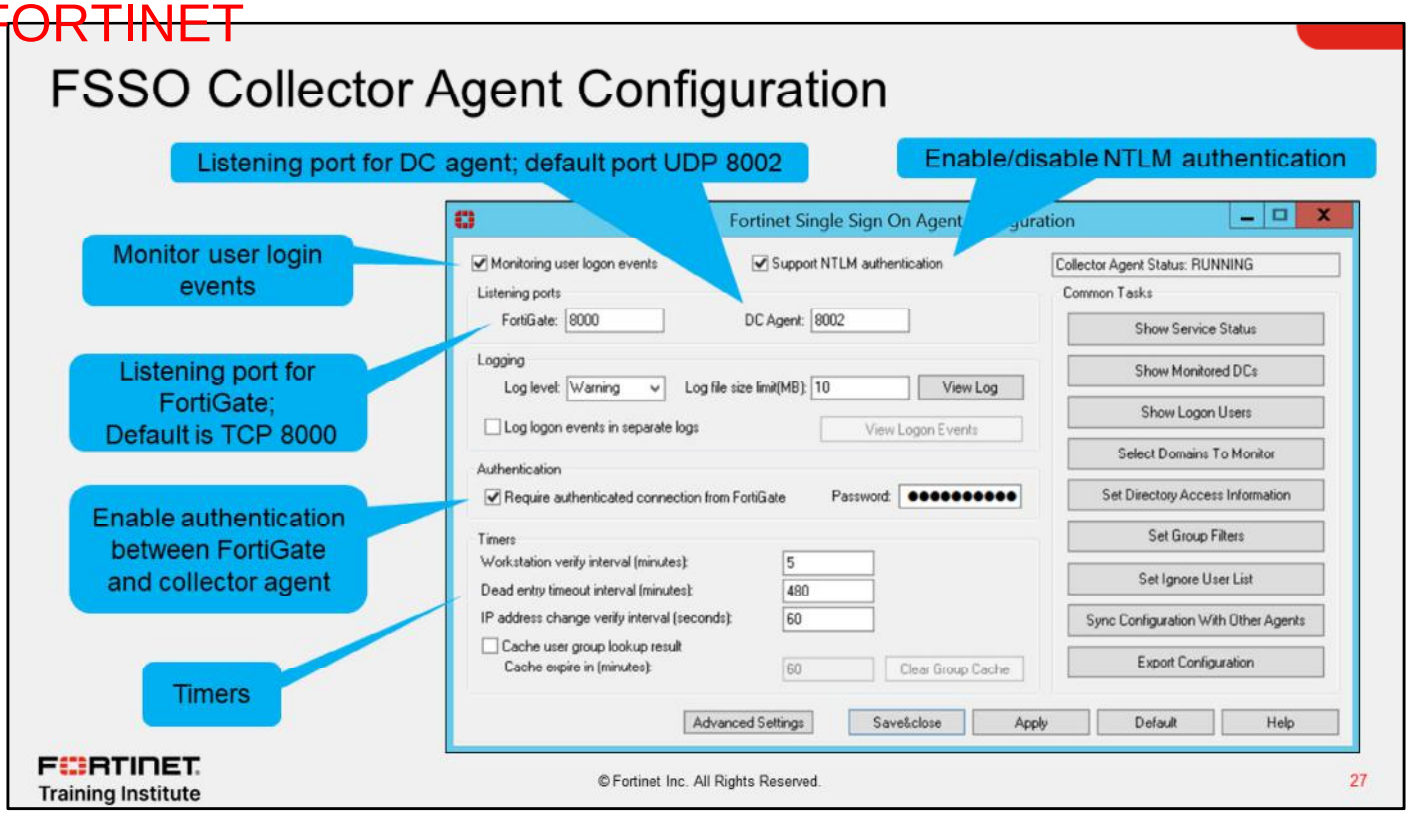
1. Read and accept the license agreement.
2. Optionally, change the installation location. The default folder is named `FSAE` (Fortinet Server Authentication Extension).
3. Enter the username. By default, the agent uses the name of the currently running account; however, you can change it using the format: **DomainName\UserName**.
4. Alternatively, configure your collector agent for monitoring, NTLM authentication, and directory access. These options are also customizable after installation. Although the default is **Standard** mode, when doing new FSSO setups it is always a best practice to install in **Advanced** mode. You will look at some of the advantages in this lesson.
5. If you want to use DC agent mode, make sure that **Launch DC Agent Install Wizard** is selected. This automatically starts the DC agent installation.



If you have just installed the collector agent and you selected **Launch DC Agent Install Wizard,** the installation process for domain controller agent automatically starts.

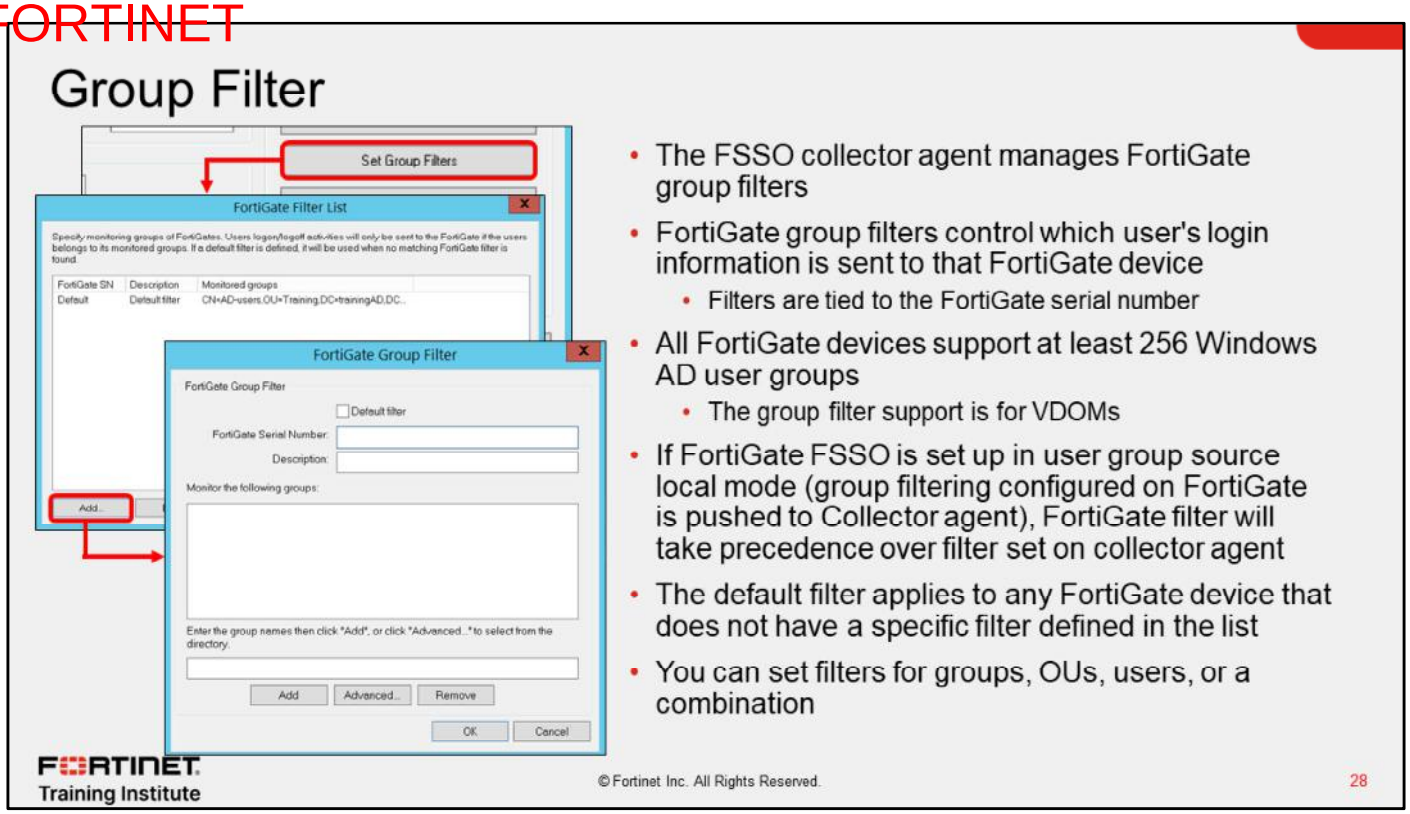
1. Enter the IP address for the collector agent. Optionally, you can customize the listening port, if the default value is already used by another service.
2. Select the domains to monitor. If any of your required domains are not listed, cancel the wizard and set up the correct trusted relationship with the domain controller. Then, run the wizard again. Note that this could also be a result of using an account without all the necessary permissions.
3. Optionally, select users that you do not want to monitor; these users' login events are not recorded by the collector and therefore are not passed to FortiGate. While these users are still able to generate login events to the domain, when they are detected by the collector agent, they are discarded so as to not interfere with the logged in user. This is especially useful in environments with a centrally managed antivirus solution, or a scheduled backup service that uses an AD account to start. These accounts can create login events for the collector agent that overwrite existing user logins. This may result in FortiGate applying the incorrect policies and profiles based on the overriding account. You can also customize the option to ignore users after installation is complete.
4. Optionally, clear the checkboxes of domain controllers that you don't want to install the DC agent on. Remember, for DC agent mode FSSO, at least one domain controller must have the DC agent installed. Also remember that installing the DC agent requires a reboot of the DC before it will start gathering login events. You can add or remove the DC agent to DCs at any time after the installation is complete.
5. Select **DC Agent Mode** as the working mode. If you select **Polling Mode**, the DC agent will not be installed.

Finally, the wizard requests a system reboot.



On the FSSO agent configuration GUI, you can configure settings such as:

- The listening port for the communication with the DC agents (UDP)
- The listening port for the communication with FortiGate (TCP)
- NTLM authentication support
- Password authentication between the collector agent and FortiGate
- Timers



The FSSO collector agent allows you to configure a FortiGate group filter, which actively controls what user login information is sent to each FortiGate device. So, you can define which groups the collector agent passes to individual FortiGate devices.

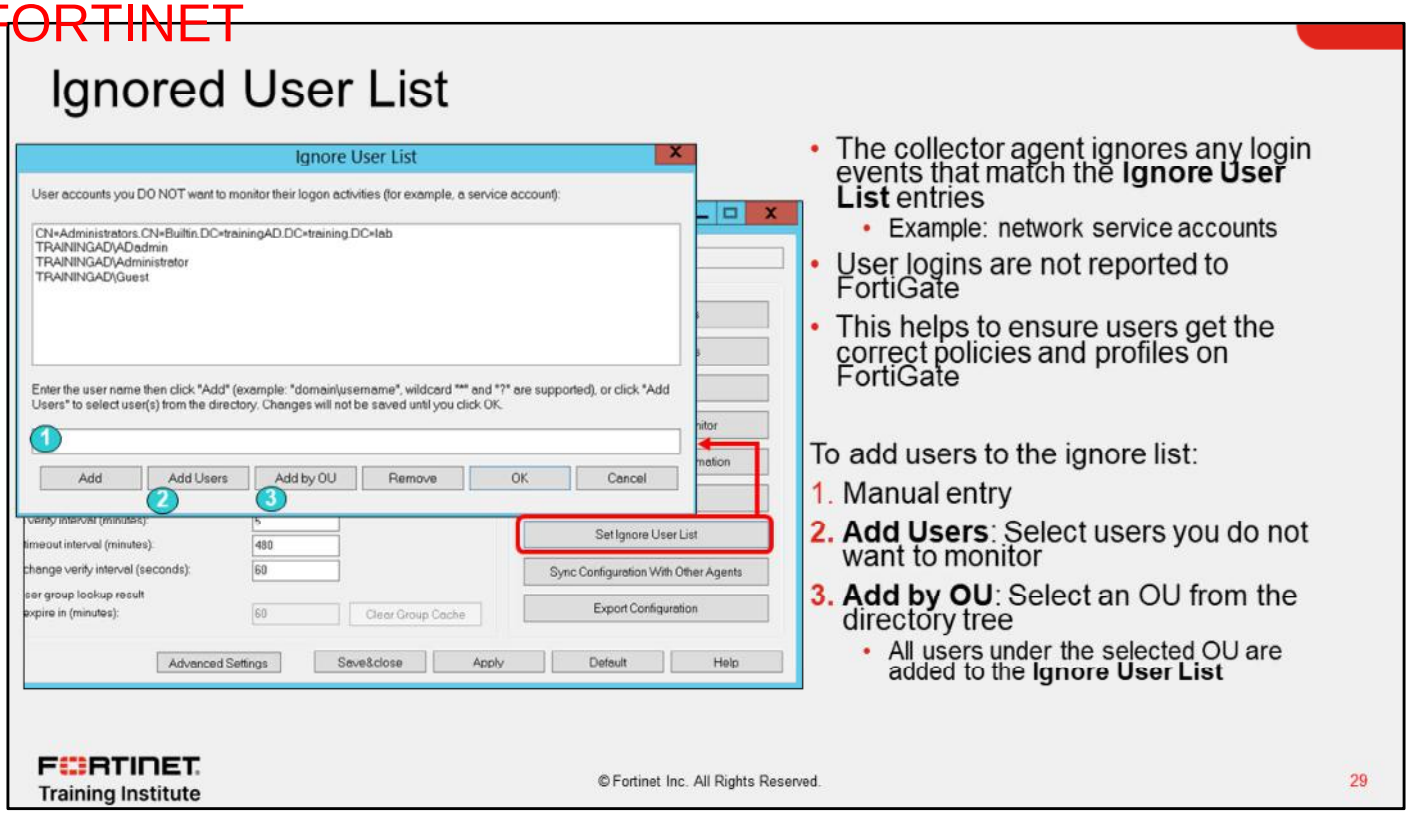
Monitoring the entire group list in a large AD structure is highly inefficient, and a waste of resources. Most FSSO deployments need group segmentation (at least four or five groups), with the intention of assigning varying levels of security profile configurations to the different groups, using identity-based policies.

Group filters also help to limit the traffic sent to FortiGate. The maximum number of Windows AD user groups allowed on FortiGate depends on the model. Low-end FortiGate models support 256 Windows AD user groups. Mid-range and high-end models can support more groups. This is per VDOM, if VDOMs are enabled on FortiGate.

You can filter on FortiGate instead of the collector agent, but only if the collector agent is operating in advanced mode. In this case, the collector agent uses the list of groups you selected on FortiGate as its group filter for that device.

The filter list is initially empty. At a minimum, you should create a default filter that applies to all FortiGate devices without a defined filter.

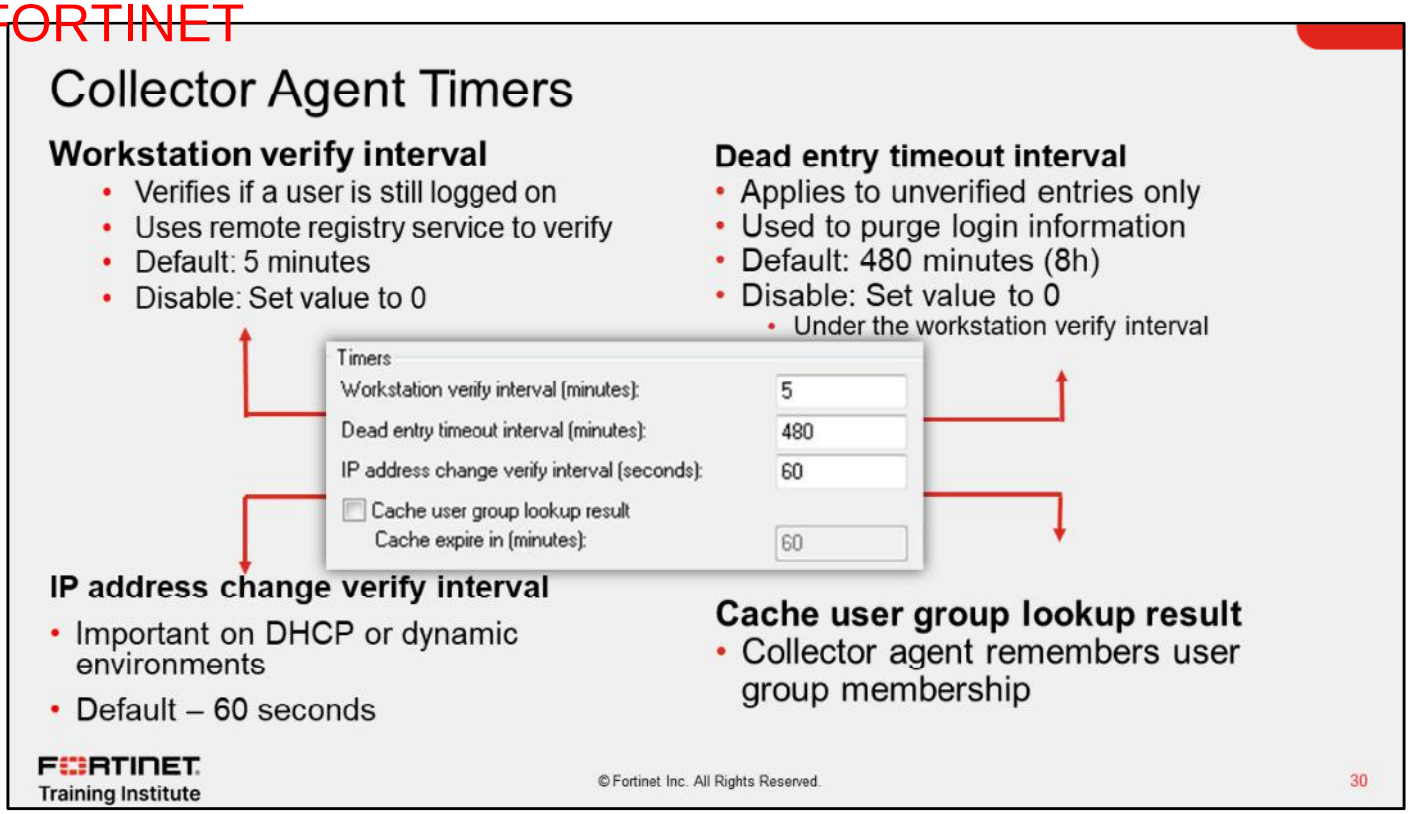
Note that if you change the AD access mode from **Standard** to **Advanced** or **Advanced** to **Standard**, you must recreate the filters because they vary depending on the mode.



The FSSO collector agent ignores any login events that match the **Ignore User List** entries. Therefore, these login events are not recorded by the collector agent, nor are they reported to FortiGate.

It is a good practice to add all network service accounts to the **Ignore User List**. Service accounts tend to overwrite user login events, and create issues with identity-based policy matching.

You can add users to the **Ignore Users List** in the following ways:
- Manually enter the username.
- Click **Add Users**, and then choose the users you do not want to monitor.
- Click **Add by OU**, and then select an OU from the directory tree.



The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

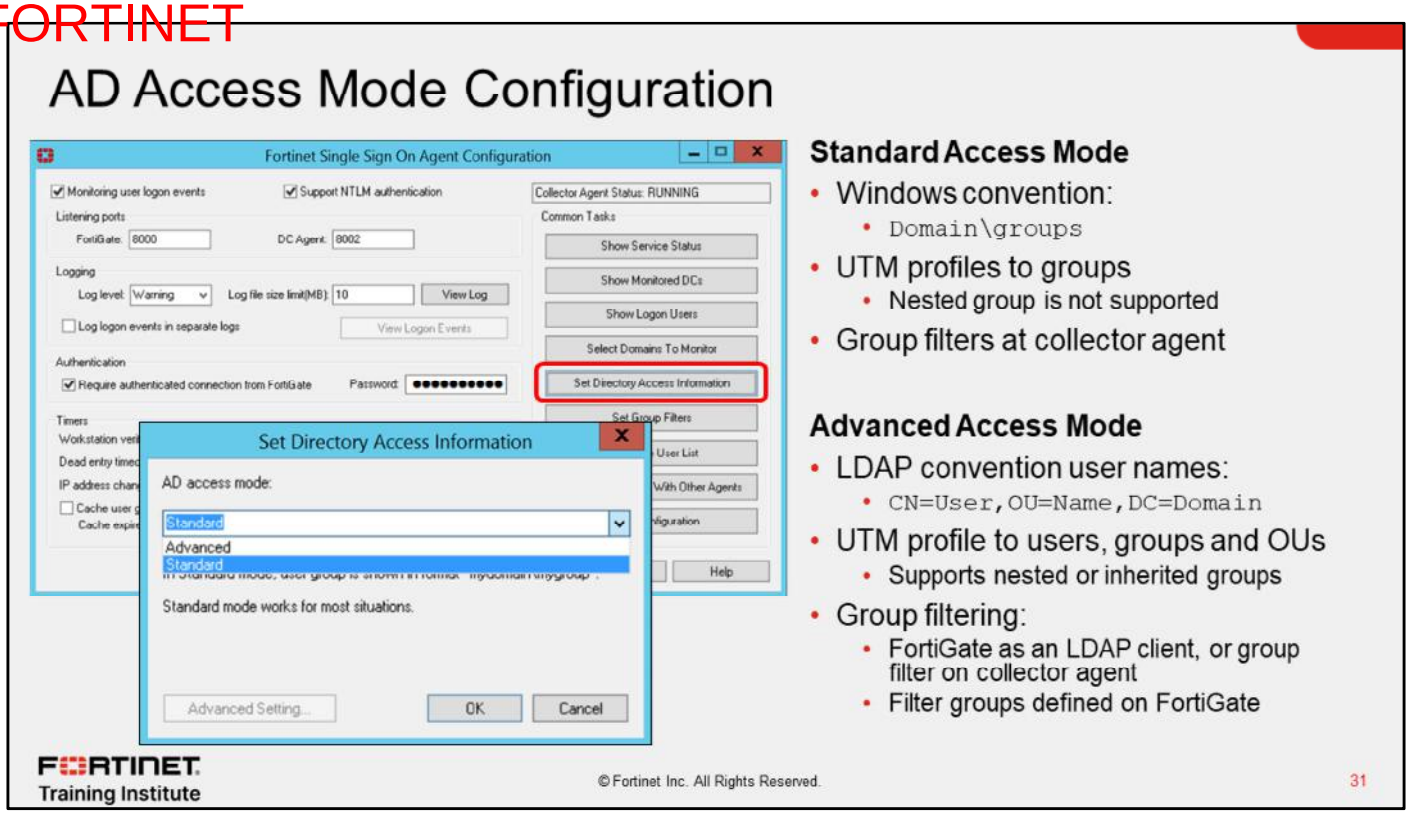
Now, you'll take a look at each one and how they work.

- **Workstation verify interval**. This setting controls when the collector agent connects to individual workstations on port 139 (or port 445), and uses the remote registry service to verify if a user is still logged in to the same station. It changes the status of the user under **Show login User**, to **not verified** when it cannot connect to the workstation. If it does connect, it verifies the user and the status remains **OK**. To facilitate this verification process, you should set the remote registry service to auto start on all domain member PCs.

- **Dead entry timeout interval**. This setting applies only to entries with an unverified status. When an entry is not verified, the collector starts this timer. It's used to age out the entry. When the timer expires, the login is removed from the collector. From the perspective of FortiGate, there is no difference between entries that are **OK** and entries that are **not verified**. Both are considered valid.

- **IP address change verify interval**. This setting checks the IP addresses of logged in users and updates FortiGate when a user's IP address changes. This timer is especially important in DHCP or dynamic environments to prevent users from being locked out if they change IP address. The domain DNS server should be accurate; if the DNS server does not update the affected records promptly, the collector agent's IP information is inaccurate.

- **Cache user group lookup result**. This setting caches the user group membership for a defined period of time. It is not updated, even if the user changes group membership in AD.



Another important FSSO setting is the AD access mode. You can set the AD access mode by clicking **Set Directory Access Information**. The AD access mode specifies how the collector agent accesses and collects the user and user group information. There are two modes that you can use to access AD user information: **Standard** and **Advanced**.

The main difference between modes is the naming convention used:
- **Standard** mode uses the Windows convention, NetBios: `Domain\groups`, while
- **Advanced** mode uses the LDAP convention: `CN=User, OU=Name, DC=Domain`.

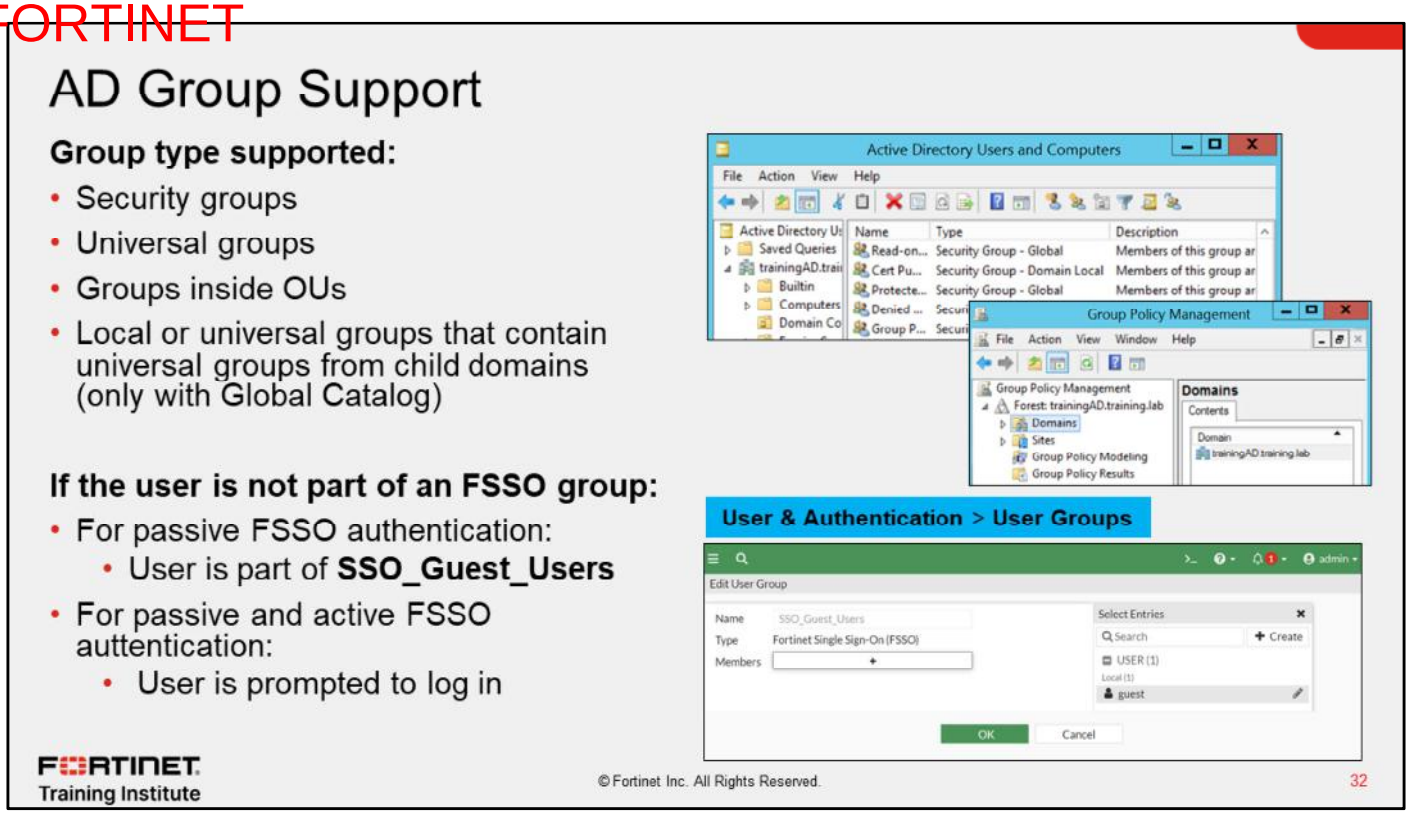
Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored *parent* groups. Additionally, in advanced mode, FortiGate can apply security profiles to individual users, user groups, and OUs.

In comparison, in standard mode, you can apply security profiles only to user groups, not individual users.

In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.

If the LDAP on the collector agent fails, it doesn't matter what the LDAP on the FortiGate says, FSSO won't work. If the FortiGate LDAP fails, but the LDAP on the collector agent is still running, the FortiGate may not be able to collect logs, but the collector agent still collects logs.

Fortinet strongly encourages users to create filters from the collector agent.



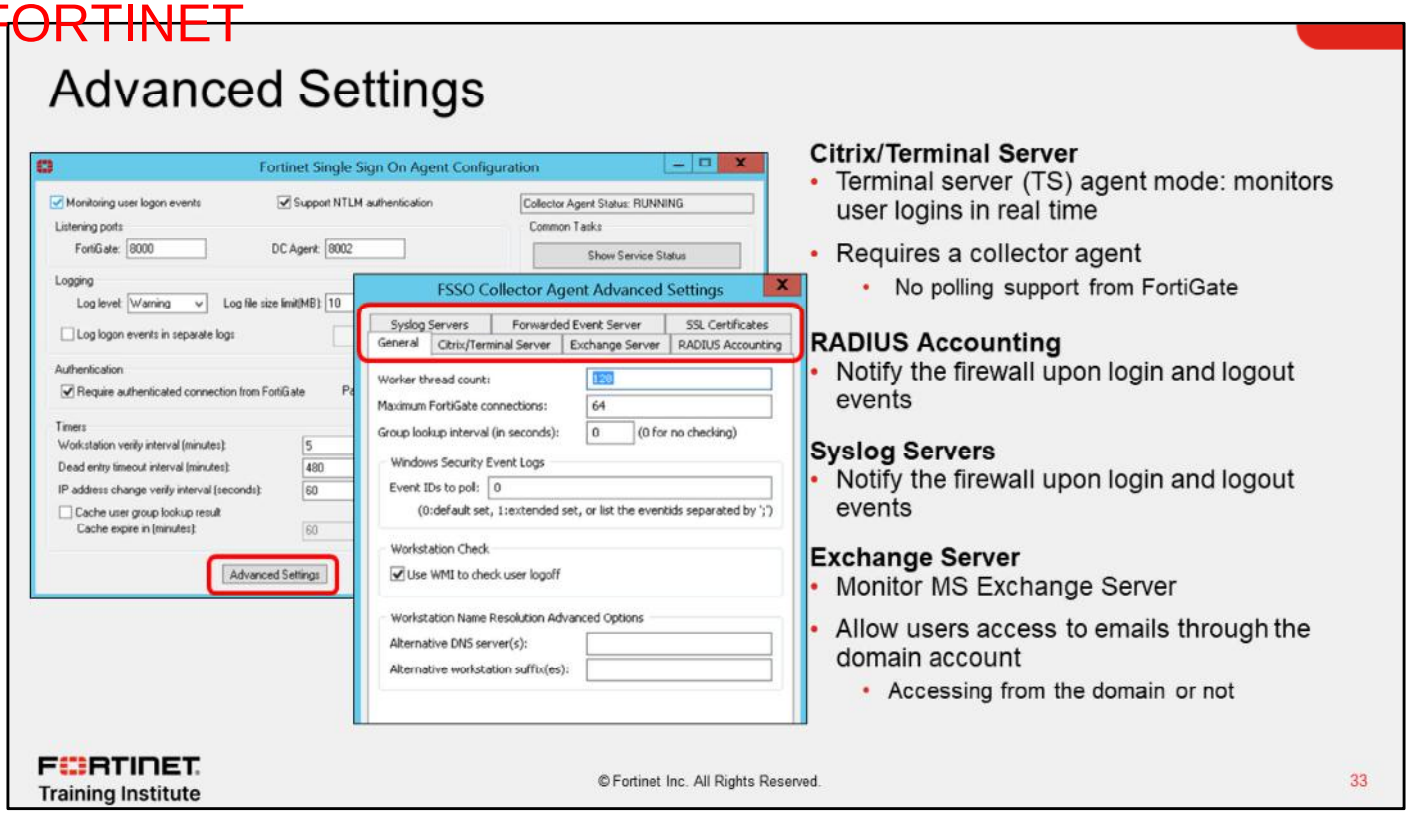
In AD settings, not all group types are supported. AD settings supports filtering groups only from:

- Security groups
- Universal groups
- Groups inside OUs
- Local or universal groups that contain universal groups from child domains (only with Global Catalog)

All FortiGate configurations include a user group called **SSO_Guest_Users**. When only passive authentication is used, all the users that do not belong to any FSSO group are automatically included in this guest group.

This allows an administrator to configure limited network access to guest users that do not belong to the Windows AD domain.

However, if both passive and active authentication are enabled for specific traffic, you cannot use **SSO_Guest_Users**, because traffic from IP addresses not on the FSSO user list must be prompted to enter their credentials.



Depending on your network, you might need to configure advanced settings in your FSSO collector agent.

Citrix servers support FSSO. Terminal server (TS) agent mode allows the server to monitor user logins in real time. The TS agent is like a DC agent, it also needs the collector agent to collect and send the login events to FortiGate. It then uses the same ports to report the logins back to the collector agent.

The collector agent on its own can get accurate login events only from Citrix servers if each user gets their own IP address. Otherwise, if multiple users share the same IP address, the TS agent is needed so that it can report to the collector agent the user, IP address, and source port range assigned to that user. The TS agent cannot forward logs directly to FortiGate, the logs first have to be gathered by a collector. This does not work with polling from FortiGate.

A RADIUS server configured as a RADIUS-based accounting system can interact in your network by sending accounting messages to the collector agent. The FSSO collector agent also supports integration with syslog servers for the same purpose.

The FSSO collector agent can also monitor a Microsoft Exchange server, which is useful when users access their email using their domain account.

For **Windows Security Event Logs** polling mode, you can configure **Event IDs to poll** here. For specific event IDs, visit the Fortinet Knowledge Base (http://kb.fortinet.com).

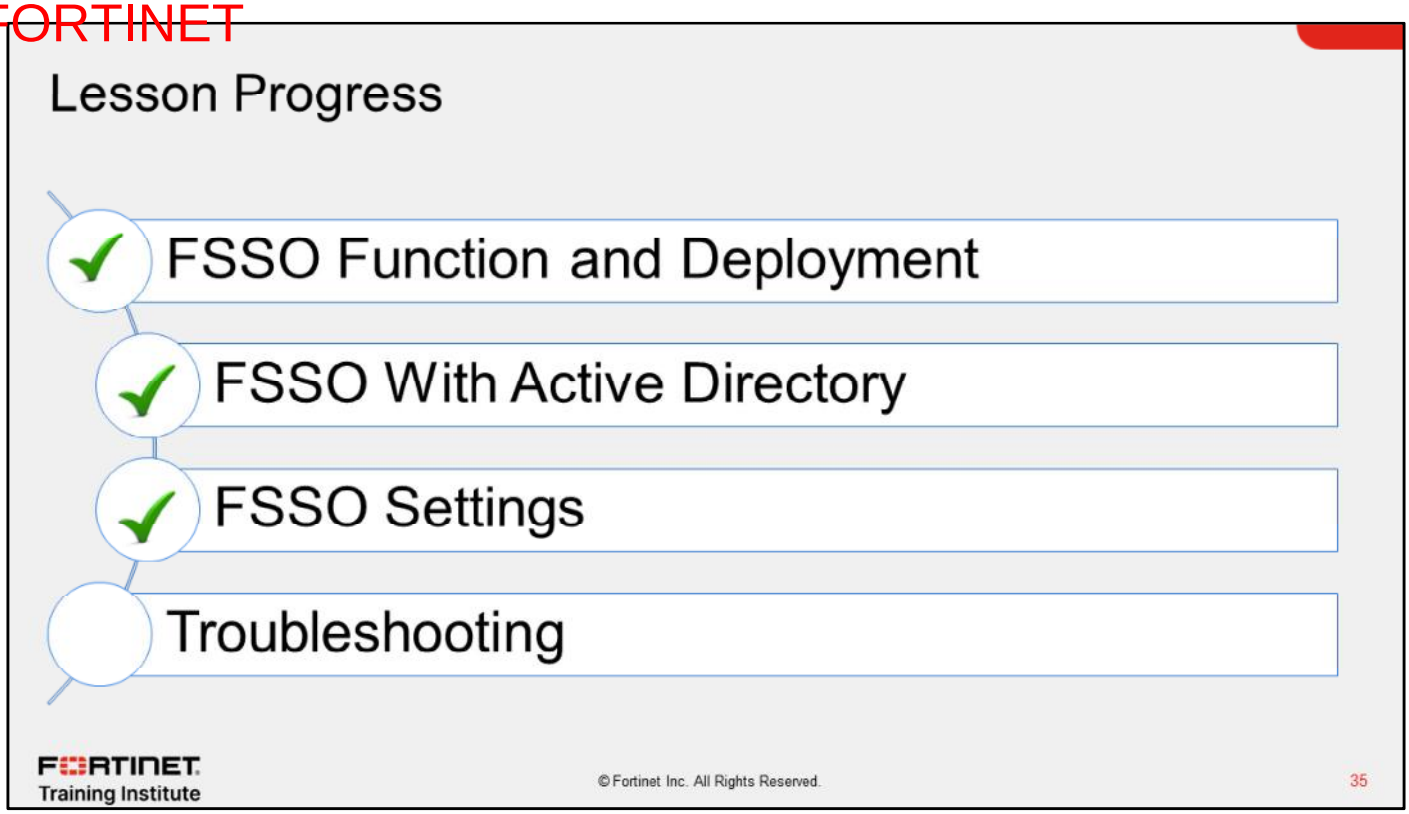
Knowledge Check

1. If you have collector agents using either the DC agent mode or the collector agent-based polling mode, which fabric connector should you select on FortiGate?
   - A. Poll Active Directory Server
   - ✓ B. Fortinet Single Sign-On Agent

2. Which naming conventions does the FSSO collector agent use to access the Windows AD in **Standard** access mode?
   - ✓ A. Windows convention - NetBios: `Domain\groups`
   - B. LDAP convention: `CN=User,OU=Name,DC=Domain`

FORTINET Training Institute

34

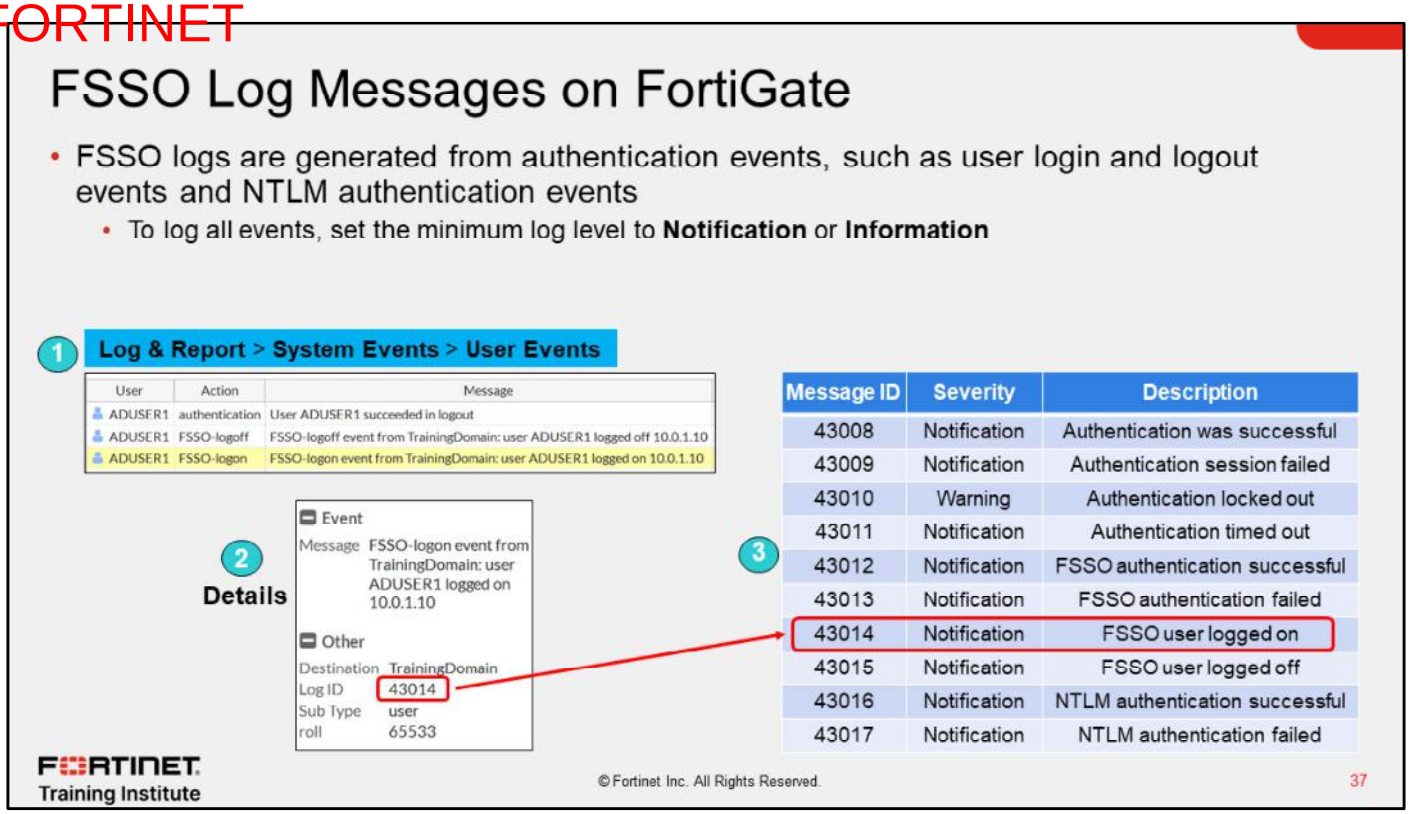


Good job! You now understand how to configure the SSO settings on FortiGate and the FSSO collector agent.

Now, you'll learn about some basic troubleshooting options.

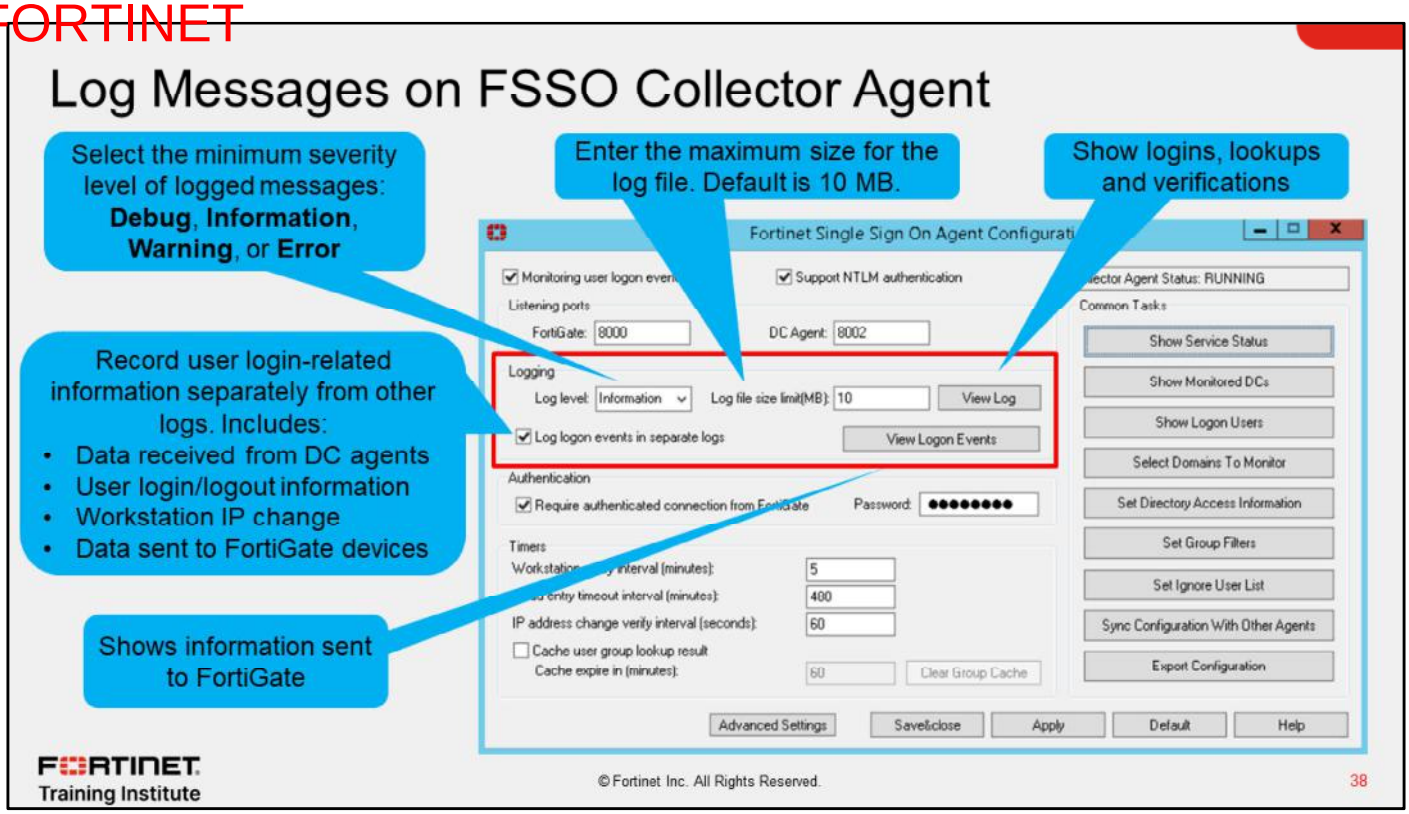
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FSSO monitoring and troubleshooting, you will be able to prevent, identify, and solve common issues related to FSSO.



FSSO-related log messages are generated from authentication events. These include user login and logout events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues.

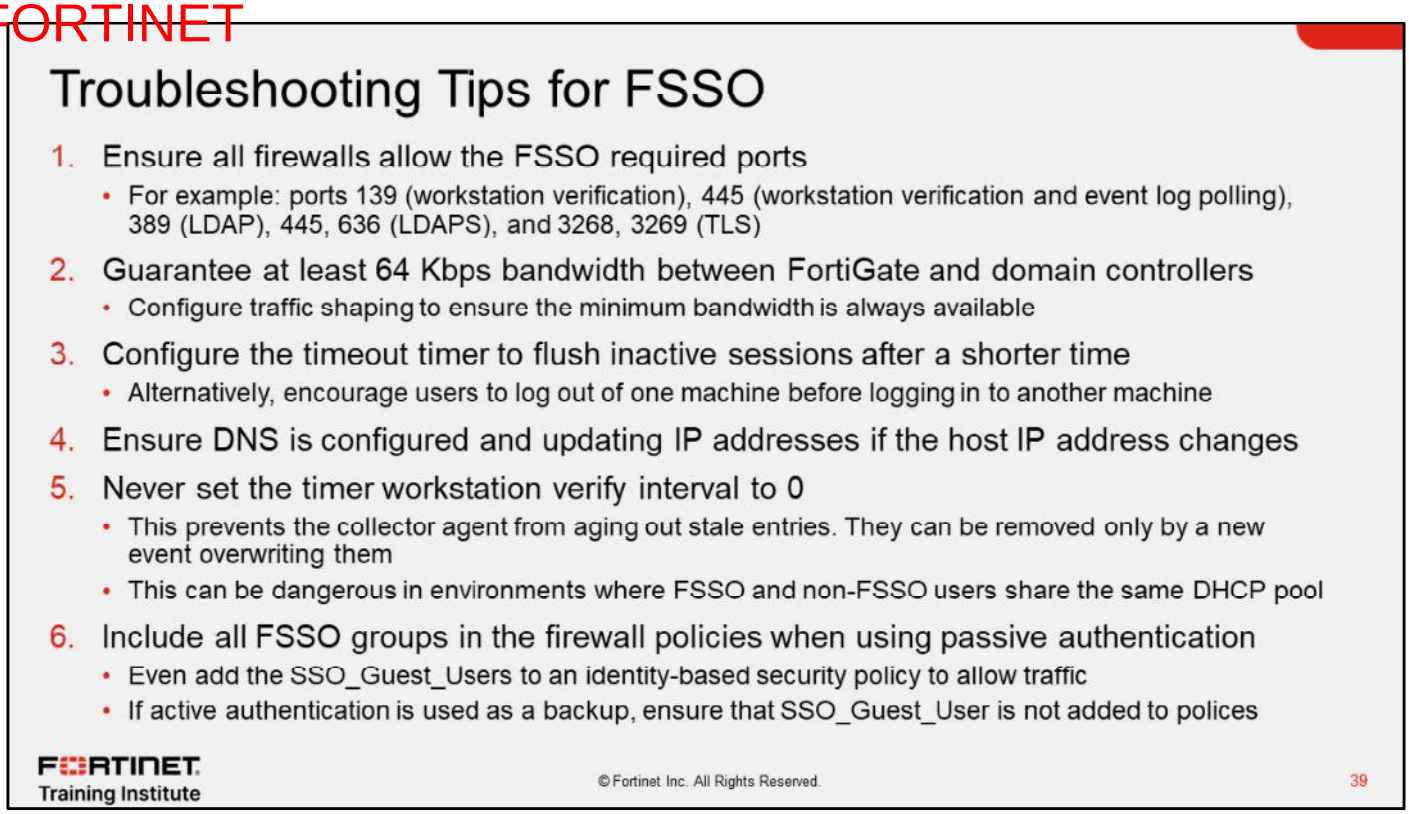
To ensure you log all the events needed, set the minimum log level to **Notification** or **Information**. Firewall logging requires **Notification** as a minimum log level. The closer the log level is to **Debug** level, the more information is logged.



When troubleshooting FSSO agent-based deployments, you might want to look at the log messages generated directly on the FSSO collector agent.

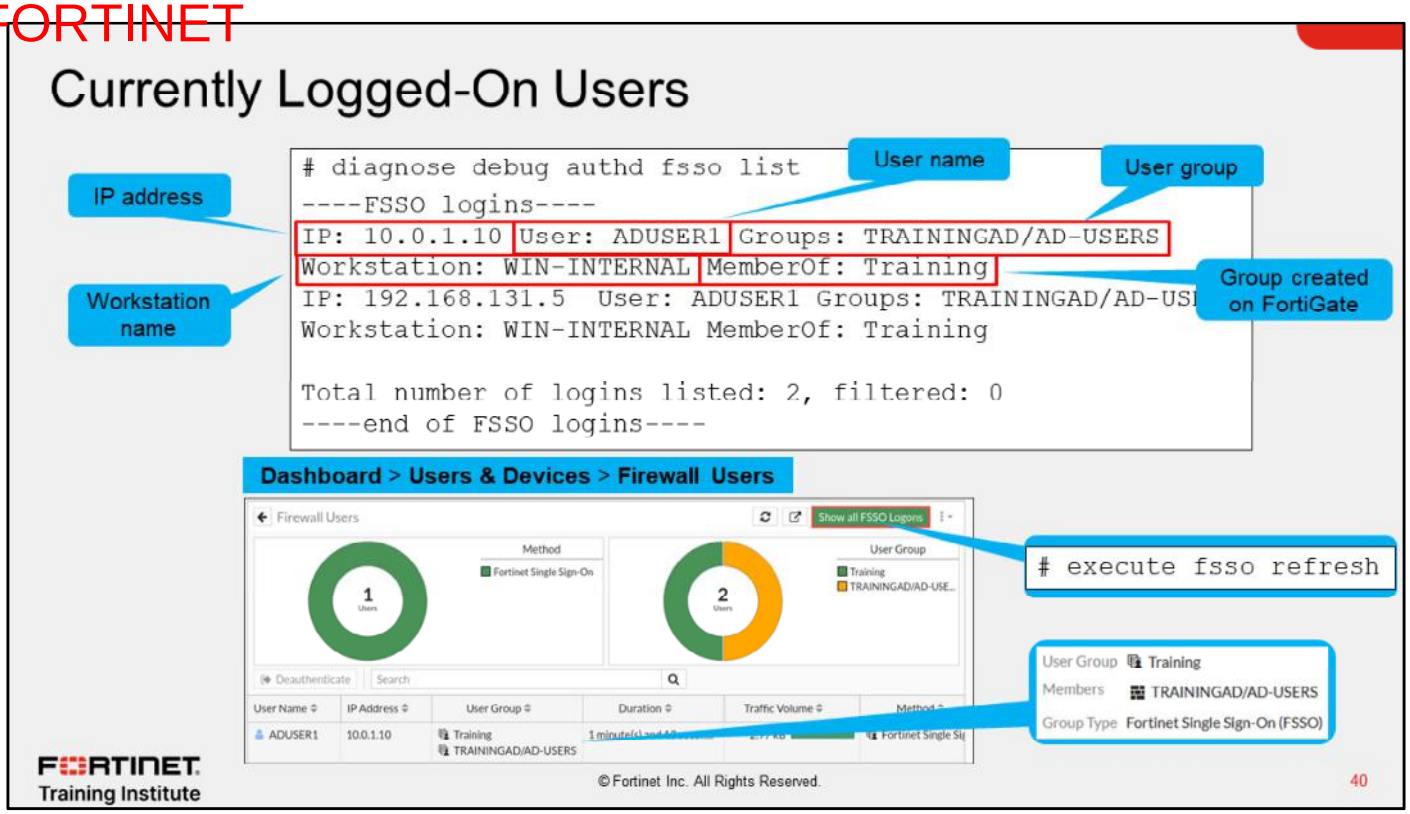
The **Logging** section of the FSSO collector agent allows the following configurations:

- **Log level**: Select the minimum severity level of logged messages. Includes these levels:
  - **Debug**: the most detailed log level. Use it when actively troubleshooting issues.
  - **Information**: includes details about login events and workstation checks. This is the recommended level for most troubleshooting.
  - **Warning**: the default level. It provides information about failures.
  - **Error**: lists only the most severe events.
- **Log file size limit (MB)**: Enter the maximum size for the log file in MB. The default is 10.
- **View Log**: View all FSSO agent logs.
- **Log login events in separate logs**: Record user login-related information separately from other logs. The information in this log includes: data received from DC agents, user login/logout information, workstation IP change information, and data sent to FortiGate devices. When selected, a summary of events sent and removed from FortiGate is listed under **View login Events**, while all other information remains under **View Log**.
- **View login Events**: If **Log login events in separate logs** is enabled, you will can view user login-related information.



Begin with the following tips, which are useful in many FSSO troubleshooting situations:

- FSSO has a number of required ports that you must allow through all firewalls, or connections will fail. These include ports: 139 (workstation verification), 445 (workstation verification and event log polling), 389 (LDAP), and 445 and 636 (LDAPS).
- Configure traffic shaping between FortiGate and the domain controllers to ensure that the minimum bandwidth is always available. If there is insufficient bandwidth, some FSSO information might not reach FortiGate.
- In an all-Windows environment, flush inactive sessions. Otherwise, you can have a session for a non-authenticated machines go out as an authenticated user. This can occur if the DHCP lease expires for the authenticated user with the collector agent being able to verify that the user has indeed logged out.
- Ensure DNS is configured correctly and updating IP addresses, if workstation IP addresses change.
- Never set the workstation verify interval to 0. This prevents the collector agent from aging out stale entries. They can be removed only by a new event overwriting them. This can be especially dangerous in environments where FSSO and non-FSSO users share the same DHCP pool.
- When using passive authentication only, include the group of guest users in a policy and give them access. Associate their group with a security policy. If you use active authentication as a backup, ensure you do not add SSO_Guest_User to polices. SSO_Guest_User and active authentication are mutually exclusive.

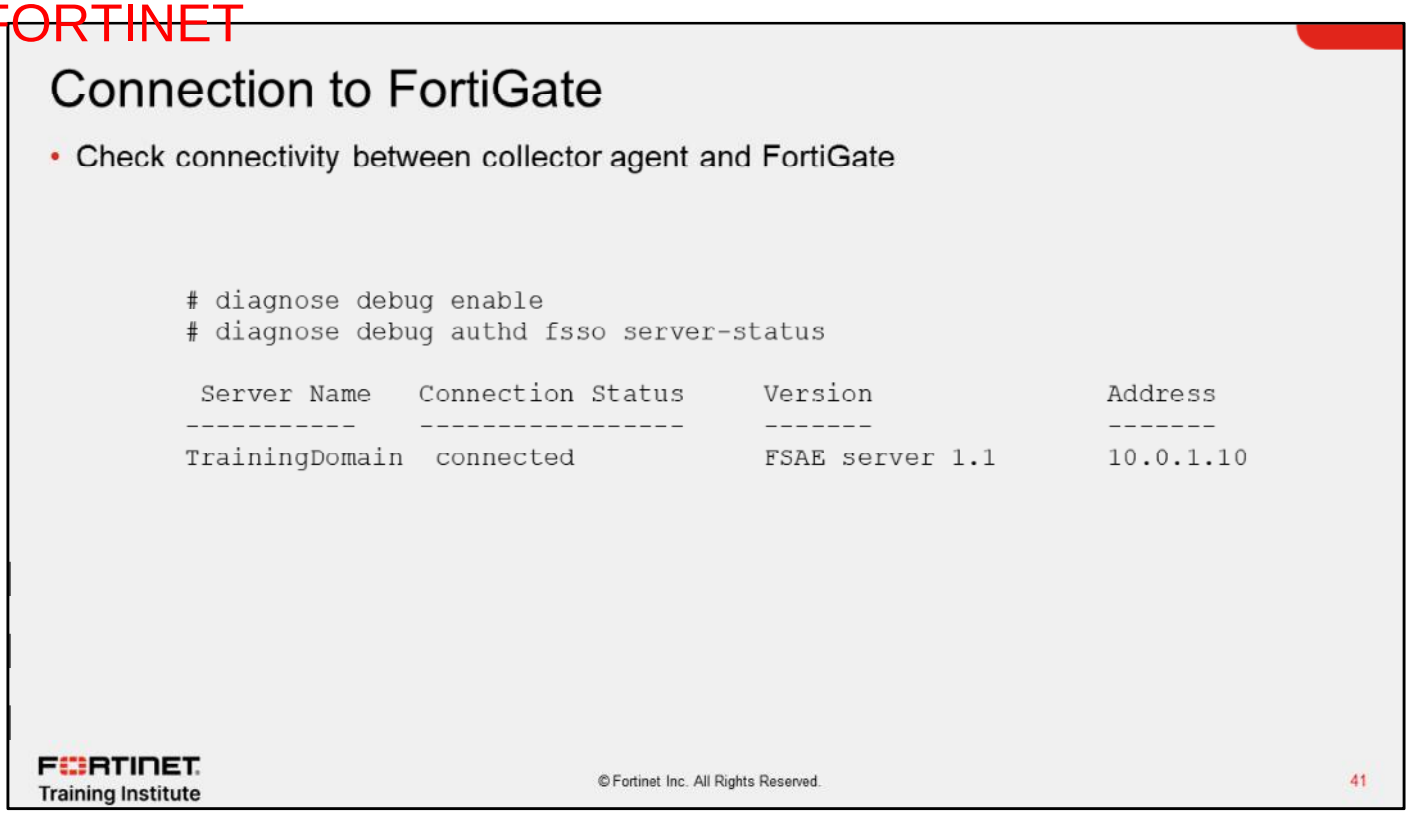


If applying the tips from the previous slide didn't solve your FSSO issues, you may need to apply some `debug` commands.

To display the list of FSSO users that are currently logged in, use the CLI command `diagnose debug authd fsso list`.

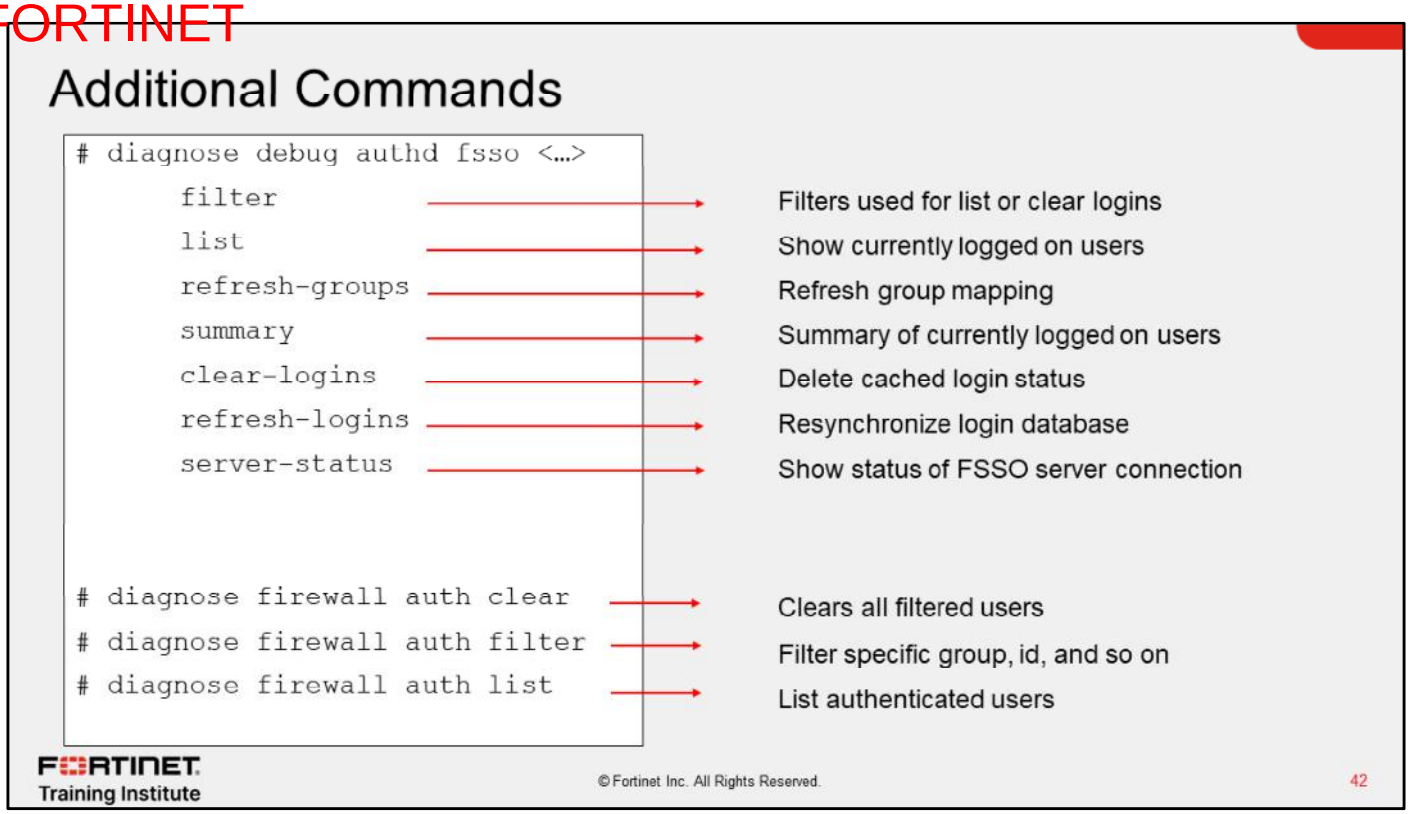
For each user, the user name, user group, IP address, and the name of the workstation from which they logged in shows. The `MemberOf` section shows the group that was created on the firewall, to which you mapped the AD group. The same group should show in the **User group** screen on the GUI.

Also, use `execute fsso refresh` to manually refresh user group information from any directory service servers connected to FortiGate, using the collector agent.

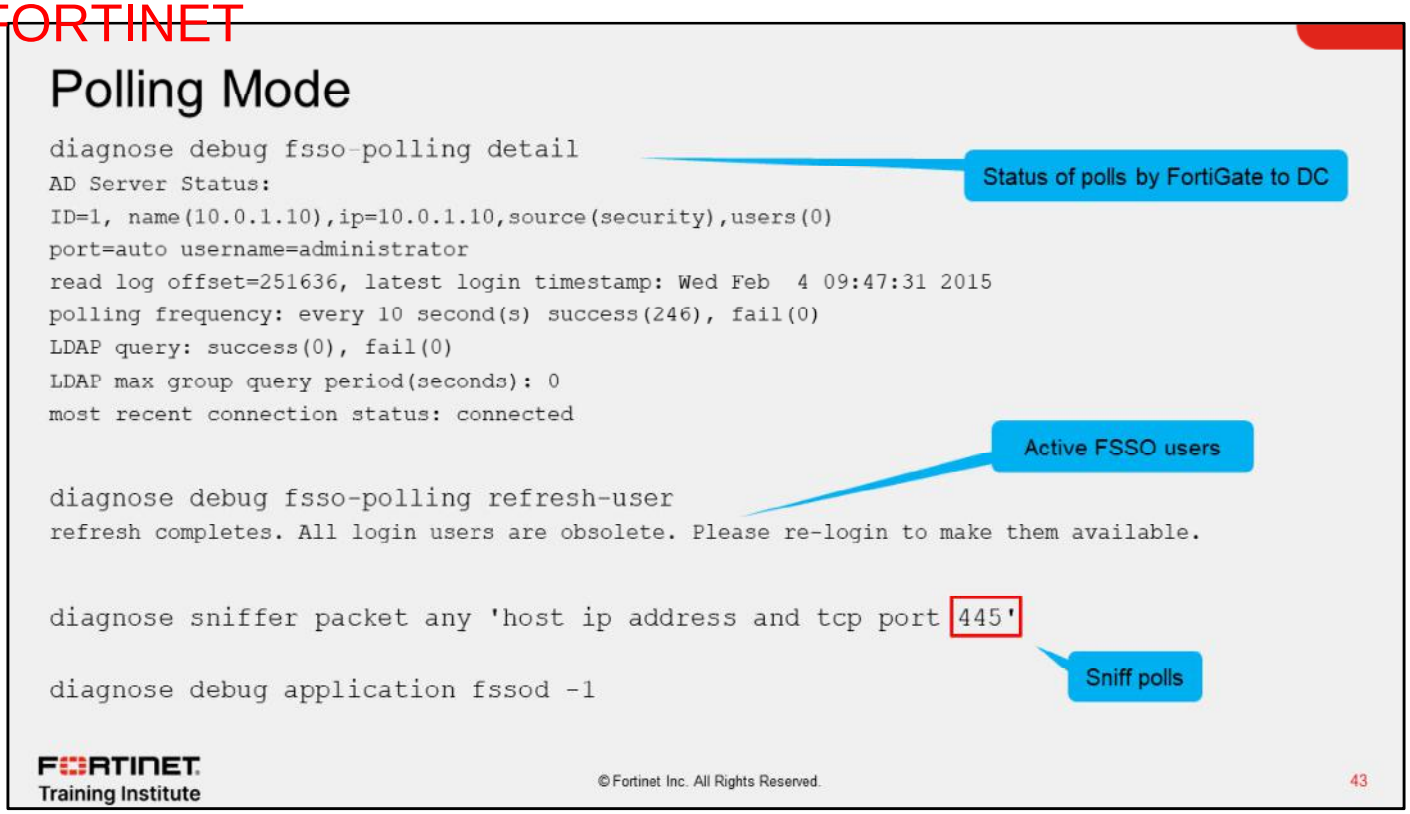


To show the status of communication between FortiGate and each collector agent, you can use the CLI command `diagnose debug authd fsso server-status`.

However, before you use that command, you must first run the command `diagnose debug enable`.



Also, available under `diagnose debug authd fsso` are commands for clearing the FortiGate cache of all currently logged in users, filtering the display of the list of logged in users, and refreshing the login and user group information.



The command `diagnose debug fsso-polling detail` displays status information and some statistics related to the polls done by FortiGate on each DC in agentless polling. If the `read log offset` is incrementing, FortiGate is connecting to and reading the logs on the domain controller. If the `read log offset` is incrementing but you are not getting any login events, check that the group filter is correct and that the domain controller is creating the correct event IDs.

The command `diagnose debug fsso-polling refresh-user` flushes information about all the active FSSO users.

In agentless polling mode, FortiGate frequently polls the event viewer to get the login events. You can sniff this traffic on port 445.

Also, there is a specific FortiGate daemon that handles polling mode. It is the `fssod` daemon. To enable agentless polling mode real-time debug, use the `diagnose debug application fssod -1` command.

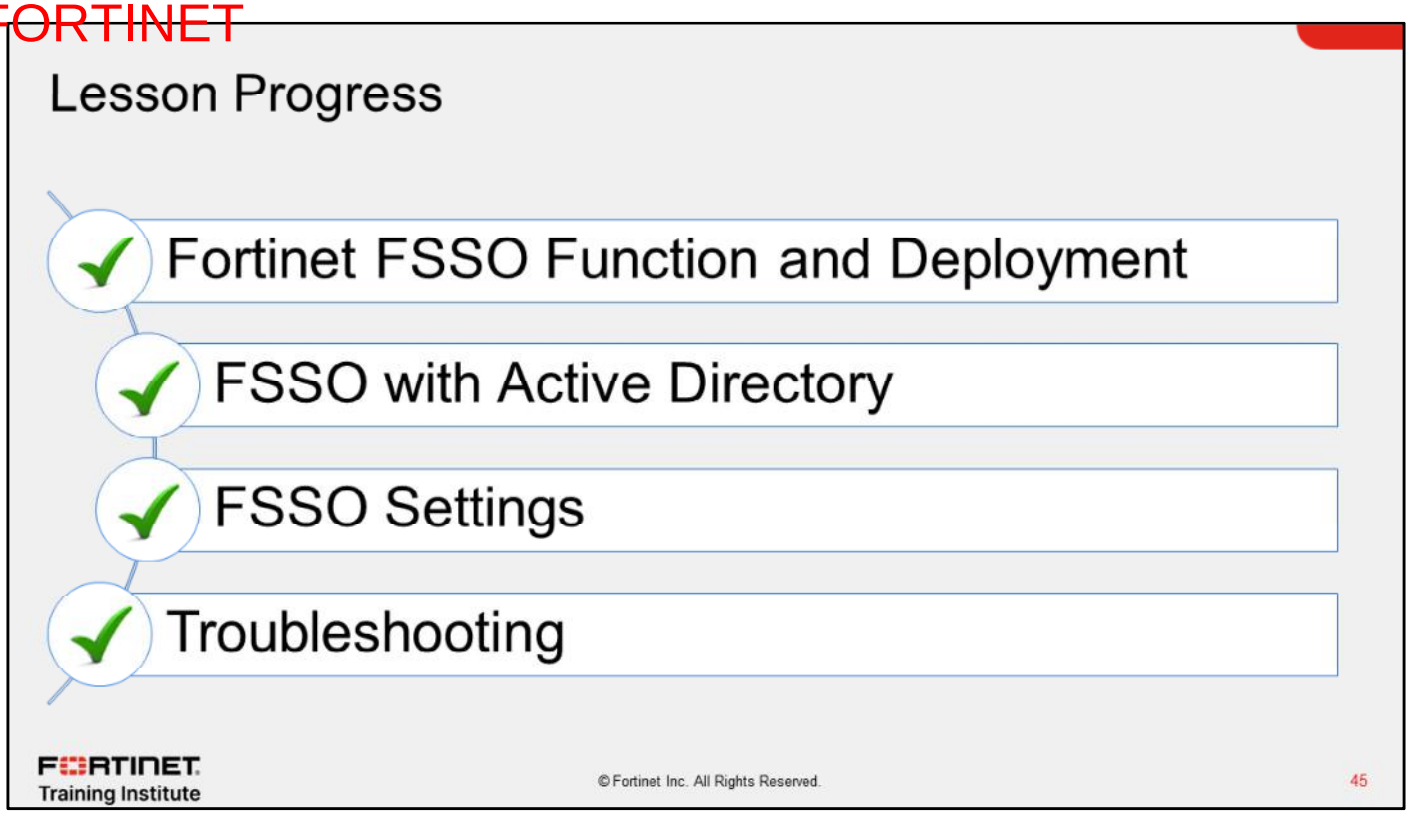
Knowledge Check

1. Which logging level shows the login events on the collector agent?
   - ✓ A. Information
   - B. Warning

2. The command `diagnose debug fsso-polling detail` displays information for which mode of FSSO?
   - ✓ A. Agentless polling
   - B. Collector agent-based polling

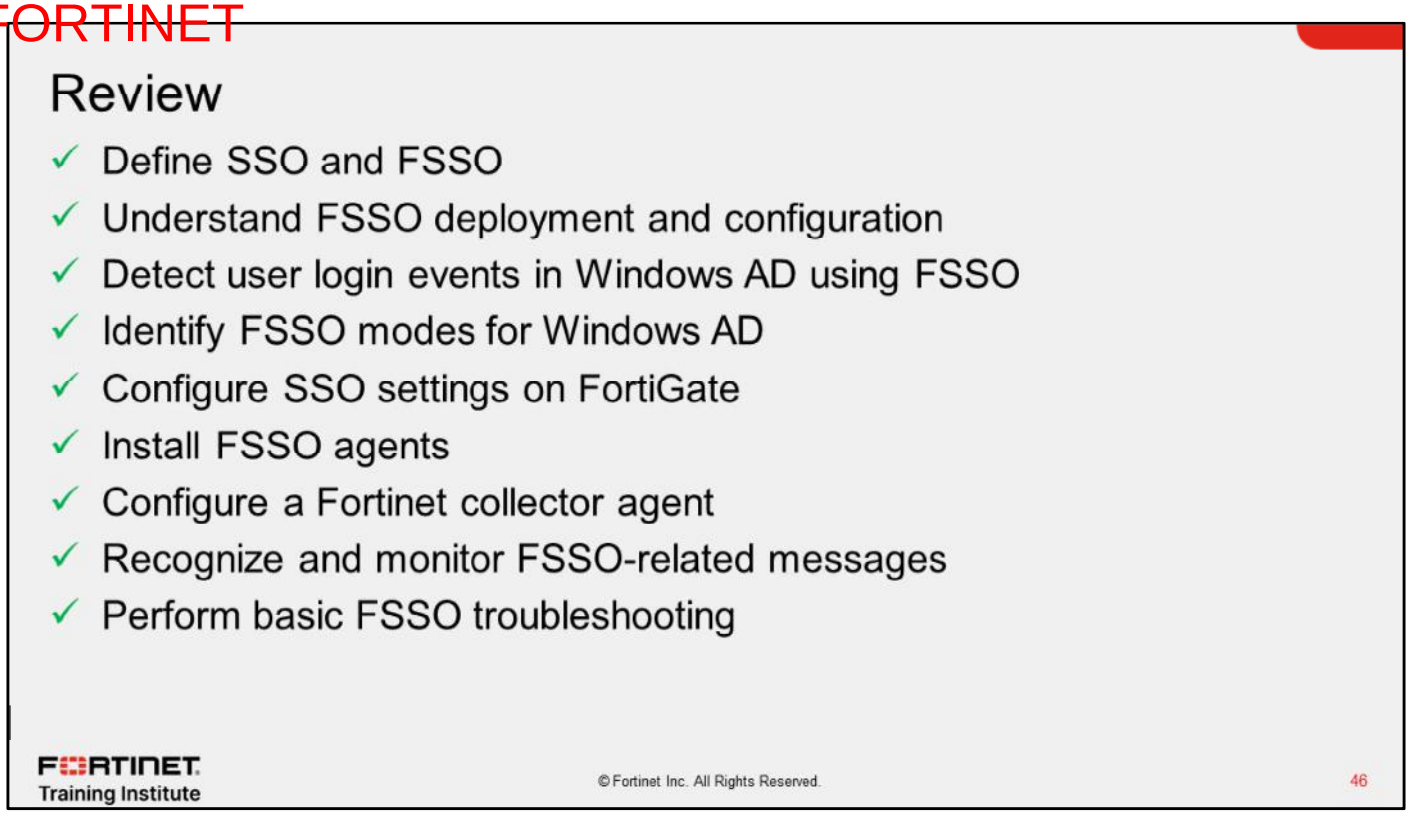
FORTINET Training Institute

44



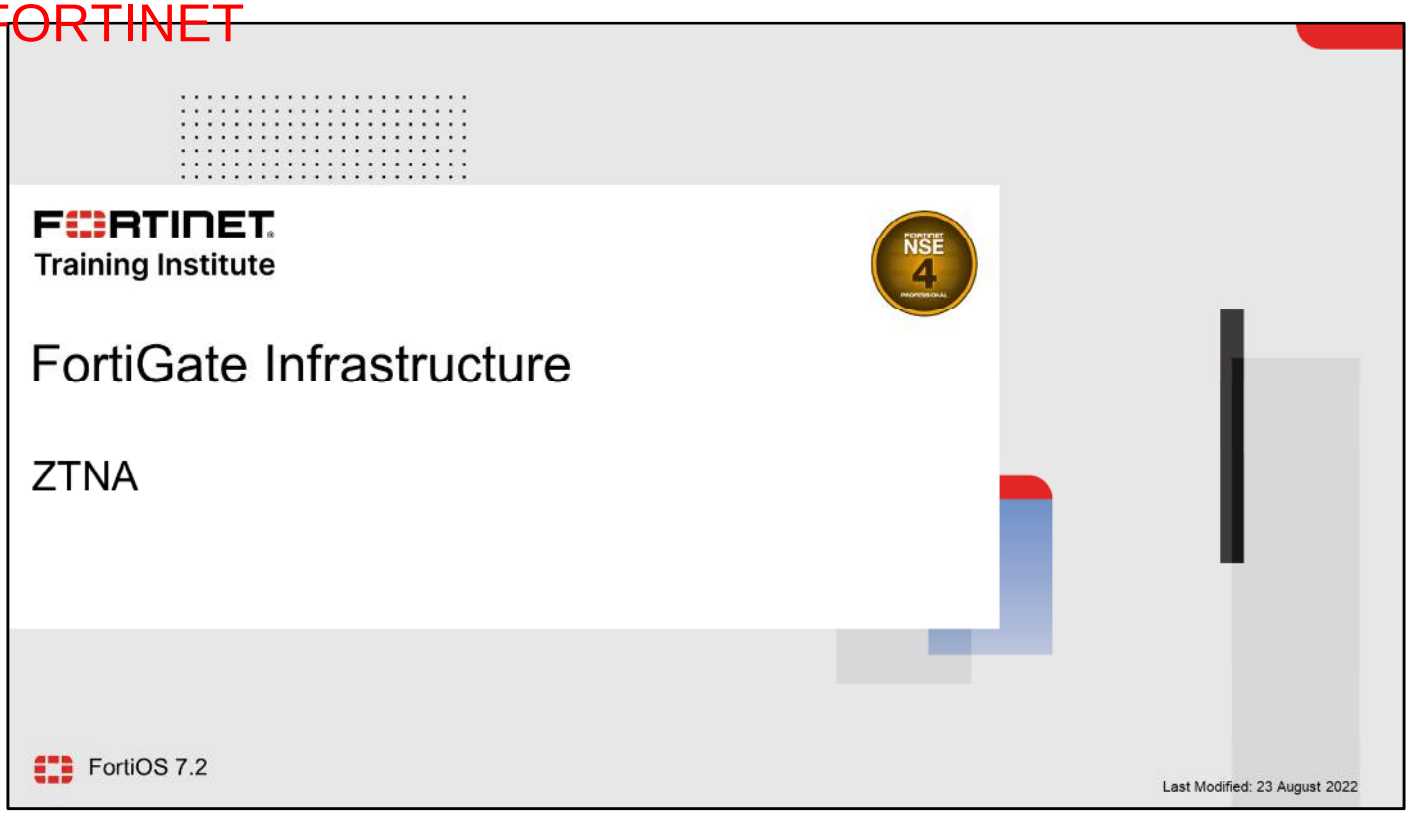
Congratulations! You have completed this lesson.

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

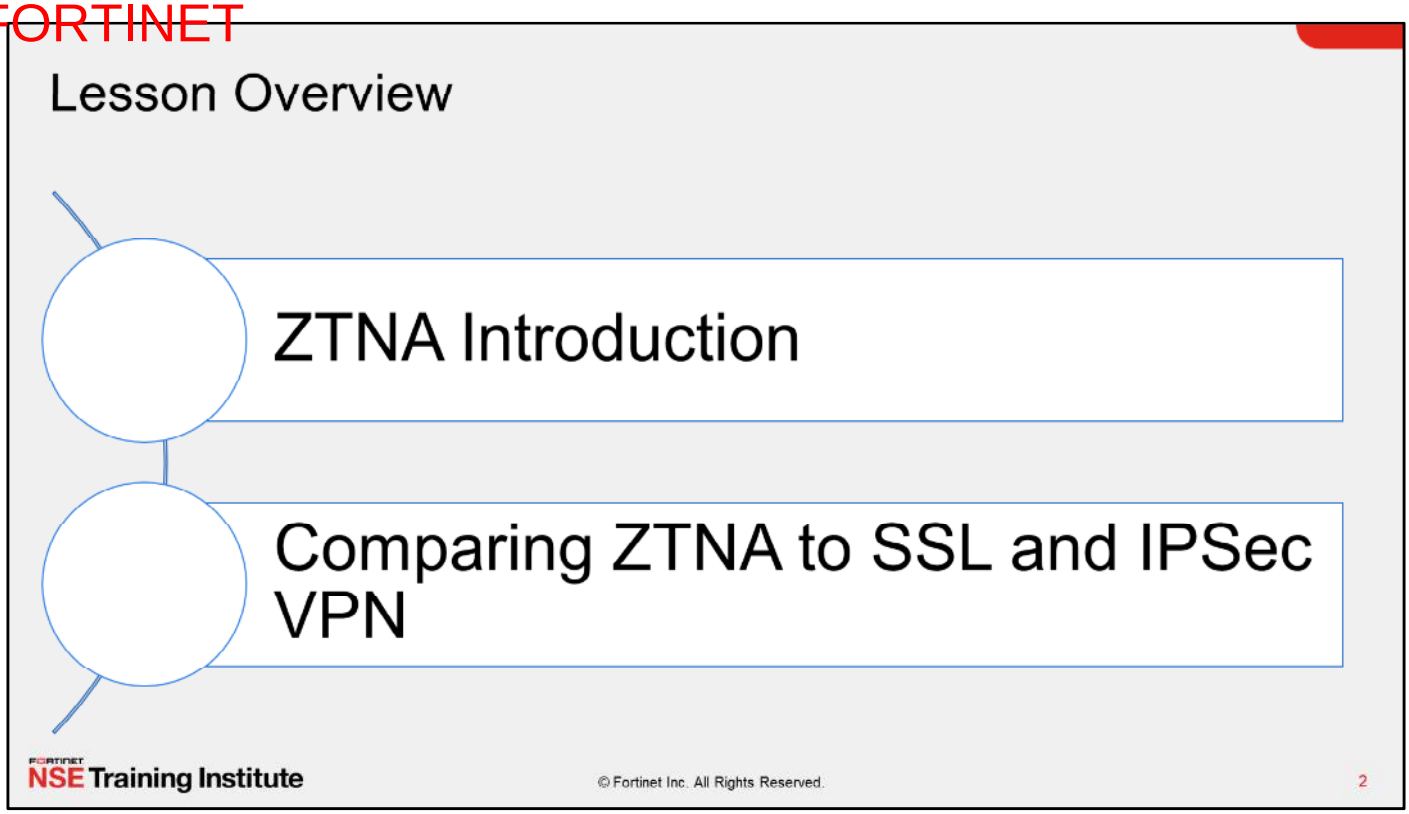


This slide shows the objectives that you covered in this lesson.

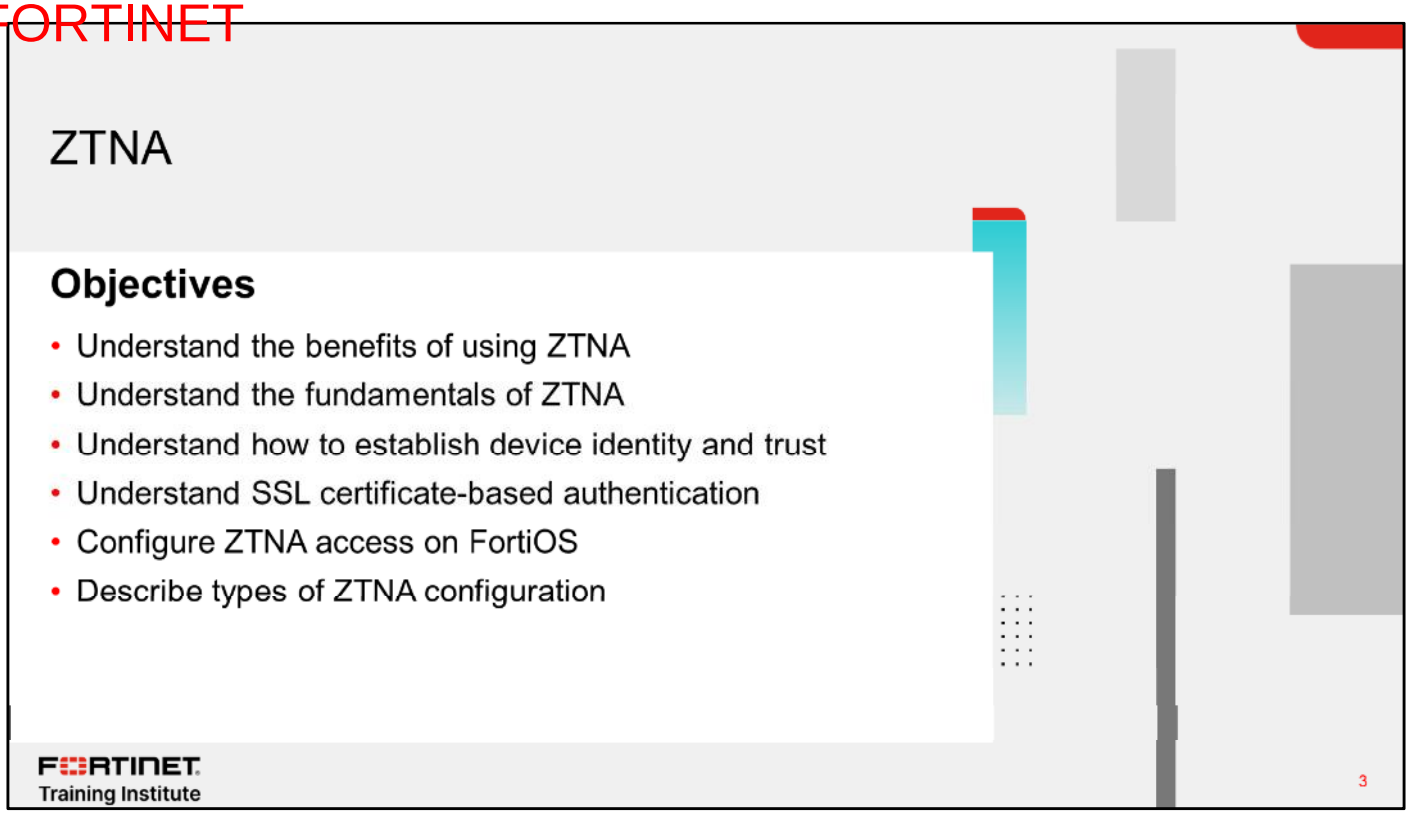
By mastering the objectives covered in this lesson, you learned how to use FSSO so that your users don't need to log in each time they access a different network resource.



In this lesson, you will learn about zero-trust network access (ZTNA).

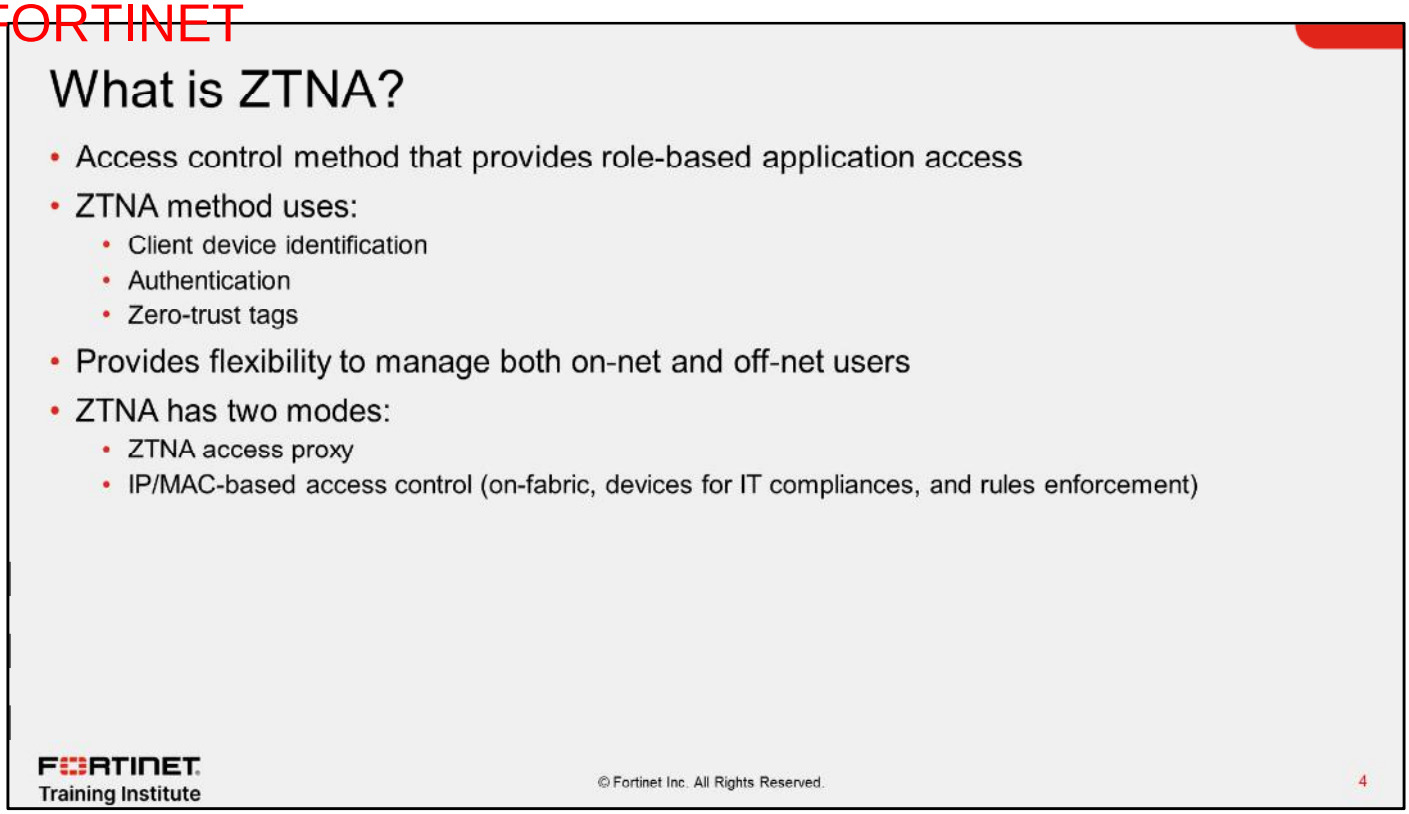


In this lesson, you will learn about the topics shown on this slide.



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

By demonstrating competence in ZTNA, you will be able to understand key ZTNA concepts and how to configure ZTNA.

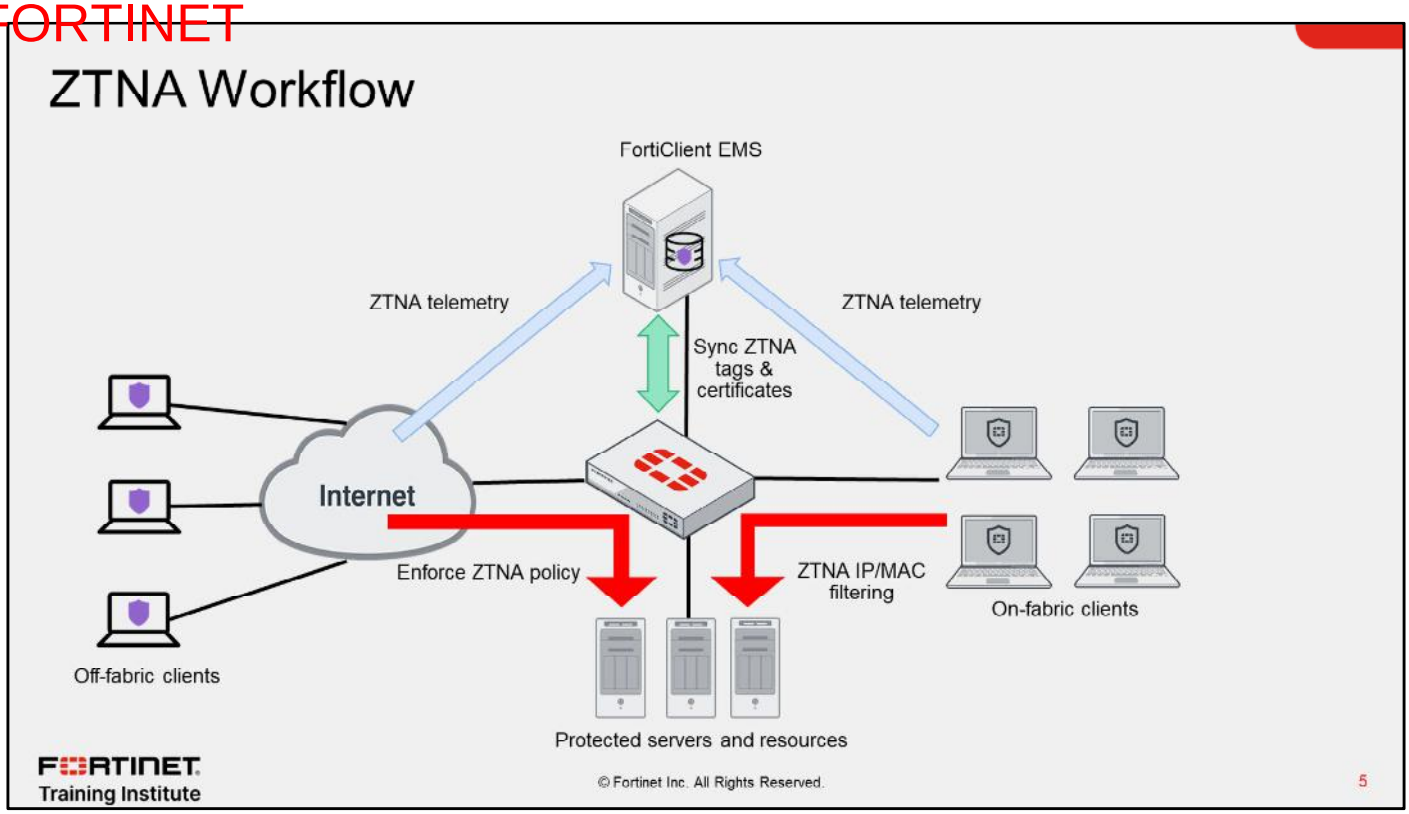


ZTNA is an access control method that uses client device identification, authentication, and zero-trust tags to provide role-based application access. ZTNA gives administrators the flexibility to manage network access for on-fabric local users and off-fabric remote users. ZTNA grants access to applications only after a device verification, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using zero-trust tags.

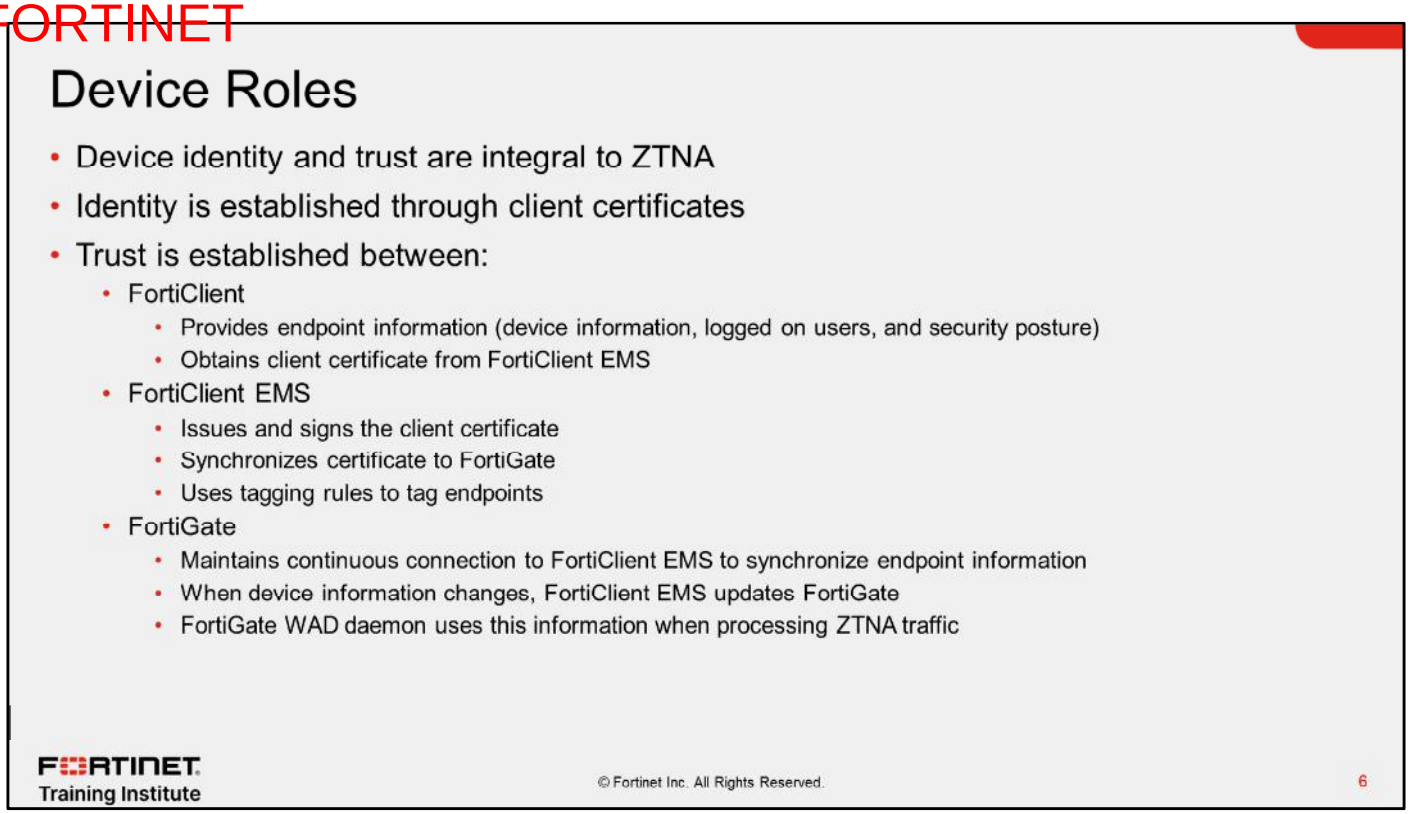
Traditionally, a user and a device have different sets of rules for on-fabric access and off-fabric VPN access to company resources. With a distributed workforce, and access that spans company networks, data centers, and the cloud, managing the rules can be complex. User experience is also affected when an organization needs multiple VPNs to access various resources.

ZTNA has two modes:

- ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.
- IP/MAC filtering uses ZTNA tags to provide an additional factor for identification, and a security posture check to implement role-based zero-trust access. IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for remote users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check to implement role-based zero-trust access. Firewall policies are configured that use ZTNA tags to control access between on-net devices and an internal webserver. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control.



This slide demonstrates ZTNA telemetry, tags, and policy enforcement. You configure ZTNA tag conditions and policies on FortiClient EMS. FortiClient EMS shares the tag information with FortiGate through Security Fabric integration. FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry. FortiGate can then use ZTNA tags to enforce access control rules to incoming traffic through ZTNA access.



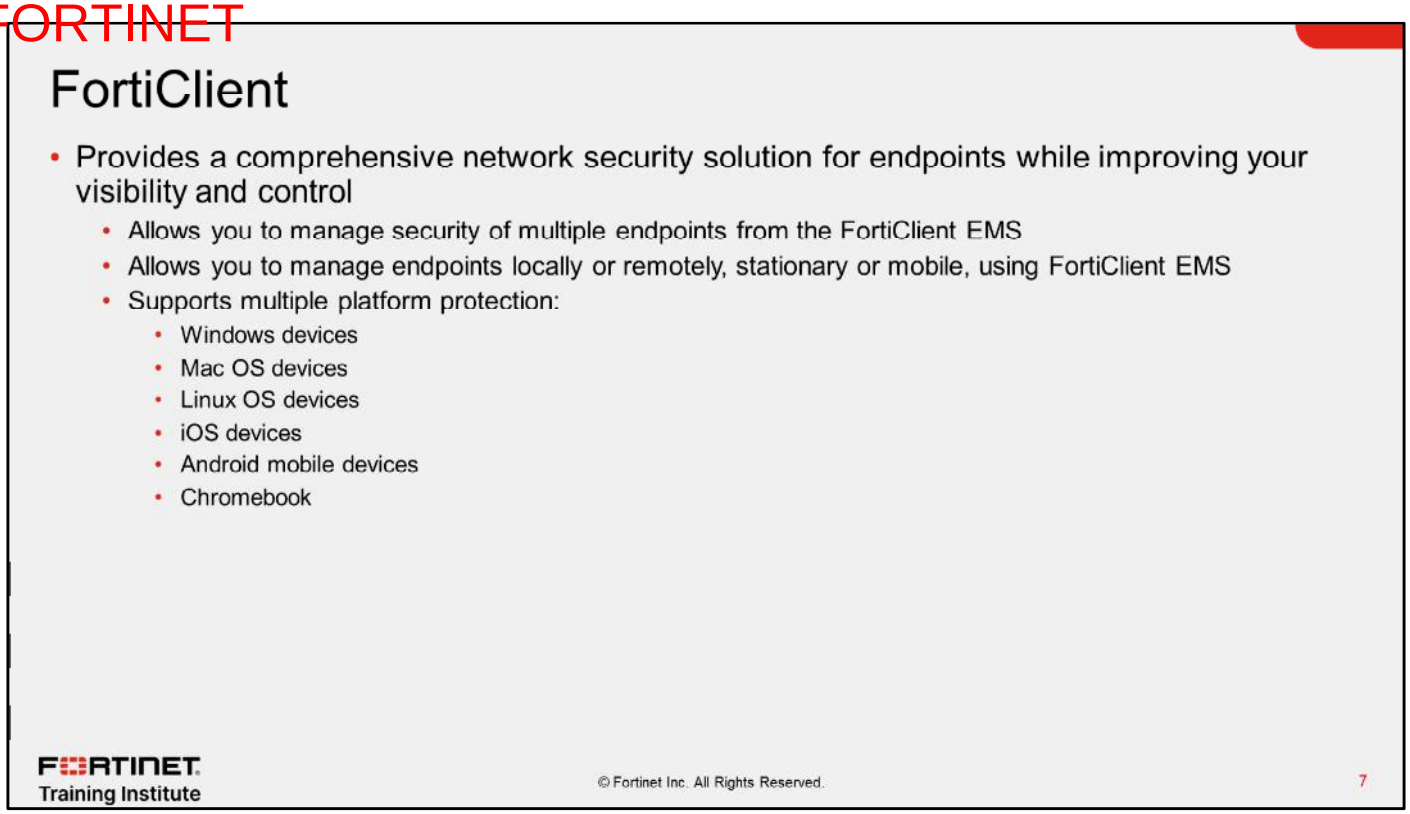
Device identity and trust are integral to ZTNA. Device identity is established through client certificates, and trust is established among FortiClient, FortiClient EMS, and FortiGate devices. In ZTNA, devices perform specific roles.

FortiClient provides the following information to FortiClient EMS when it registers:
- Device information (network details, operating system, model, and so on)
- Logged in user information
- Security posture (on-fabric and off-fabric, antivirus software, vulnerability status, and so on)

FortiClient also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) on its first attempt to connect to the access proxy. The client uses this certificate to identify itself to FortiGate.

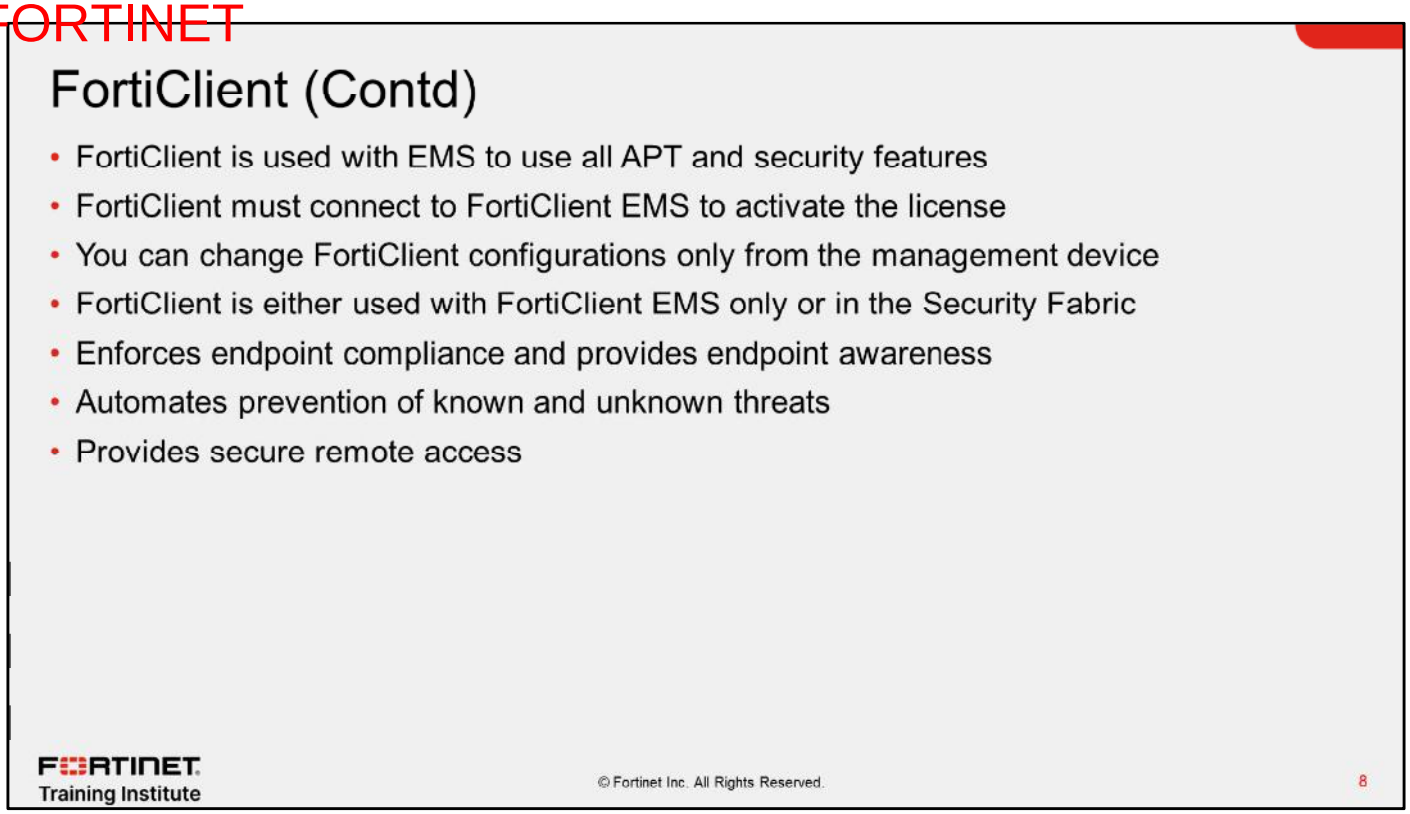
FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. FortiClient EMS then synchronizes the certificate with FortiGate. FortiClient EMS also shares its EMS ZTNA CA certificate with FortiGate, so that FortiGate can use it to authenticate the clients. FortiClient EMS uses zero-trust tagging rules to tag endpoints based on the information that it has on each endpoint. FortiClient EMS also shares the tags with FortiGate.

FortiGate maintains a continuous connection to FortiClient EMS to synchronize endpoint device information such as FortiClient UID, client certificate SN, FortiClient EMS SN, network details (IP and MAC address), and so on. When device information changes, such as when a client moves from on-fabric to off-fabric, or their security posture changes, FortiClient EMS updates the device information, and then updates the FortiGate.



FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linux-based desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

FortiClient enables every device—local or remote, stationary or mobile—to integrate with your FortiClient EMS and FortiGate. FortiClient supports Windows, Mac OS, Linux, iOS, Android mobile devices and Chromebook, and also integrates your home offices, mobile workers, and visiting partners.

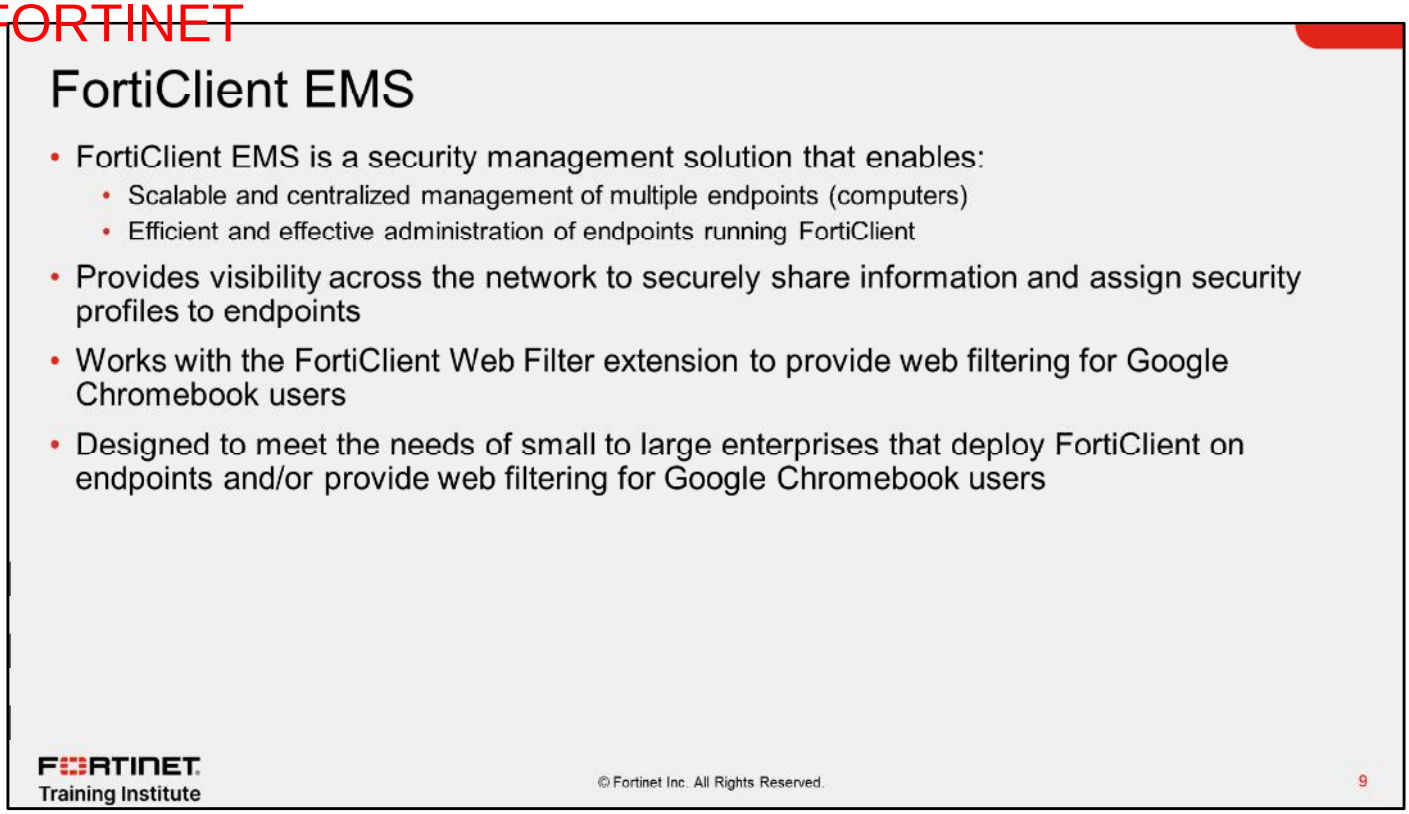


FortiClient must be used with FortiClient EMS. FortiClient must connect to FortiClient EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in FortiClient EMS. You cannot use any FortiClient features until FortiClient is connected to FortiClient EMS and licensed.

When FortiClient is connected only to FortiClient EMS, FortiClient EMS provisions and manages FortiClient. FortiClient EMS also sends zero-trust tagging rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. Only FortiClient EMS can control the connection between FortiClient and FortiClient EMS. However, FortiClient cannot participate in the Fortinet Security Fabric.

FortiClient in the security fabric connects to FortiClient EMS to receive a profile of configuration information as part of an endpoint policy. FortiClient EMS is connected to FortiGate to participate in the Security Fabric. FortiClient EMS sends FortiClient endpoint information to FortiGate. FortiGate can also receive dynamic endpoint group lists from FortiClient EMS and use them to build dynamic firewall policies.

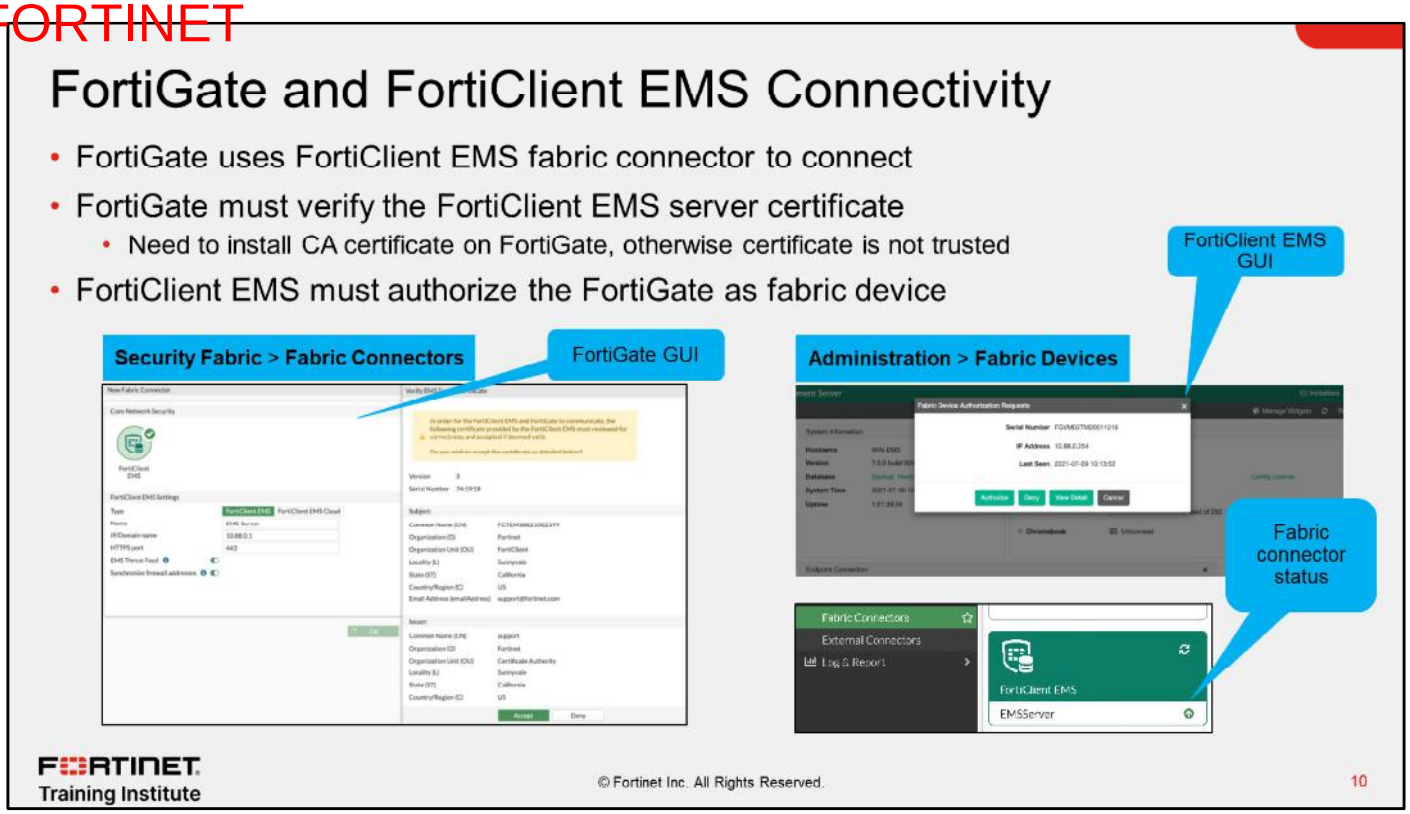
FortiClient also provides secure remote access to corporate assets through VPN.



FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.
FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:
- Remotely deploying FortiClient software to Windows computers
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile, and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

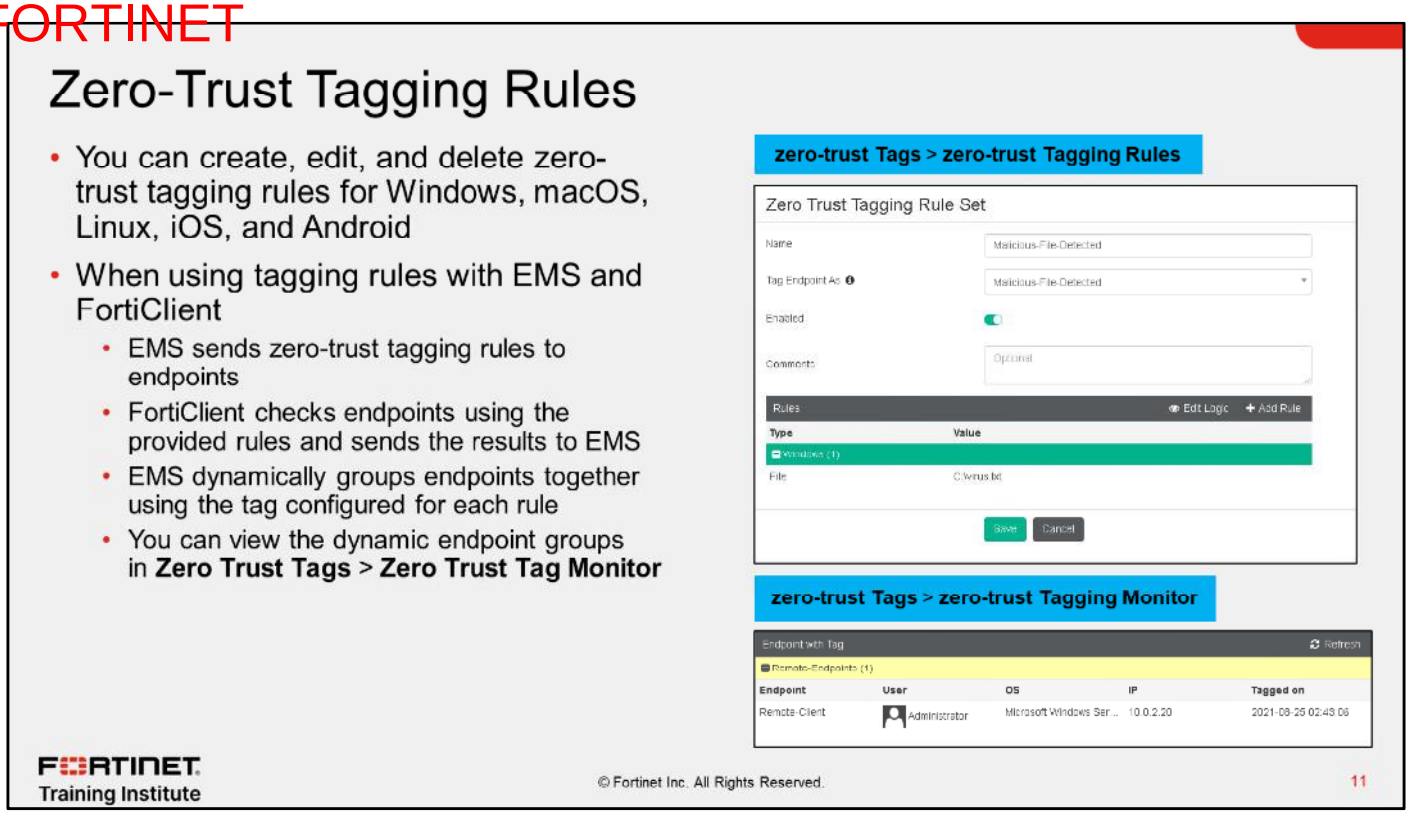
You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.



You can configure the on-premises FortiClient EMS connector on FortiGate by clicking **Security Fabric** > **Fabric Connectors**. After applying the FortiClient EMS settings, FortiGate must accept the FortiClient EMS server certificate. However, when you configure a new connection to FortiClient EMS server, the certificate might not be trusted. To resolve, you must manually export and install the root CA certificate on FortiGate. The FortiClient EMS certificate that is used by default for the SDN connection is signed by the CA certificate that is saved on the Windows server when you first install FortiClient EMS. This certificate is stored in the **Trusted Root Certification Authorities** folder on the server. For more information about exporting and installing certificates on FortiGate, refer to the *FortiOS-7.0.1 Administration Guide*.

Next, you must authorize FortiGate on FortiClient EMS. If you log in to FortiClient EMS, a pop-up window opens, requesting you to authorize FortiGate. If you do not log in, you can click **Administration** > **Devices**, select the FortiGate device, and then authorize it. Note that the FortiClient EMS connector status appears down until you authorize FortiGate on FortiClient EMS.

FortiGate automatically synchronizes ZTNA tags after it connects to FortiClient EMS.



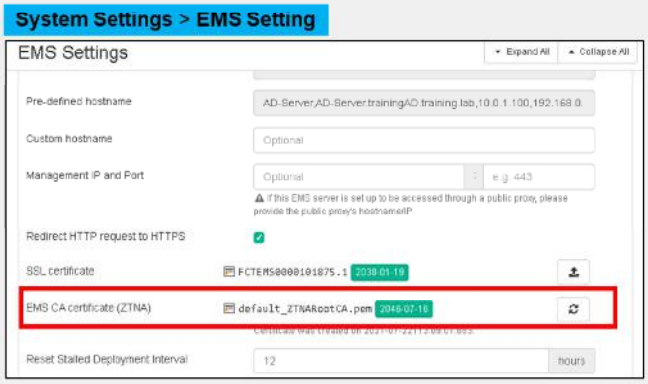
You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android endpoints. The following happens when using zero-trust tagging rules with FortiClient EMS and FortiClient:

- FortiClient EMS sends zero-trust tagging rules to endpoints through telemetry communication.
- FortiClient checks endpoints using the provided rules and sends the results to FortiClient EMS.
- FortiClient EMS receives the results from FortiClient.
- FortiClient EMS dynamically groups endpoints together using the tag configured for each rule. You can view the dynamic endpoint groups by clicking **Zero Trust Tags** > **Zero Trust Tag Monitor**.

Note that when the endpoint network changes or user login and logout events occur, FortiClient triggers an X-FFCK-TAG message to EMS, even if there are no tag changes. After FortiClient EMS receives the tags, it processes them immediately, and updates the FortiOS tags within five seconds of the REST API response. For other tag changes, FortiClient sends the information to FortiClient EMS regularly.

FortiClient EMS Certificate Management

- FortiClient EMS has a default root CA certificate
- ZTNA CA uses root certificate to sign CSRs from the FortiClient endpoints
- You can revoke and update root CA
  - Force updates to the FortiGate and FortiClient endpoints by generating new certificates
- FortiClient EMS manages individual client certificates



FORTINET Training Institute

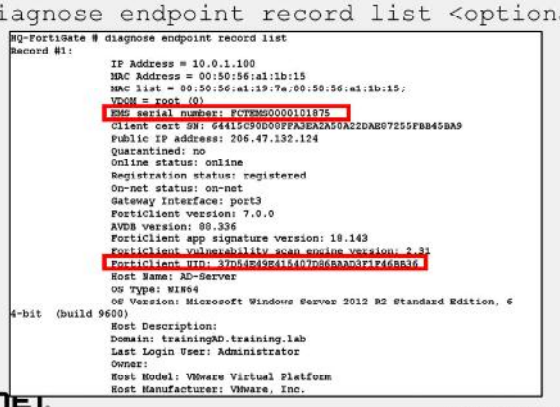
12

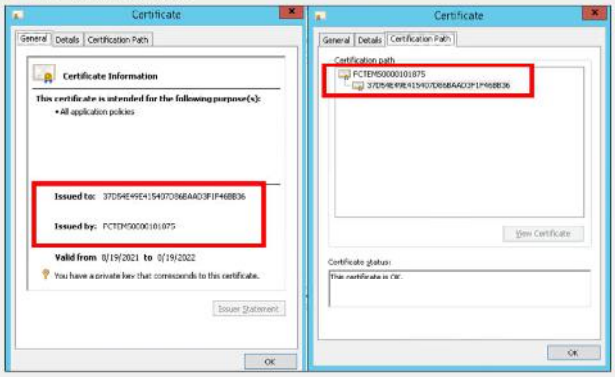
FortiClient EMS has a **default_ZTNARootCA** certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client. FortiClient EMS can also manage individual client certificates. You can also revoke the certificate that is used by the endpoint when certificate private keys show signs of being compromised. Click **Endpoint** > **All Endpoints**, select the client, and then click **Action** > **Revoke Client Certificate**.

Do not confuse the FortiClient EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by FortiClient EMS for HTTPS access and fabric connectivity to the FortiClient EMS server.

FortiClient EMS Certificate Management (Contd)

- On Windows endpoints, FortiClient automatically installs certificates in the certificate store
  - Certificate information, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate
  - **Certificates** > **Personal** > **Certificates**
- You can verify by CLI command on FortiGate
  - `diagnose endpoint record list <optional IP address>`





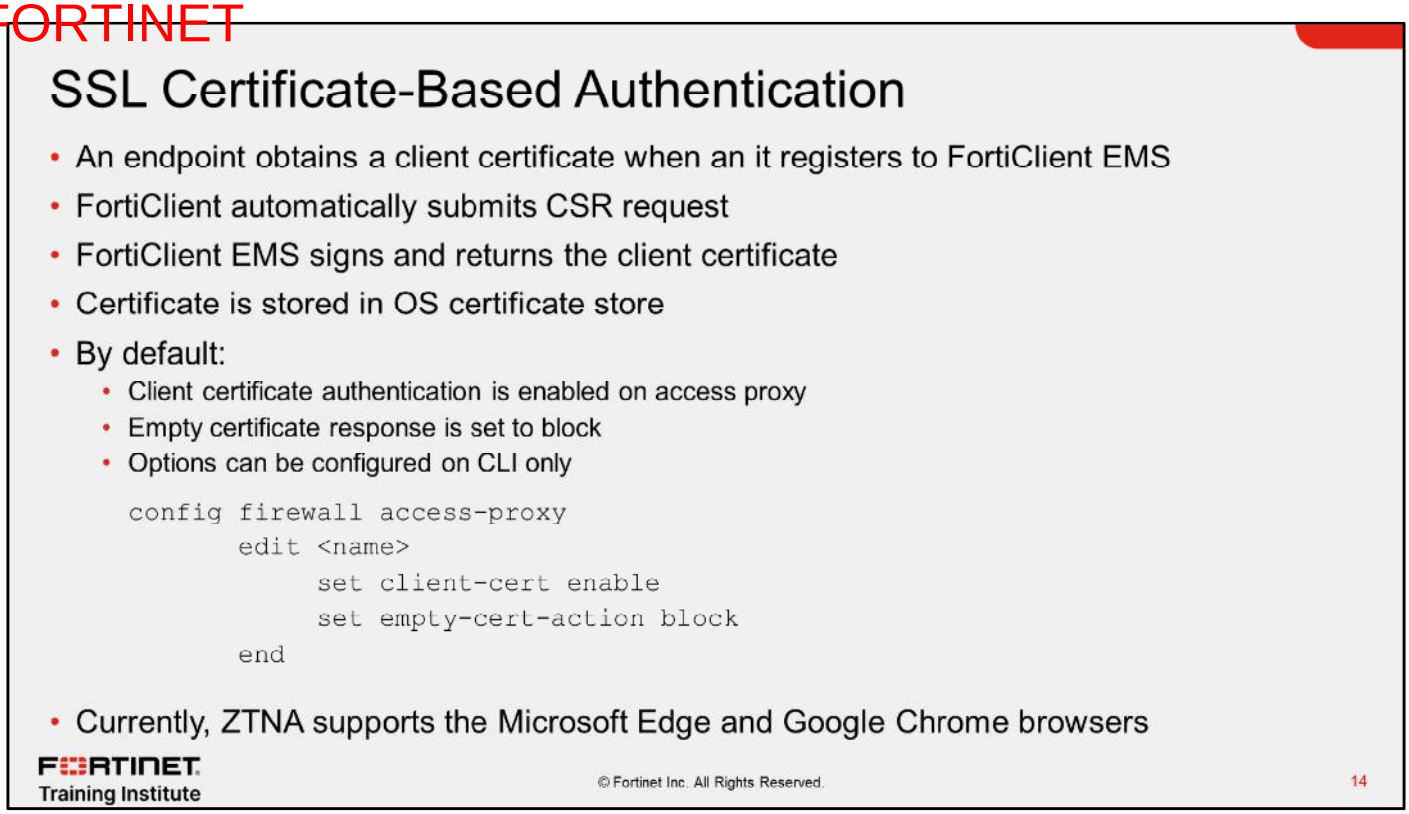
FORTINET Training Institute

13

In Windows, FortiClient automatically installs certificates in the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate. To locate certificates on other operating systems, consult the vendor documentation.

You can use the CLI command `diagnose endpoint record list` a to verify the presence of a matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on the FortiGate. If any of the information is missing or incomplete, client certificate authentication might fail because FortiClient cannot locate the corresponding endpoint entry.

This slide shows that client certificate information is synchronized with FortiGate.

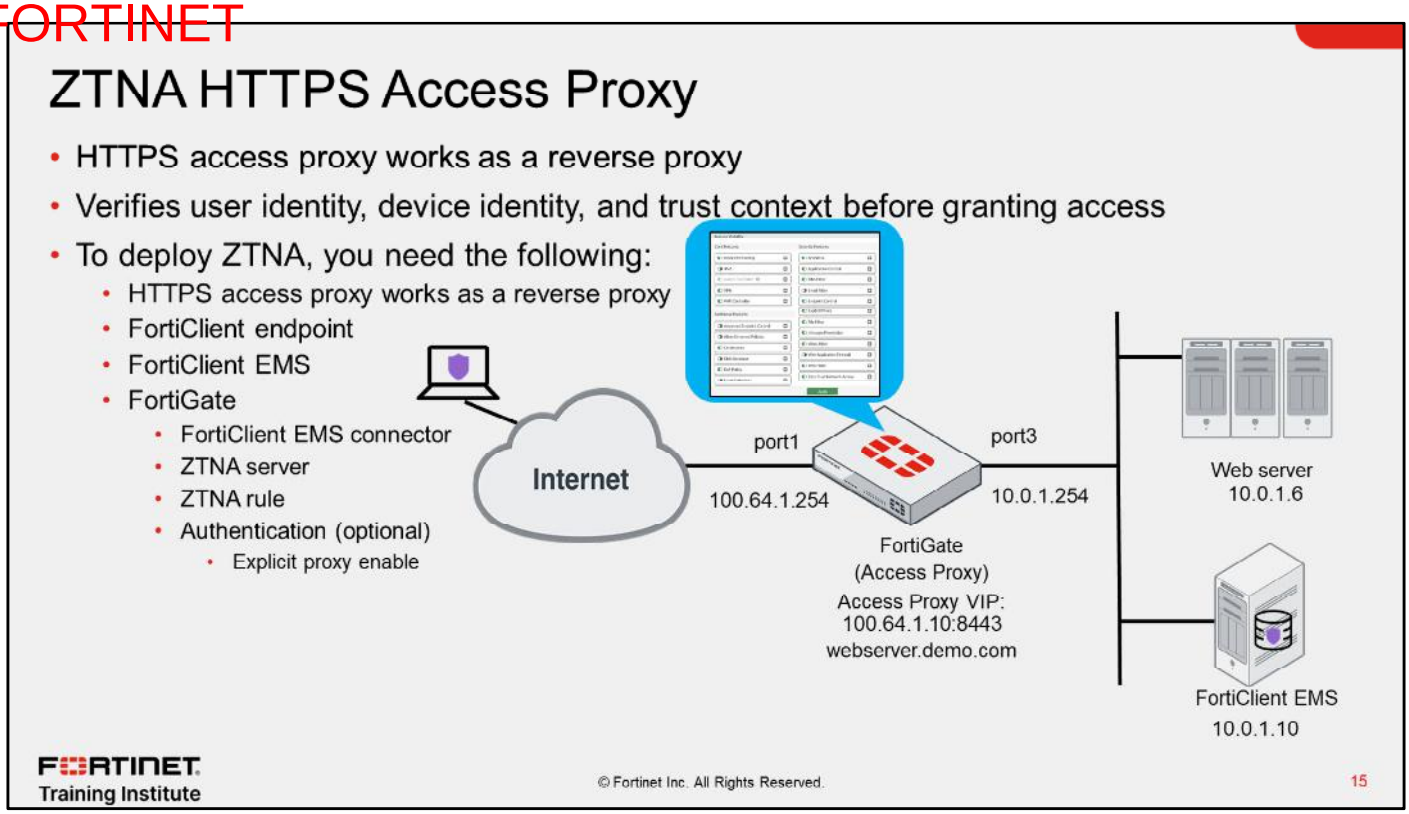


Endpoint obtains a client certificate when it registers to FortiClient EMS. FortiClient automatically submits a CSR request and the FortiClient EMS signs and returns the client certificate. This certificate is stored in the operating system certificate store for subsequent connections. The endpoint information is synchronized between FortiGate and FortiClient EMS. When an endpoint disconnects or is unregistered from FortiClient EMS, its certificate is removed from the certificate store and revokes on FortiClient EMS. The endpoint obtains a certificate again when it reconnects to the FortiClient EMS.

By default, client certificate authentication is enabled on the access proxy, so when FortiGate receives the HTTPS request, the FortiGate WAD process challenges the client to identify itself with its certificate. The FortiGate makes a decision based on specific possibilities.

If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:
- If the client UID and certificate SN match the record on FortiGate, the client is allowed to continue with the ZTNA proxy rule processing.
- If the client UID and certificate SN do not match the record on FortiGate, the client is blocked from further ZTNA proxy rule processing.

If the client cancels and responds with an empty client certificate, the client is allowed to continue with ZTNA proxy rule processing when you can set `empty-cert-action` to `accept`. If `empty-cert-action` is set to `block`, FortiGate blocks the client from further ZTNA proxy rule processing.



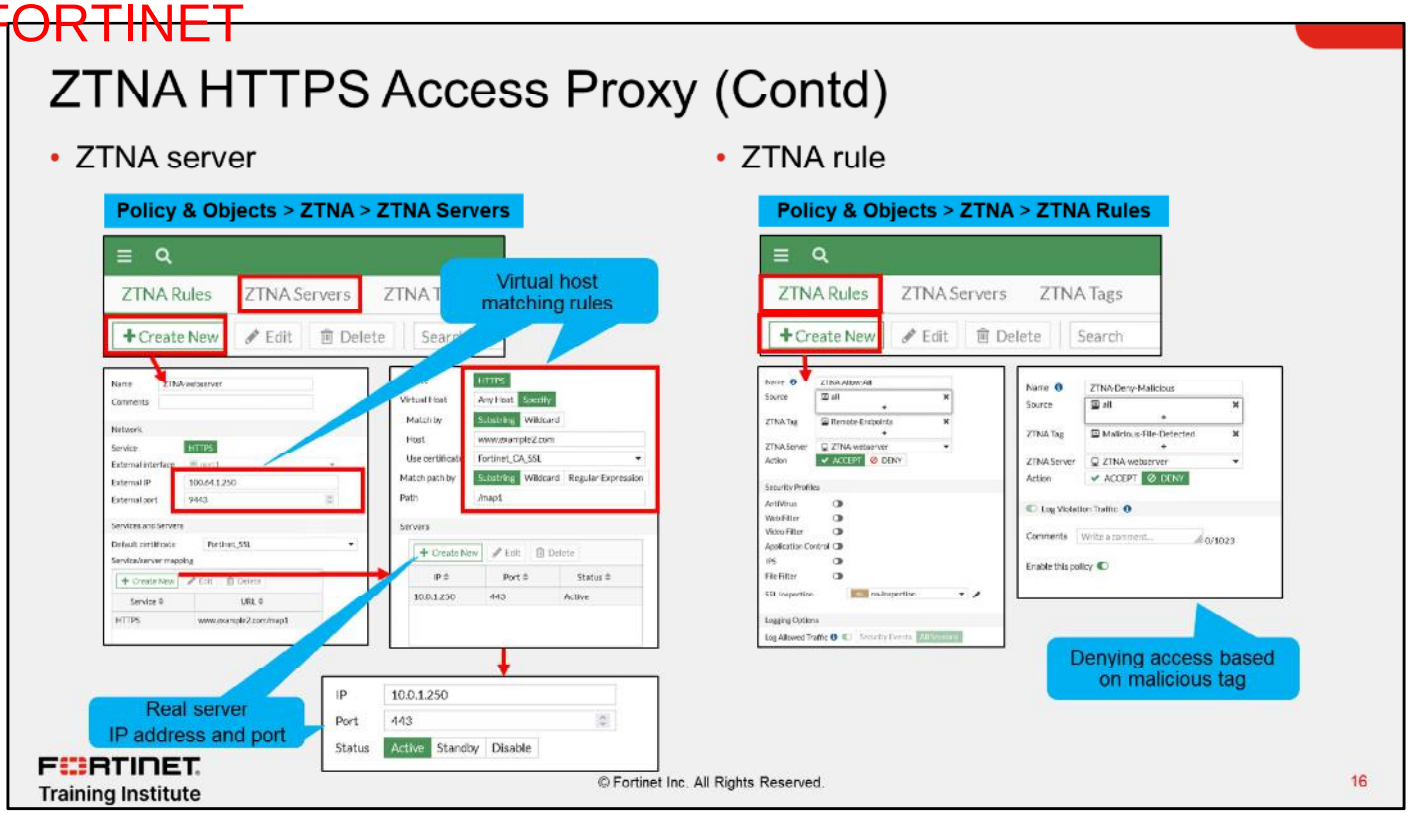
The FortiGate HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a web page hosted by the protected server, the address resolves to the FortiGate access proxy VIP (`100.64.1.10:8443`), as shown on this slide. FortiGate proxies the connection and takes steps to authenticate the device. It prompts the user for the endpoint certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the FortiClient EMS.

To enable ZTNA on the GUI, you must click **System** > **Feature Visibility**, and then enabling **Zero Trust Network Access**.

ZTNA configuration on FortiGate requires the following configuration:

- FortiClient EMS adds a fabric connector in the Security Fabric. FortiGate maintains a continuous connection to the EMS server to synchronize endpoint device information, and also automatically synchronizes ZTNA tags. You can create groups and add tags to use in the ZTNA rules and firewall policies.
- The ZTNA server defines the access proxy VIP and the real servers that clients connect to. You can also enable authentication.
- A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. You can configure security profiles to protect this traffic.

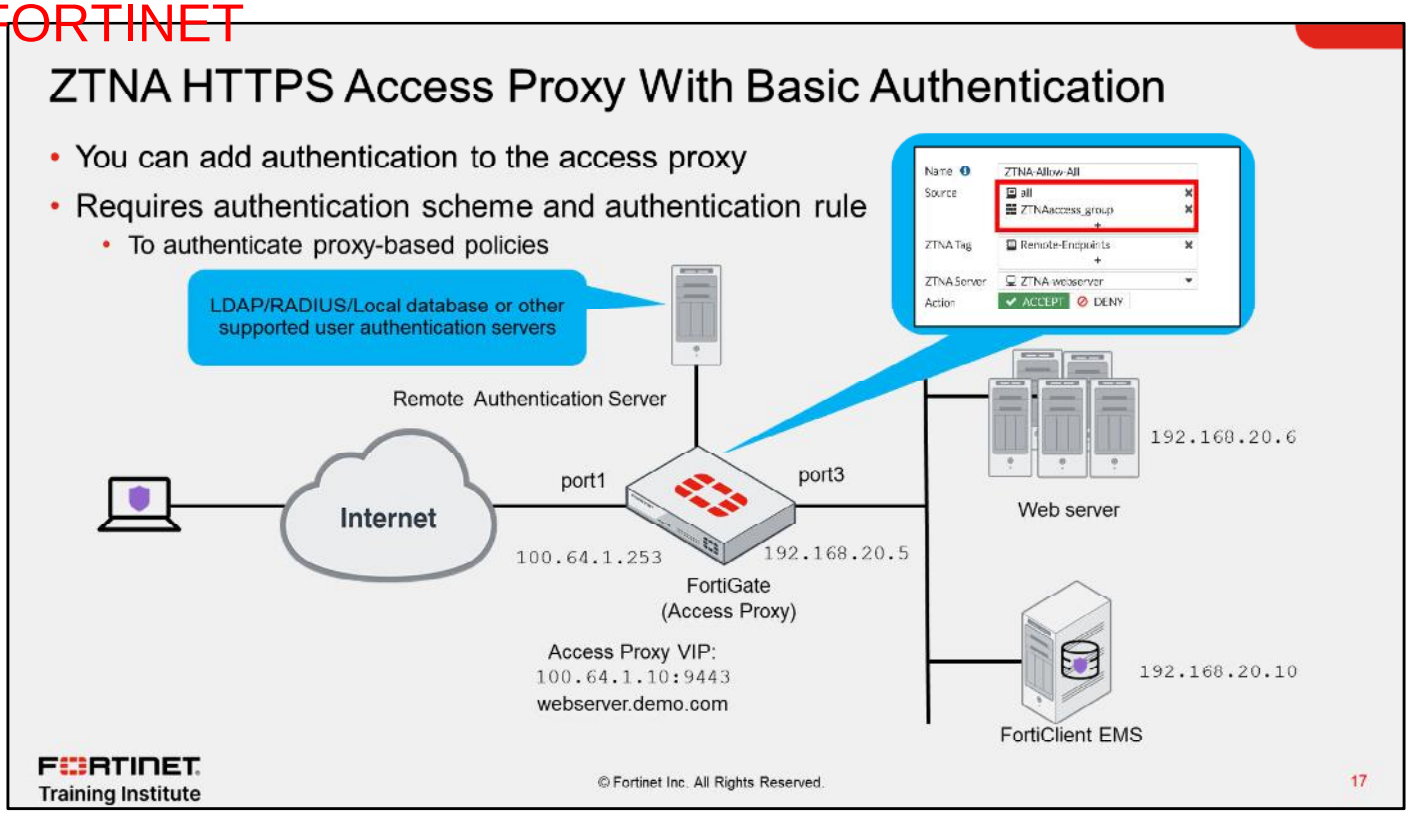
You can also configure authentication to the access proxy. ZTNA supports basic HTTP and SAML methods.



After you configure FortiClient EMS as the fabric connector and you sync ZTNA tags with FortiGate, you must create a ZTNA server or access proxy. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service and server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic.

Note that UTM processing of the traffic happens at the ZTNA rule.

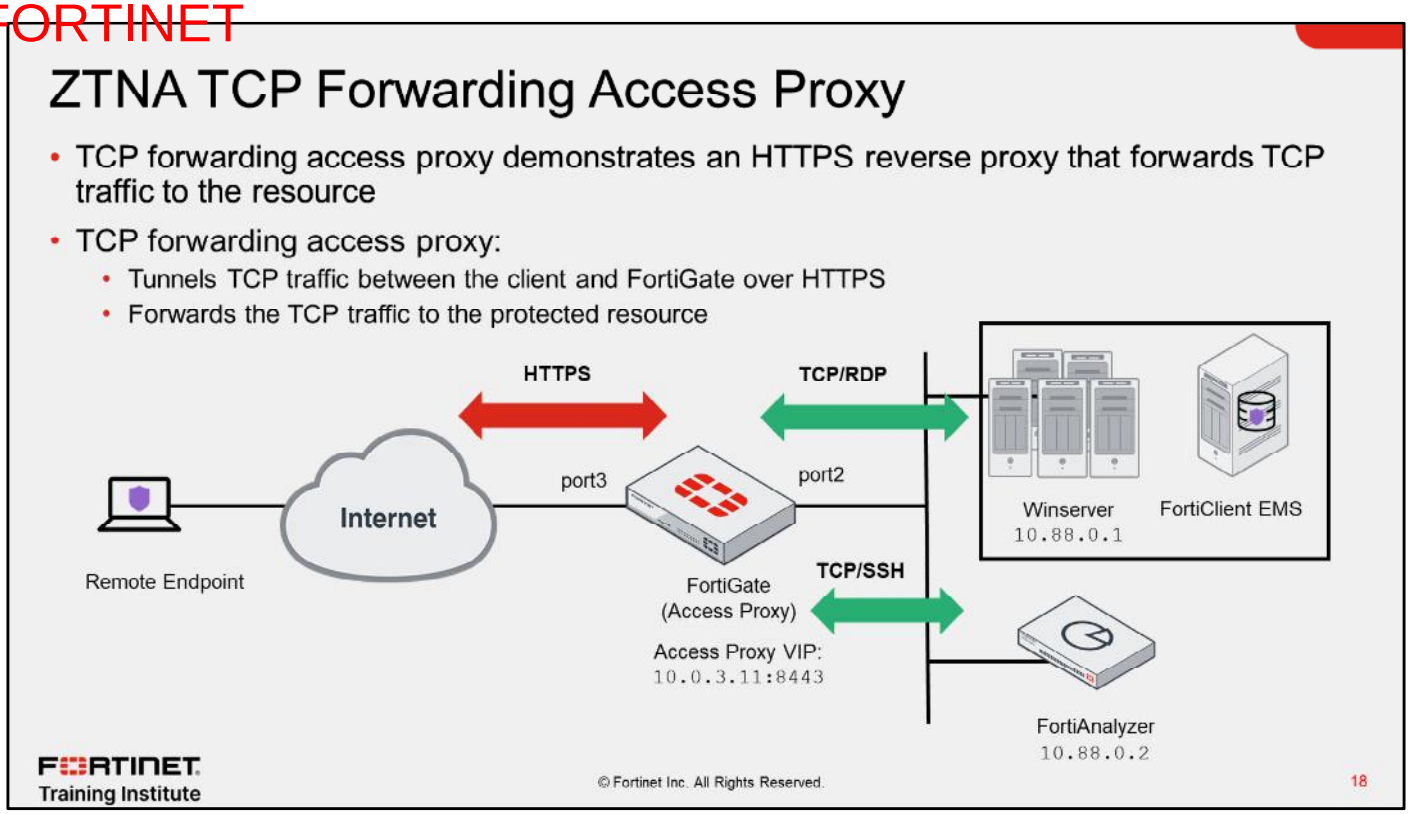


You can add authentication to the access proxy, which requires you to configure an authentication scheme and authentication rule on the FortiGate CLI. You use authentication schemes and authentication rules to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. ZTNA supports basic HTTP and SAML methods. Each method has additional settings to define the data source. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they are with basic authentication. After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to.

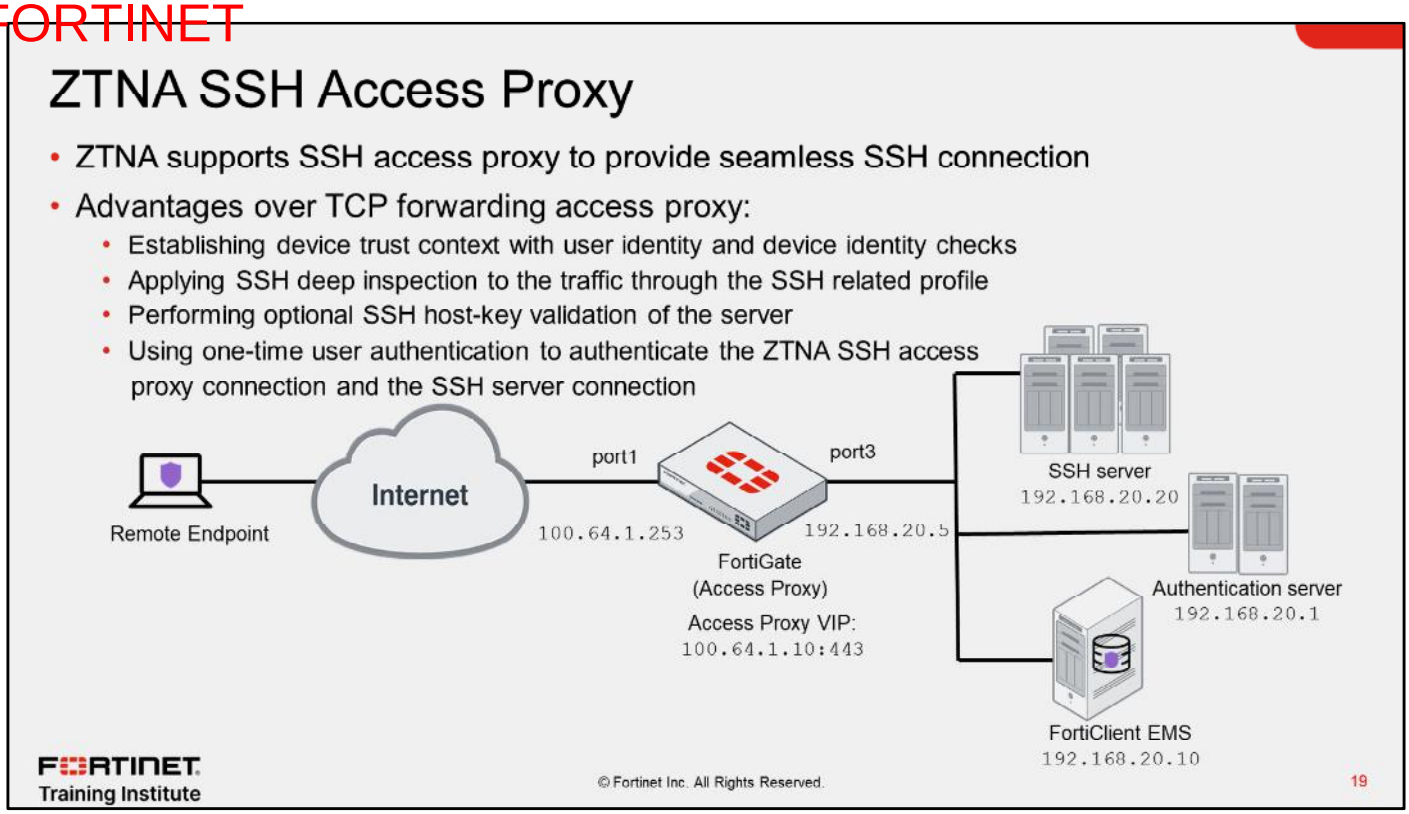
In the ZTNA rule and proxy policy, you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy. This slide shows the ZTNA rule example that user group **ZTNAaccess_group** was added to the authentication configuration after the authentication scheme and authentication rule were added to FortiGate.



In the example shown on this slide, a TCP forwarding access proxy (TFAP) is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

RDP access is configured to Winserver, and SSH access to FortiAnalyzer. The topology shown on this slide uses IP address `10.0.3.11` and port-8443 for the external access proxy VIP.

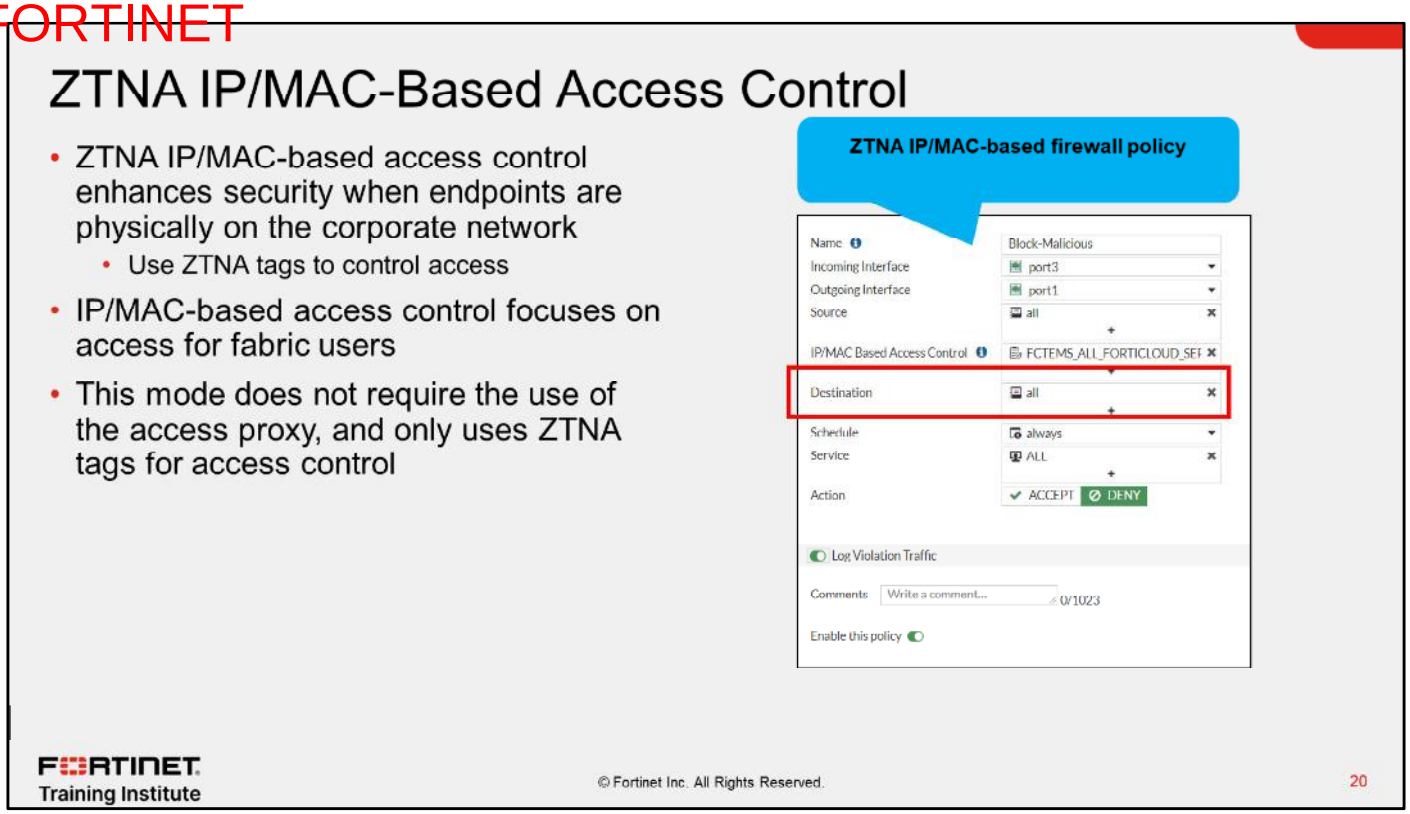
You can also add authentication and a security posture check for TCP Forwarding Access Proxy, which you learned about earlier in this lesson.



You can configure ZTNA with an SSH access proxy to provide a seamless SSH connection to the server.

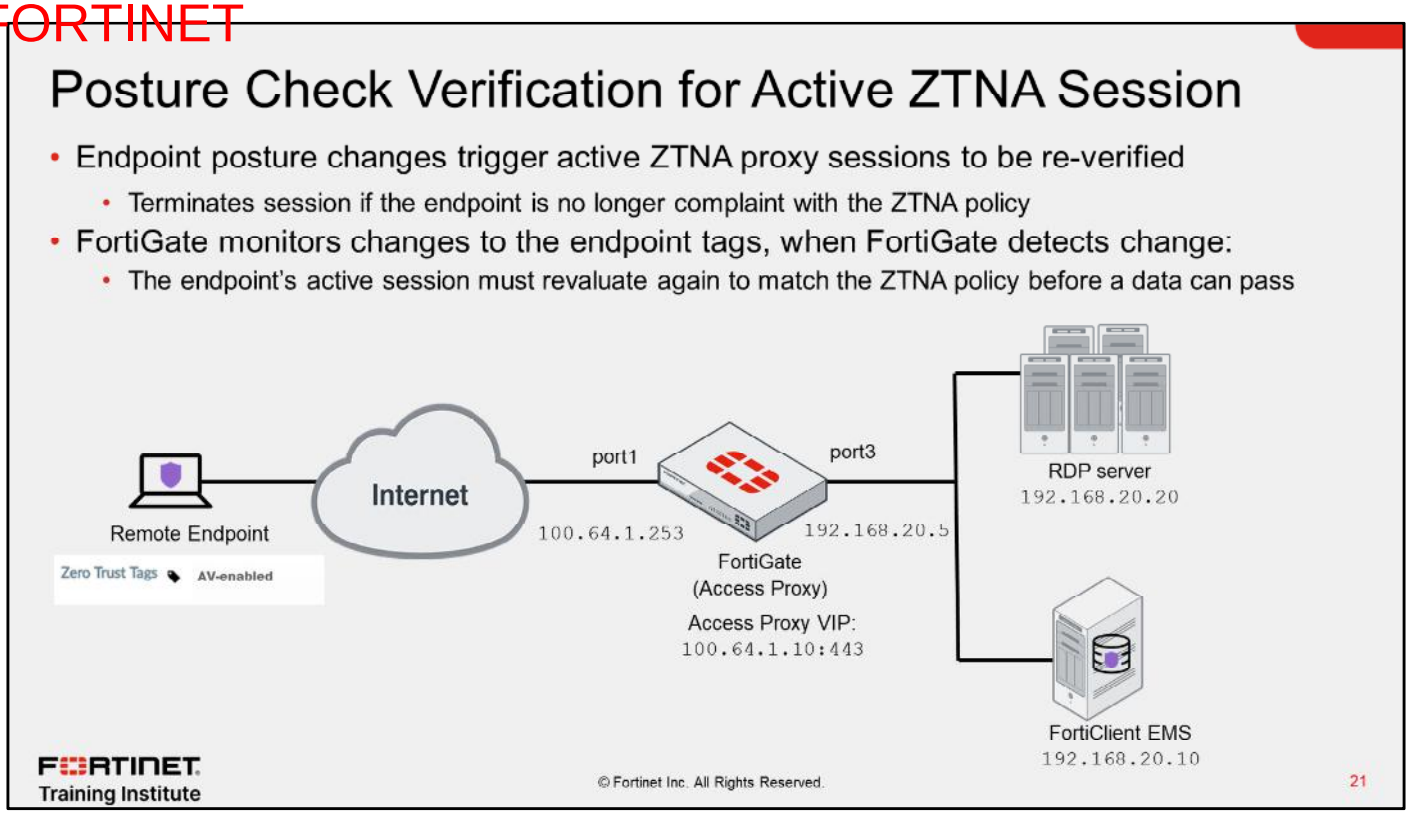
Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:
- Establishing device trust context with user identity and device identity checks
- Applying SSH deep inspection to the traffic through the SSH related profile
- Performing optional SSH host-key validation of the server
- Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection

To act as a reverse proxy for the SSH server, FortiGate must perform SSH host-key validation to verify the identity of the SSH server. FortiGate does this by storing the public key of the SSH server in its SSH host-key configurations. When endpoint makes a connection to the SSH server, if the public key matches one that is used by the server, then the connection is established. If there is no match, then the connection fails.



ZTNA IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for fabric users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check, to implement role-based zero-trust access. Firewall policies are configured that use ZTNA tags to control access between on-net devices and an internal webserver. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control.

The example firewall policy on this slide uses the existing tag to control access. Traffic is denied to the internet when the FortiClient endpoint is tagged with **FCTEMS_ALL_FORTICLOUD_Malicious**.



Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy. The FortiGate monitors changes to the endpoint tags that are updated by FortiClient EMS. When a change is detected, the endpoint's active ZTNA sessions must match the ZTNA policy again before data can pass.

Note that changes to the ZTNA policy, such as changing the ZTNA tag matching logic, will also trigger re-verification of the client device against the policy.

In the example on this slide, a ZTNA rule is configured to allow access for endpoints that have the *AV-enabled* tag. After an RDP sessions is established, Windows antivirus is disabled on the remote endpoint. The FortiGate re-verifies the session and the active RDP session is removed from the FortiGate session table, causing the RDP session to be disconnected.

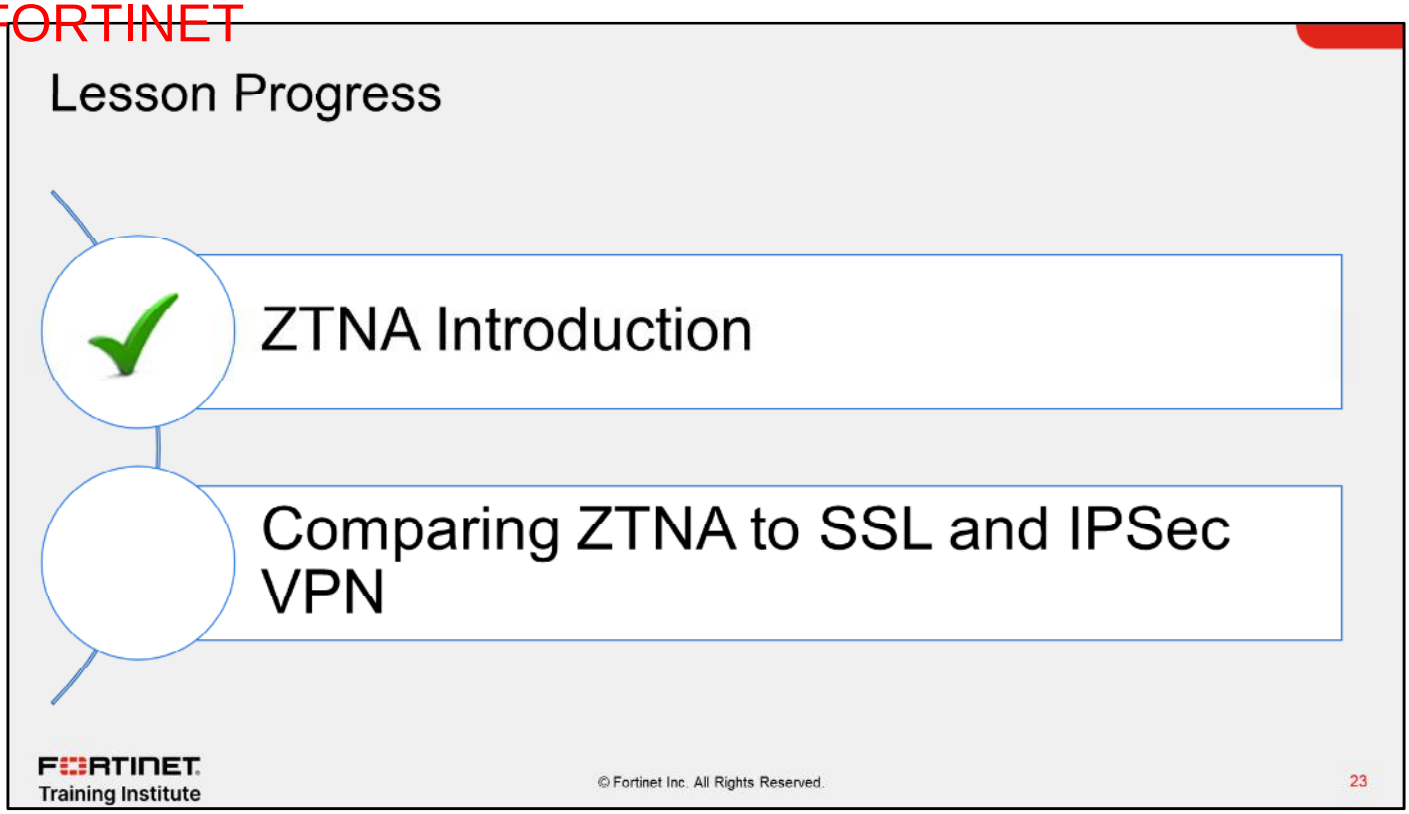
Knowledge Check

1. Which component issues and signs the client certificate?
✓A. FortiClient EMS
B. FortiClient

2. Which internet browser supports Fortinet ZTNA?
A. Firefox
✓B. Chrome

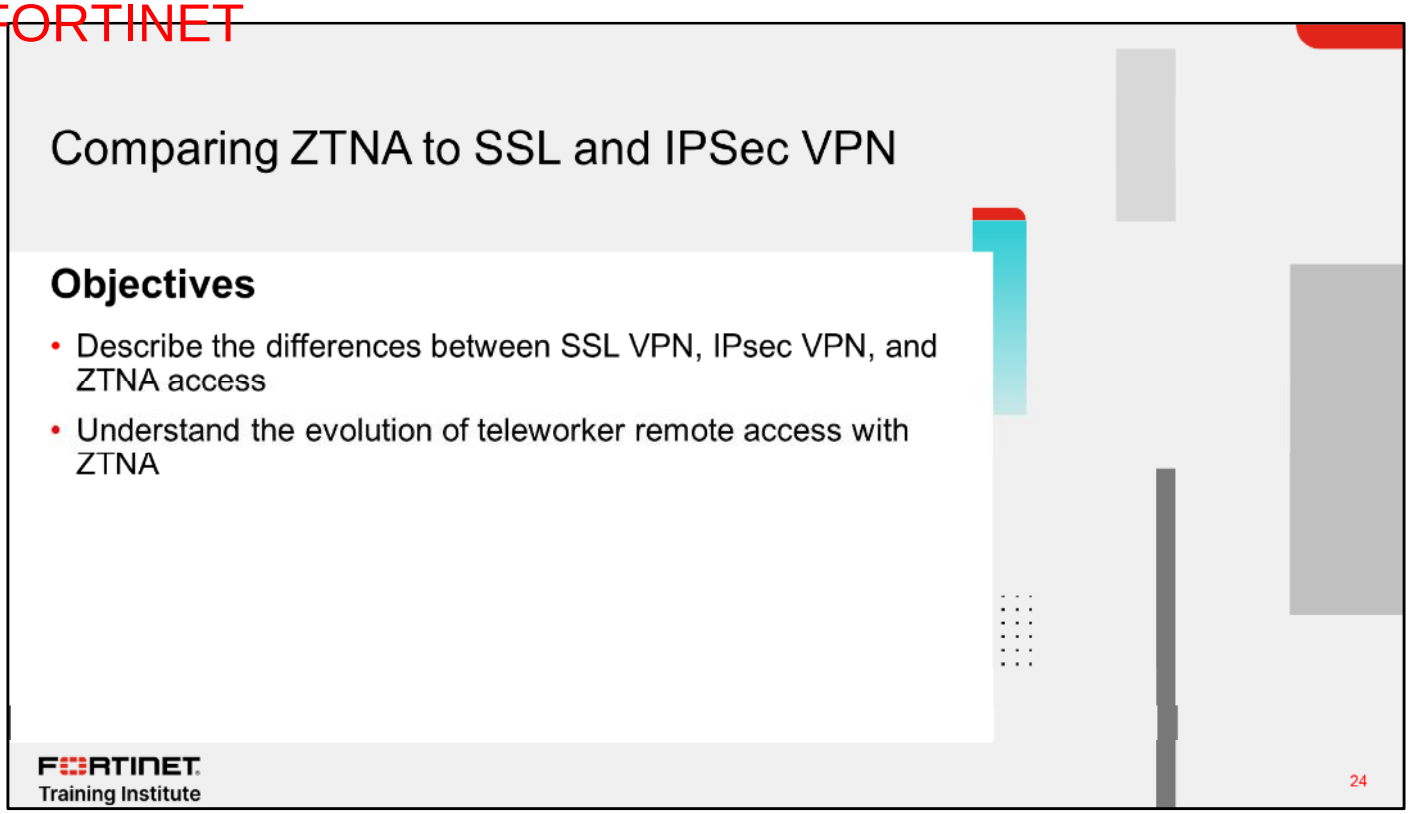
FORTINET Training Institute

22



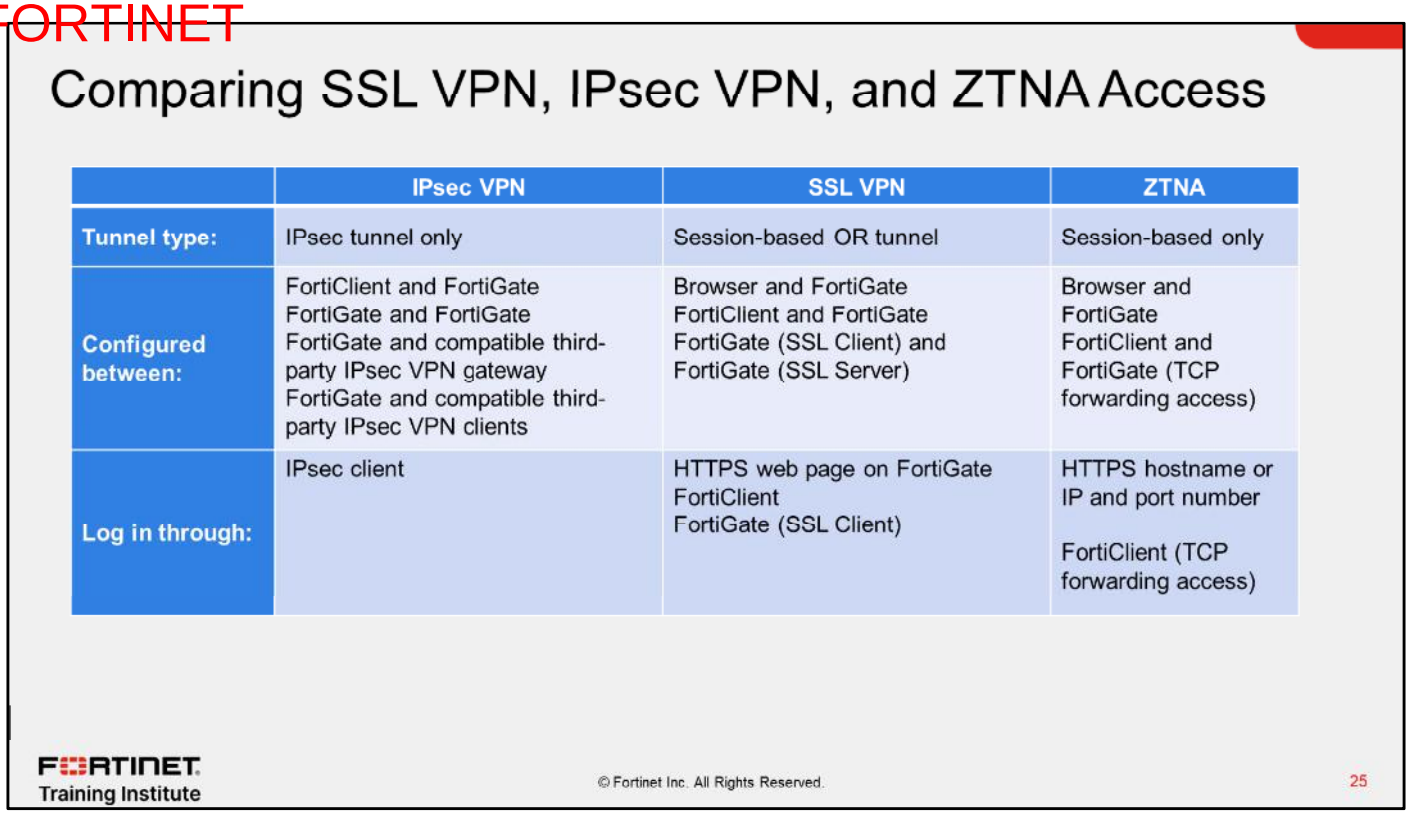
Good job! You now understand key ZTNA concepts and how to configure ZTNA

Now, you will compare ZTNA to SSL and IPsec VPN.



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

By demonstrating competence in understanding the evolution of remote access with ZTNA, you will be able to migrate from VPN to ZTNA HTTPS access proxy.



How are SSL VPN and ZTNA access different from IPsec VPNs?

SSL and TLS are commonly used to encapsulate and secure e-commerce and online banking on the internet (HTTP). SSL VPNs and ZTNA use a similar technique, and support non-HTTP protocol encapsulation as well. SSL resides higher up on the network stack than IP and, therefore, it usually requires more bits—more bandwidth—for SSL VPN headers. In comparison, IPsec uses some different methods to provide confidentiality and integrity. The primary protocol used in IPSec is ESP, which encapsulates and encrypts UDP, RDP, HTTP, or other protocols inside the IPsec tunnel.

IPSec is also an industry-standard protocol that can work with multiple vendors and supports peers that are devices and gateways—not just user clients with FortiGate only, like SSL VPN or ZTNA does.

The client software is also different. In an SSL VPN or ZTNA, your web browser might be the only client software you need. You can go to the FortiGate SSL VPN portal (an HTTPS web page) and then log in. Alternatively, you can install FortiClient or configure FortiGate as an SSL VPN client. In comparison, to use IPsec VPN, install special client software or have a local gateway, such as a desktop model FortiGate, to connect to the remote gateway. You might also need to configure firewalls between VPN peers to allow IPsec protocols.

Comparing SSL VPN, IPsec VPN, and ZTNA Access (Contd)

	IPsec VPN	SSL VPN	ZTNA
Category:	Industry standard	Vendor specific	Vendor specific

Ease of use (Configuration):	• Requires installation
	• Flexible setup
	  • Mesh and star topologies
	  • For clients or peer gateways
	  • Performance based: IPsec encryptography is faster in FortiOS
		• Does not require installation
		• Simpler setup
		  • Client-to-FortiGate
		  • FortiGate-to-FortiGate
		  • No user-configured settings
		  • Technical support less requested
			• Does not require installation
			• Simpler setup
			  • Only client-to-FortiGate
			  • No user-configured settings
			  • Technical support less requested

Better for:	Office-to-office traffic Data centers	Provides flexibility tunnel-mode or session-based access	Session-based access only

Attack surface protection	• Traditional perimeter protection:
	  • Defends against external threats only
	  • Doesn't address threat inside the network
		• Traditional perimeter protection:
		  • Defends against external threats only
		  • Doesn't address threat inside the network
			• zero-trust philosophy
			  • No one inside or outside should be trusted
			  • Based on identity authentication

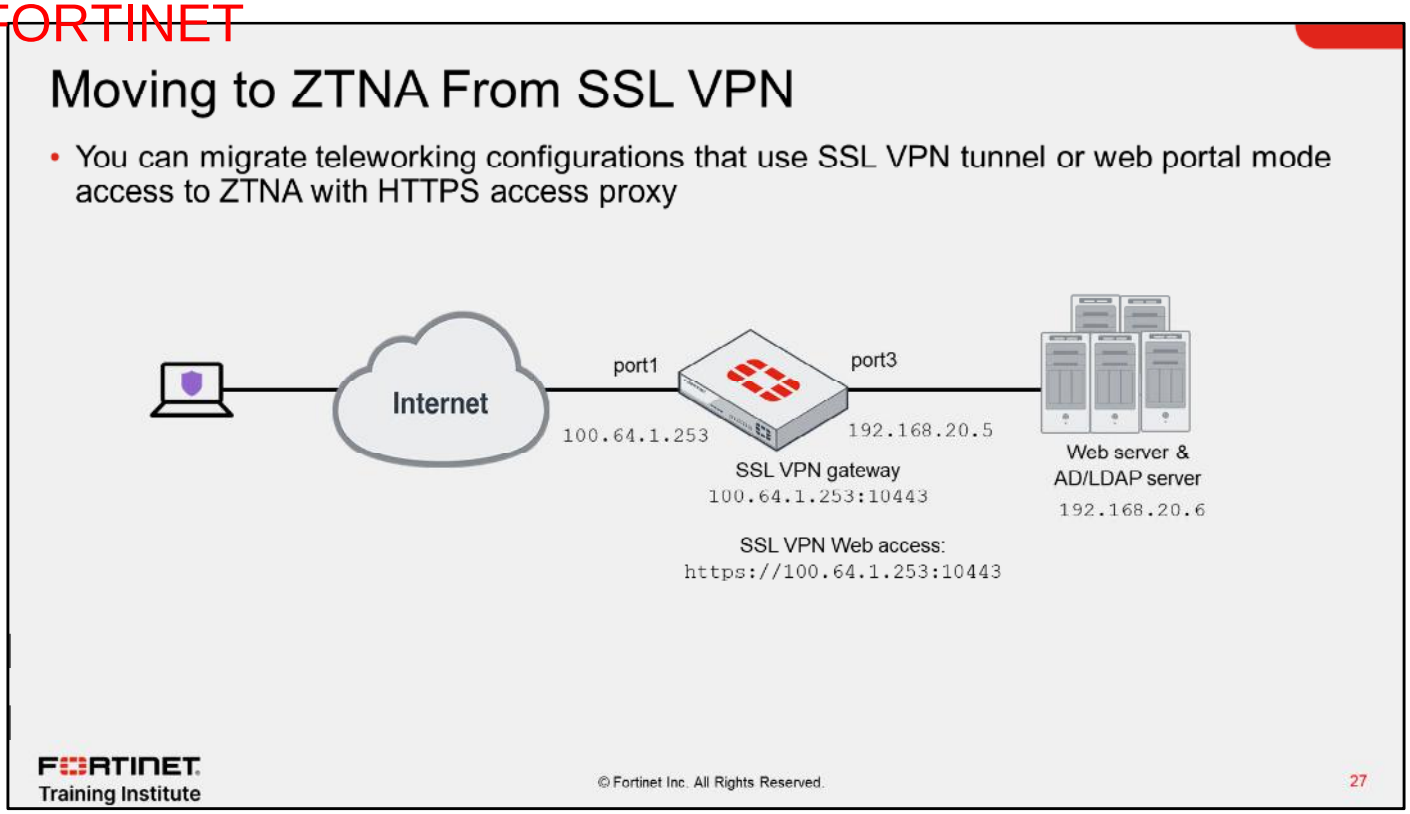
FORTINET Training Institute

26

After you log in, the SSL VPN connects your computer to your private network. No user-configured settings are required, and firewalls are typically configured to allow outgoing HTTP, so technical support calls are less likely. Simplicity makes ZTNA and SSL VPN ideal for non-technical users, or users who connect from public computers, such as those found in public libraries and internet cafés. ZTNA takes this a step further and makes it easier for administrators to perform device compliance checks and configuration. ZTNA also provides an additional authentication mechanism for access control without any interaction required from the end user.

ZTNA follows the zero-trust philosophy to protect the attack surface that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. zero-trust also assumes that every attempt to access the network or an application is a threat.

Both IPSec and SSL VPN are traditional perimeter-based security approach that only distrusts factors outside the existing network and fail to address threats that already exist within the network.



You can use ZTNA to replace VPN-based teleworking solutions. The example on this slide shows that you can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy, and continue to use the same authentication server and groups to authenticate your remote users.

In addition, by integrating with FortiClient EMS, you can also ensure that FortiGate performs device identification is using client certificates, and checks the security posture before allowing the remote user into the website. This provides granular control over who can access the web resource using role-based access control. It also gives the user transparent access to the website using only their browser. You can even configure ZTNA IP/MAC filtering mode for on-fabric devices to provide similar access control while users are on the network.

Knowledge Check

1. Which remote access solution proxies HTTP and TCP over a secure HTTPS connection?

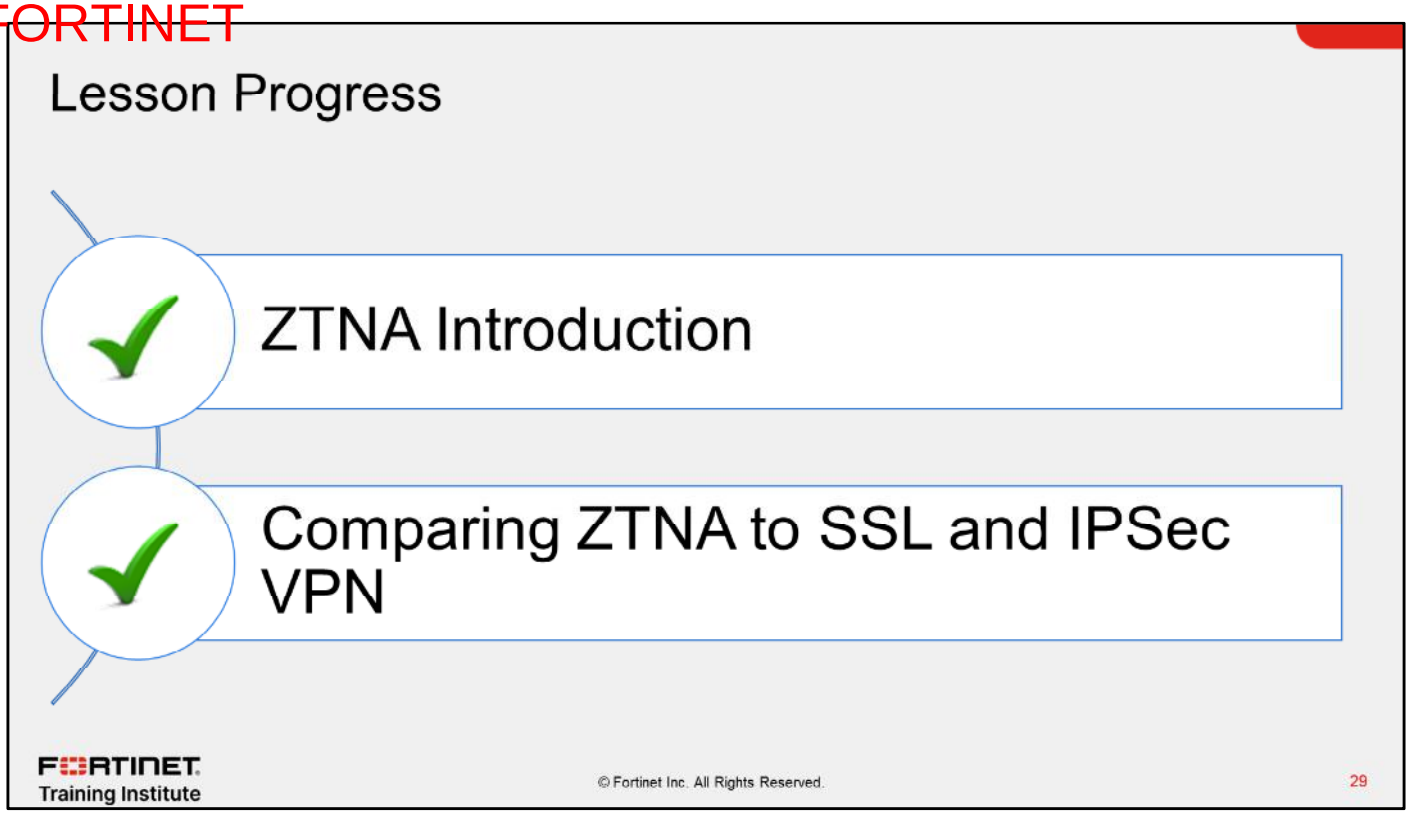
✓A. ZTNA
B. IPSec

2. What does FortiClient EMS integration ensure?

✓A. Device identification
B. User identification

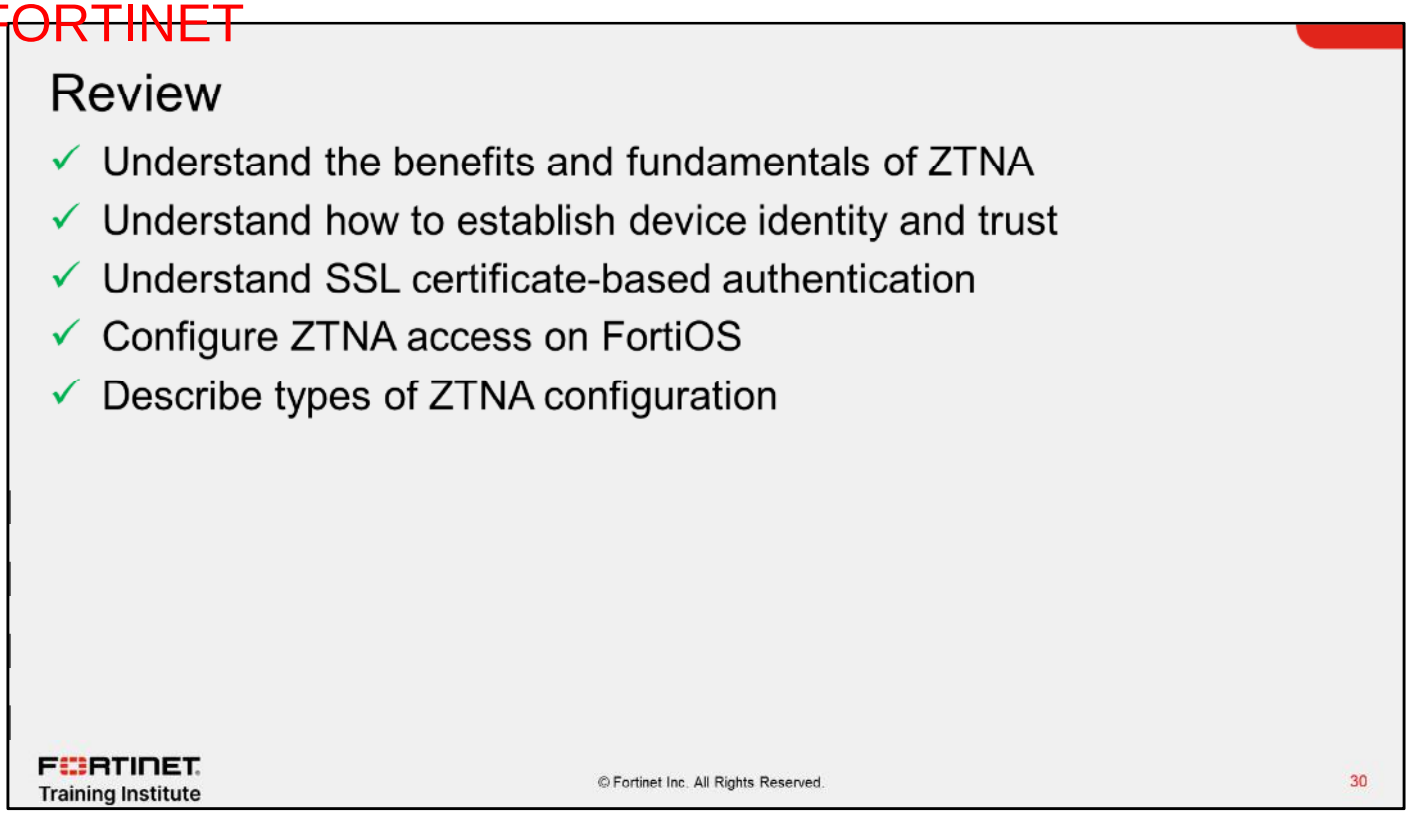
FORTINET Training Institute

28



Congratulations! You have completed this lesson.

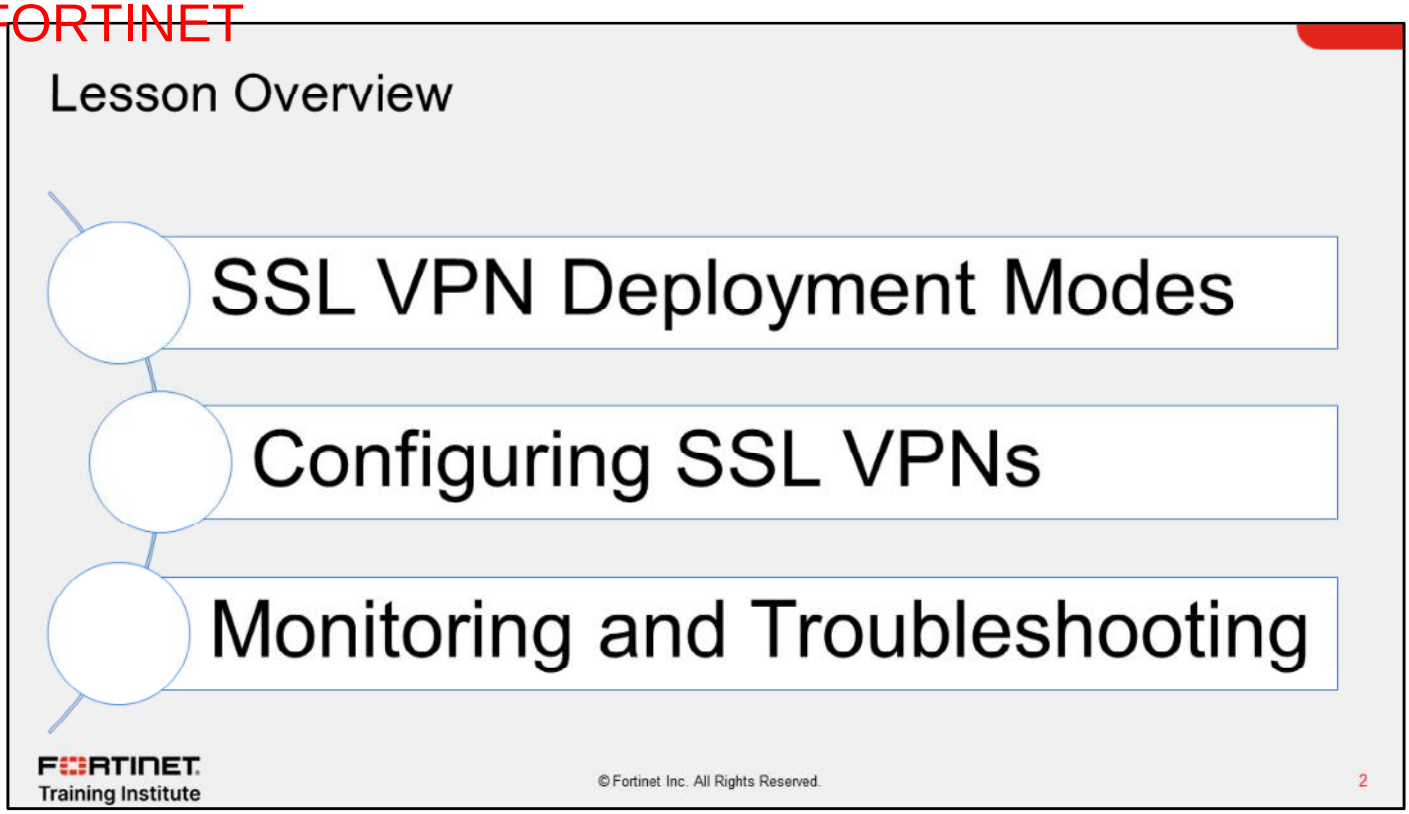
Now, you will review the objectives that you covered in this lesson.



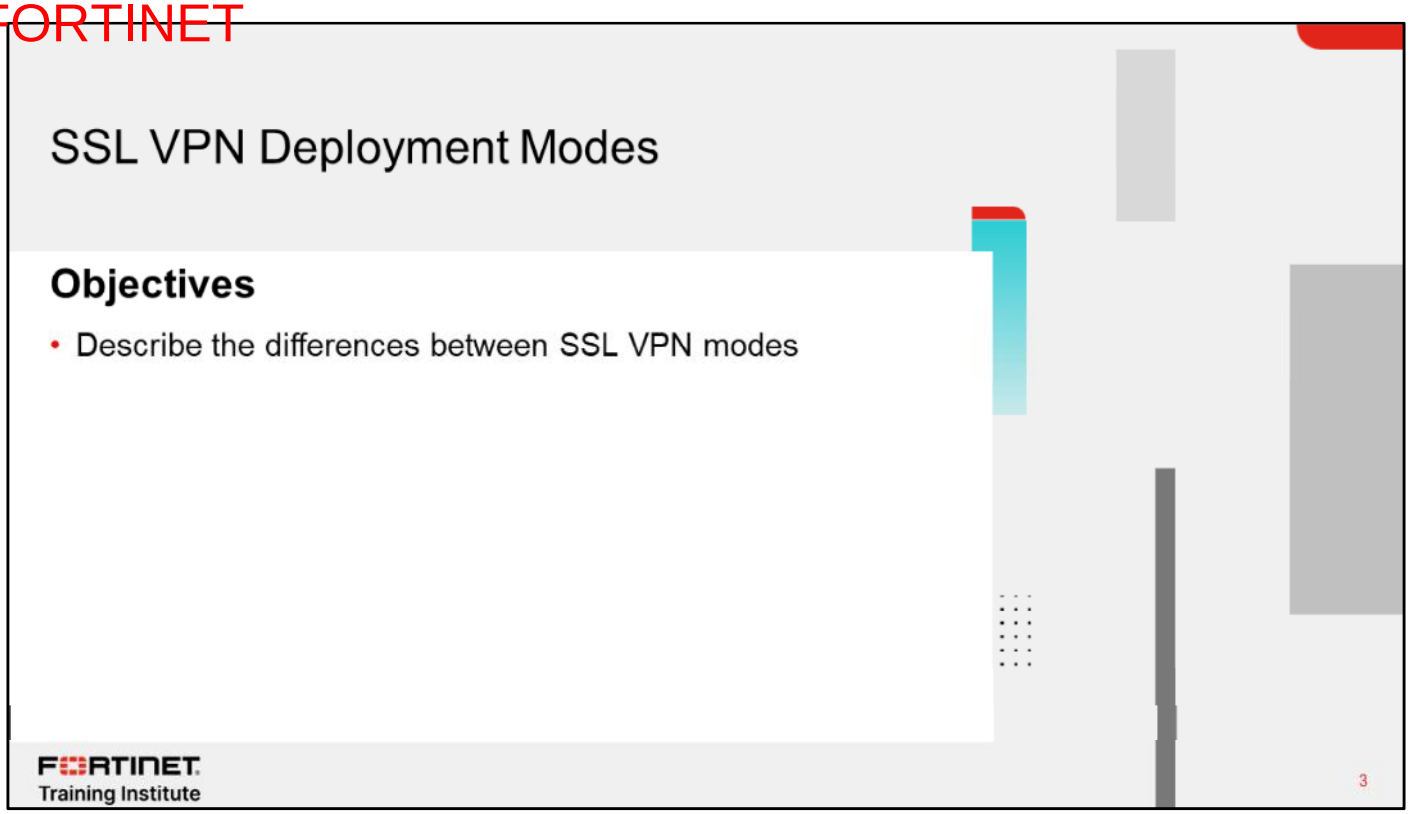
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about how to configure and use ZTNA.

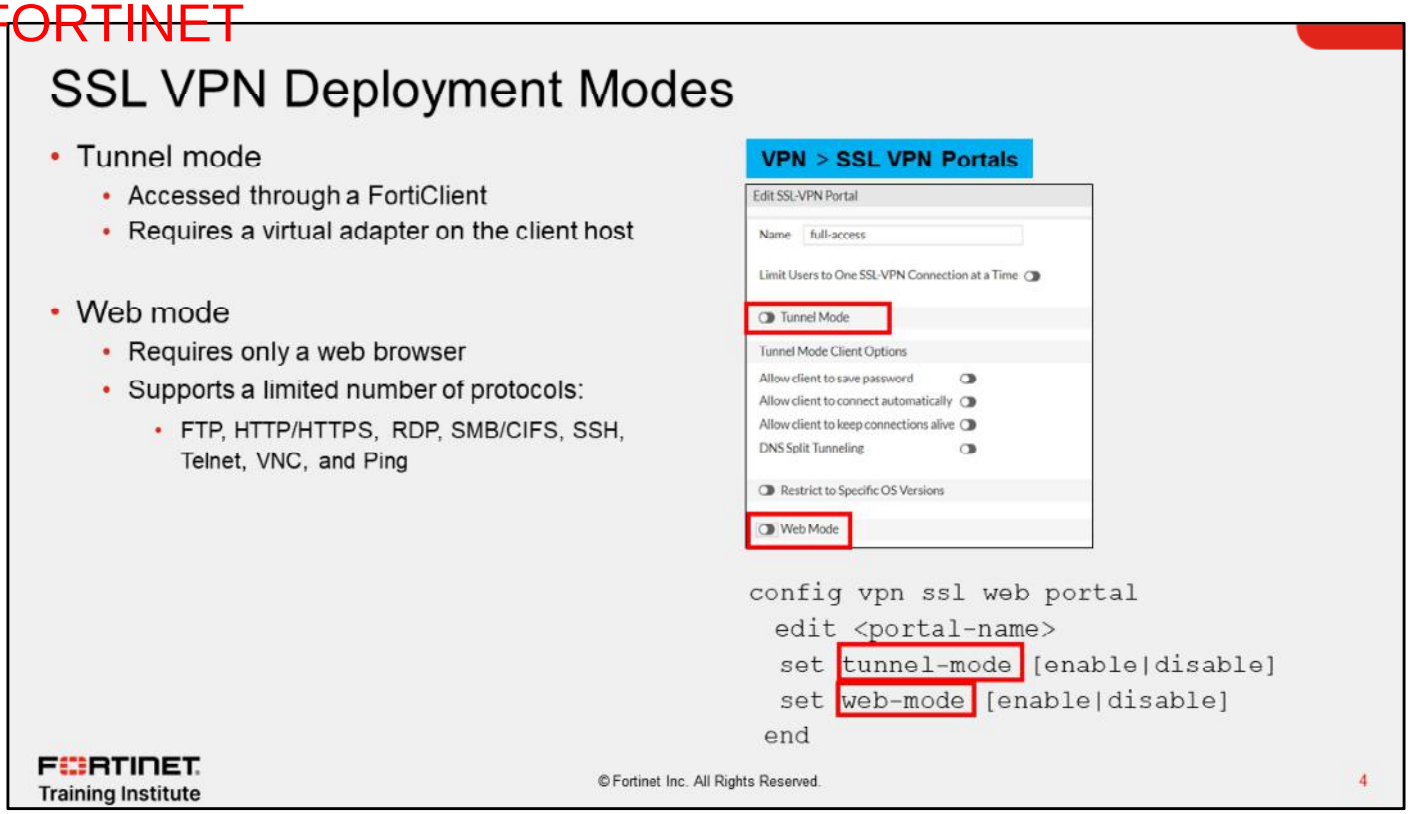
In this lesson, you will learn how to configure and use SSL VPNs. SSL VPNs are an easy way to give remote users access to your private network.



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



After completing this section, you should be able to achieve the objective shown on this slide. By demonstrating competence in understanding the different ways FortiGate allows SSL VPN connections, you will be able to better design the configuration of your SSL VPN.

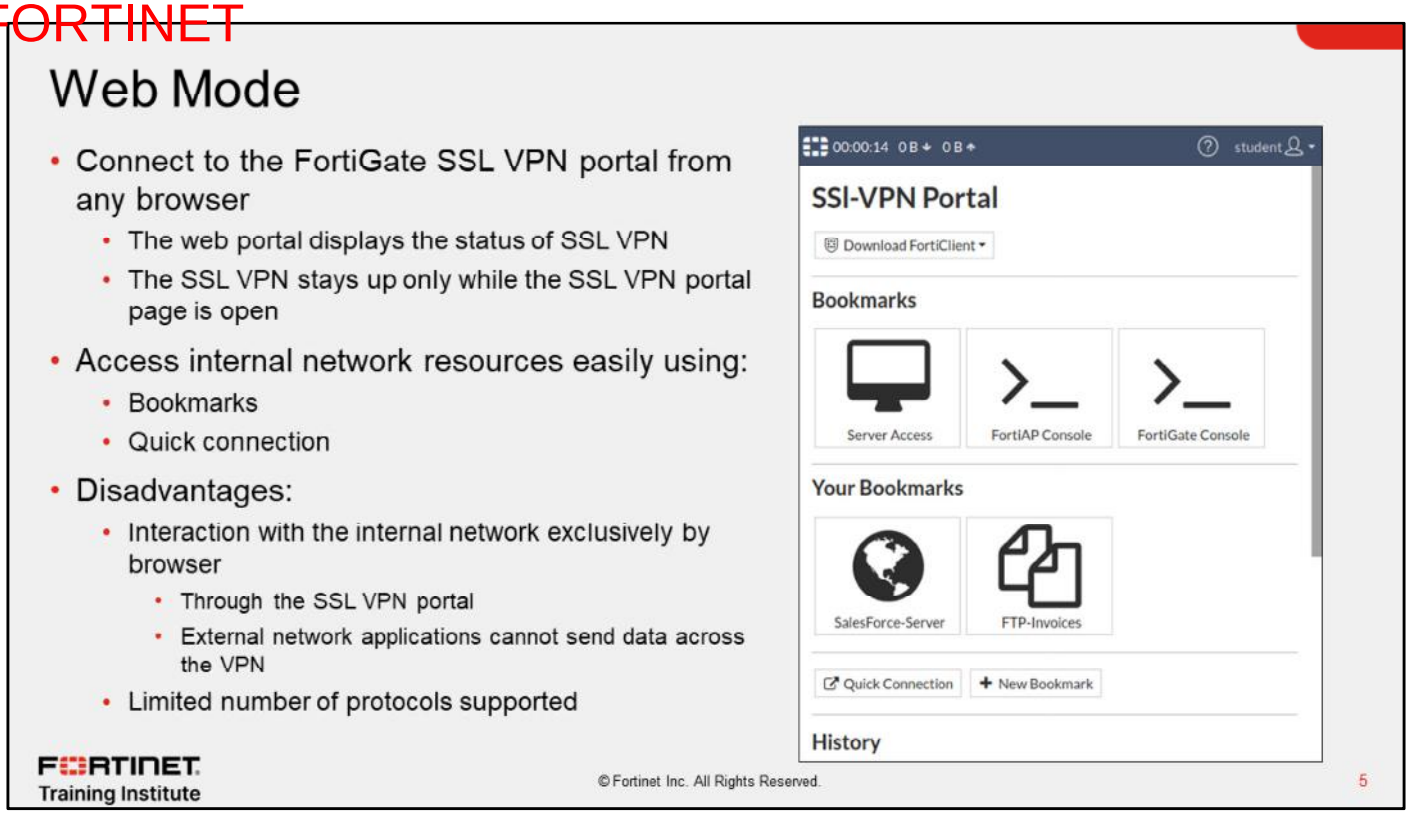


There are two modes you can use to access an SSL VPN. Both can build an SSL VPN connection, but they don't support the same features.

Which should you choose?
It depends on which applications you need to send through the VPN, the technical knowledge of your users, and whether or not you have administrative permissions on their computers.

Tunnel mode supports the most protocols, but requires the installation of a VPN client, or more specifically, a virtual network adapter. To tunnel traffic using the virtual adapter, you must use the FortiClient remote access feature or FortiClient VPN-only client.

Web mode requires only a web browser, but supports a limited number of protocols.



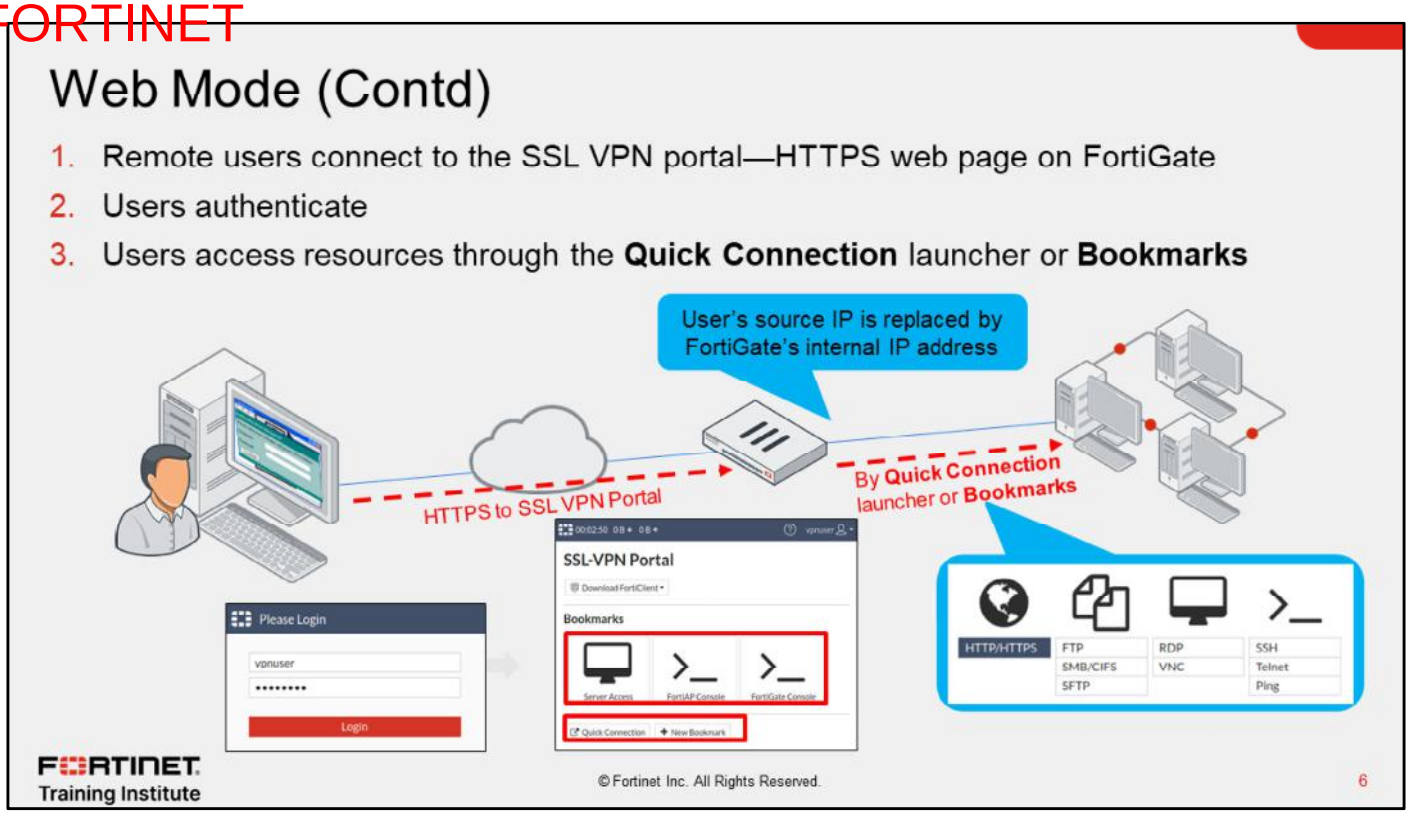
Web mode is the simplest SSL VPN mode.

Like you would with any other HTTPS website, you simply log in to the SSL VPN portal web page on FortiGate. It acts like a server-side reverse proxy, or a simple secure HTTP/HTTPS gateway, that connects you with the applications on the private network.

The **Bookmarks** section on the **SSL VPN Portal** page contains links to all or some of the resources available for the user to access. The **Quick Connection** widget allows users to type the URL or IP address of the server they want to reach. A web SSL VPN user makes use of these two widgets to access the internal network. The main advantage of web mode is that it does not usually require you to install extra software.

Web mode has two main disadvantages:

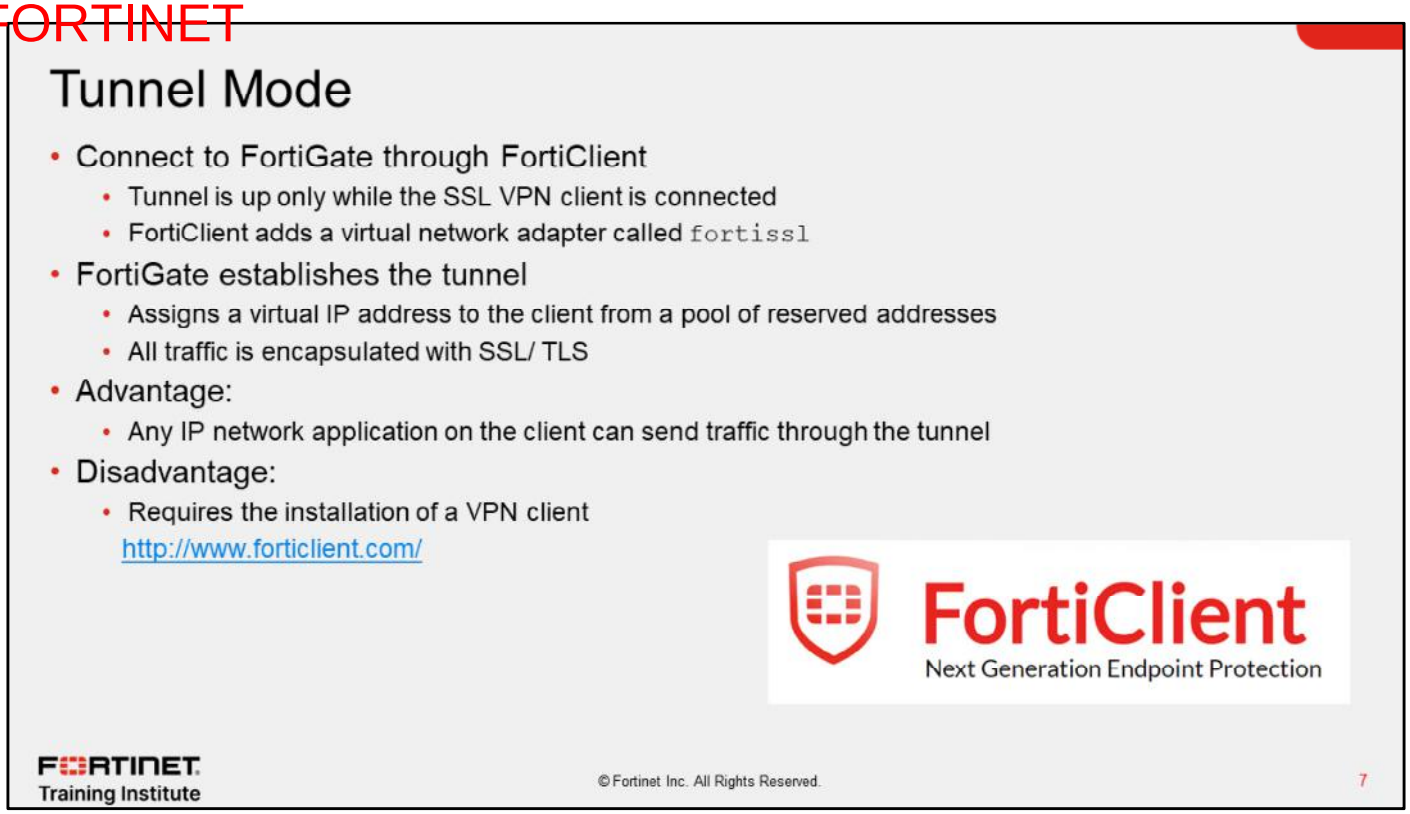
- All interaction with the internal network must be done using the browser exclusively (through the web portal). External network applications running on the user's PC cannot send data across the VPN.
- This a secure HTTP/HTTPS gateway mechanism that doesn't work for accessing everything, but just few popular protocols, such as HTTP, FTP, and Windows shares.



How does web mode work?

1. Remote users establish a secure connection between the SSL security in the web browser and the FortiGate SSL VPN portal, using HTTPS.
2. Once connected, users provide credentials in order to pass an authentication check.
3. Then, FortiGate displays the SSL VPN portal that contains services and network resources for users to access.

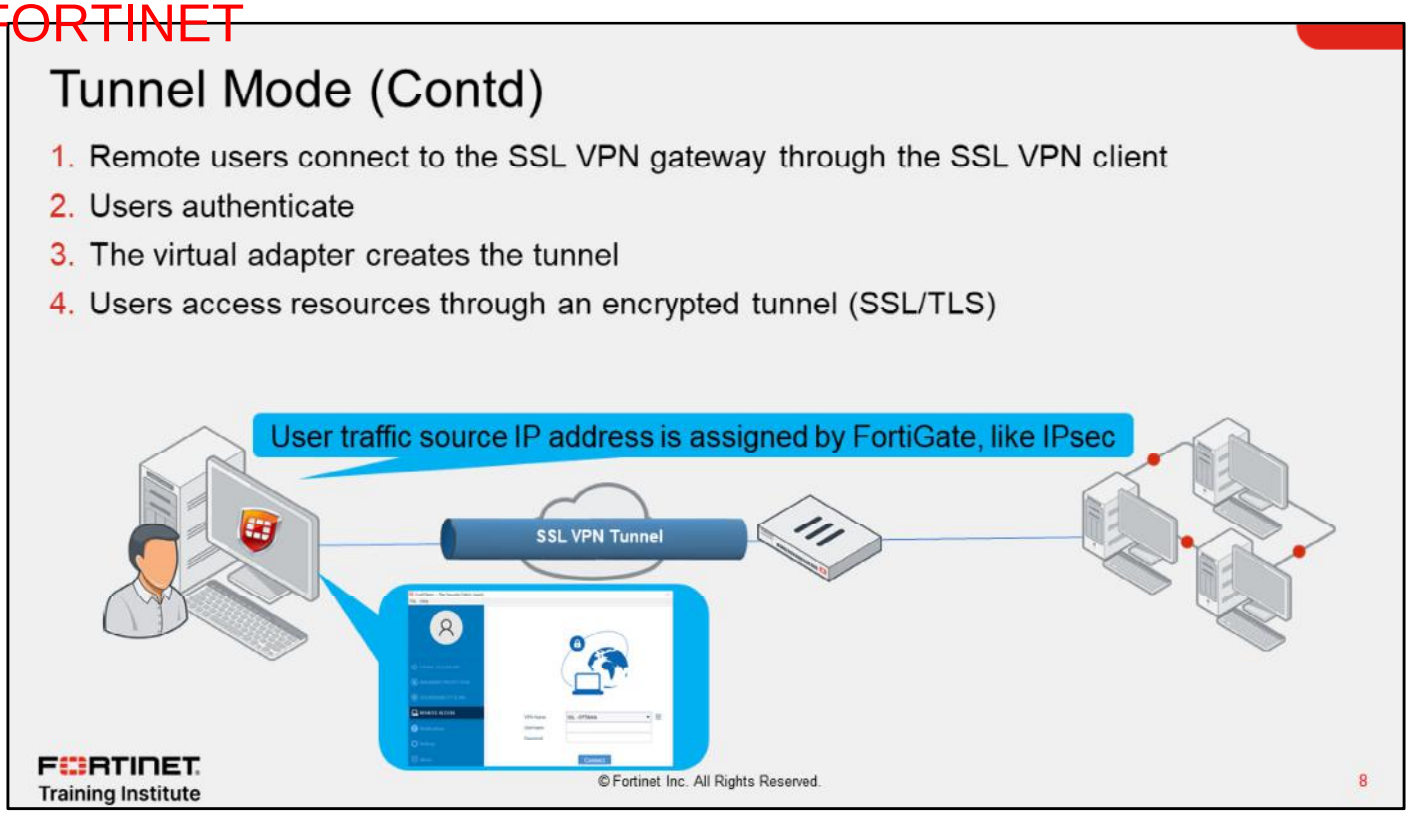
Different users can have different portals with different resources and access permissions. Also notice the source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address.



Tunnel mode is the second option FortiGate provides to access resources within an SSL VPN.

Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as `fortissl` to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated.

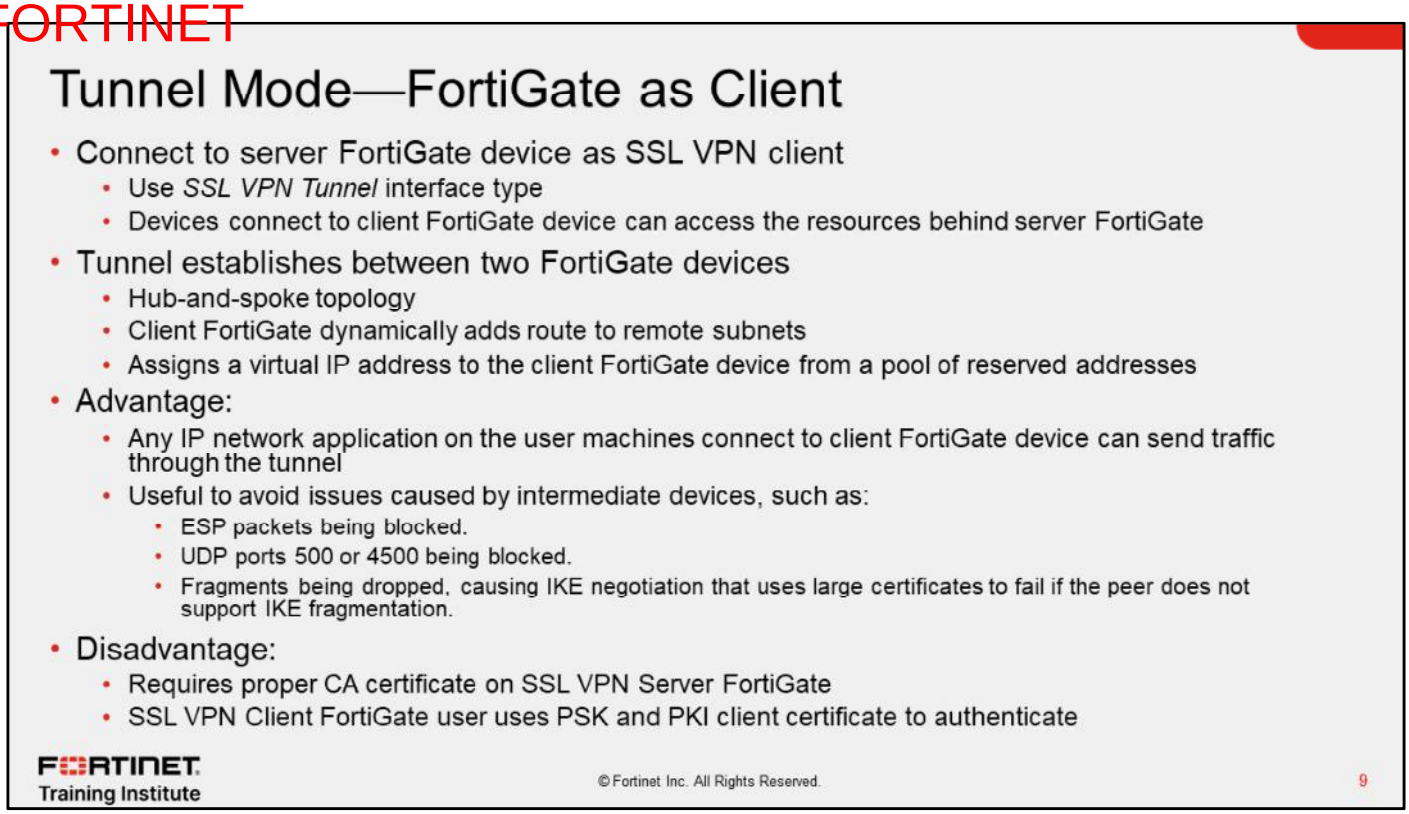
The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel. The main disadvantage is that tunnel mode requires the installation of a VPN software client, which requires administrative privileges.



How does tunnel mode work?

1. Users connect to FortiGate through FortiClient.
2. Users provide credentials to successfully authenticate.
3. FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter (`fortissl`). This is the client's source IP address for the duration of the connection.
4. Then, users can access services and network resources through the encrypted tunnel.

FortiClient encrypts all traffic from the remote computer and sends it over the SSL VPN tunnel. FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.



The FortiGate can be configured as an SSL VPN client, using an *SSL-VPN Tunnel* interface type. When an SSL VPN client connection is established, the client dynamically adds a route to the subnets that are returned by the SSL VPN server. Policies can be defined to allow users that are behind the client to be tunneled through SSL VPN to destinations on the SSL VPN server.

This setup provides IP-level connectivity in tunnel mode and allows hub-and-spoke topologies to be configured with FortiGates as both the SSL VPN hub and spokes. This can be useful to avoid issues caused by intermediate devices, such as:

- ESP packets being blocked.
- UDP ports 500 or 4500 being blocked.
- Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.

If the client specified destination is *all*, a default route is effectively dynamically created on the SSL VPN client, and the new default route is added to the existing default route in the form of ECMP. You can modify route's distance or priority according to your requirements. To avoid a default route being learned on the SSL VPN client, on the SSL VPN server define a specific destination. Split tunneling is used so that only the destination addresses defined in the server's firewall policies are routed to the server, and all other traffic is connected directly to the internet.

This configuration requires proper CA certificate installation as the SSL VPN client FortiGate/user uses PSK and a PKI client certificate to authenticate. The FortiGate devices must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.