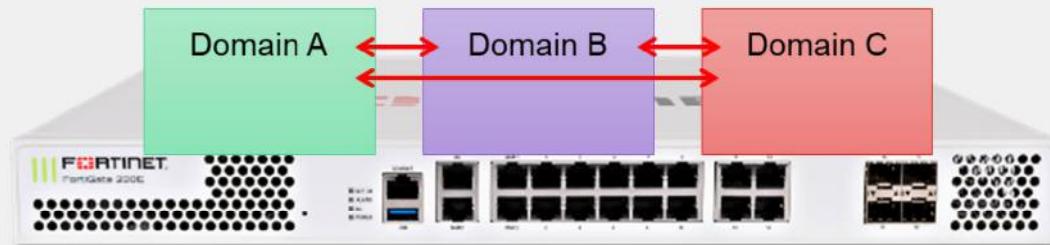


**DO NOT REPRINT****© FORTINET**

## Inter-VDOM Links



- Can connect different VDOMs
- Support varies by VDOM operating mode
  - NAT-to-NAT ✓
  - NAT-to-transparent and transparent-to-NAT ✓
  - Transparent-transparent (no Layer 3; potential Layer 2 loops) ✗

To review, each VDOM behaves like it is on a separate FortiGate device. With separate FortiGate devices, you would normally connect a network cable and configure routing and policies between them. But VDOMs are on the same FortiGate. So, how should you route traffic between them?

The solution is inter-VDOM links. Inter-VDOM links are a type of virtual interface that route traffic between VDOMs. This removes the need to loop a physical cable between two VDOMs.

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

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

**DO NOT REPRINT****© FORTINET**

## Inter-VDOM Links (Contd)

- Inter-VDOM links allow VDOMs to communicate
  - Traffic is not required to leave a physical interface then re-enter FortiGate
  - Fewer physical interfaces or cables are required
    - This prevents the wasting of physical interfaces, and eliminates the need for a loopback cable
- Routes are required to forward the traffic from one VDOM to another
- Firewall policies are also required to allow traffic from other VDOMs, the same as traffic coming from physical interfaces



© Fortinet Inc. All Rights Reserved.

35

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

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

DO NOT REPRINT  
© FORTINET

## Creating Inter-VDOM Links

The screenshot shows the FortiGate Management Interface under 'Global > Network > Interfaces'. A red arrow points from the 'Create New' button in the interface list to the 'VDOM Link' option in the dropdown menu. The 'VDOM Link' dialog box is open on the right, titled 'New VDOM Link'. It contains fields for 'Name' (vlink), 'Interface 0 (vlink0)', 'Interface 1 (vlink1)', and various configuration options like 'Virtual Domain', 'IP/Netmask', and 'Administrative Access' (HTTPS, PING, SSH, SNMP). The status is set to 'Enabled'. At the bottom are 'OK' and 'Cancel' buttons.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

36

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

**DO NOT REPRINT****© FORTINET**

## Inter-VDOM Link Acceleration

- FortiGate devices with NP4 or NP6 processors include inter-VDOM links that FortiGate can use to accelerate inter-VDOM link traffic
- For a FortiGate device with two NP4 or NP6 processors, there are two accelerated inter-VDOM links, each with two interfaces:
  - **npu0\_vlink:**
    - npu0\_vlink0
    - npu0\_vlink1
  - **npu1\_vlink:**
    - npu1\_vlink0
    - npu1\_vlink1
- These interfaces are visible on the GUI and CLI



© Fortinet Inc. All Rights Reserved.

37

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

- **npu0\_vlink:**
  - npu0\_vlink0
  - npu0\_vlink1
- **npu1\_vlink:**
  - npu1\_vlink0
  - npu1\_vlink1

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. What is a requirement for creating an inter-VDOM link between two VDOMs?
  - A. The NGFW mode of at least one VDOM must be profile based.
  - B. At least one of the VDOMs must be operating in NAT mode.
  
2. Which type of VDOM link requires that both sides of the link be assigned an IP address within the same subnet?
  - A. NAT-to-transparent
  - B. NAT-to-NAT

**DO NOT REPRINT****© FORTINET**

## Lesson Progress

**VDOM Concepts****VDOM Administrators****Configuring VDOMs****Inter-VDOM Links****Best Practices and Troubleshooting**

Good job! You now understand inter-VDOM Links.

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

**DO NOT REPRINT**  
© FORTINET

## Best Practices and Troubleshooting

### Objectives

- Limit the resources allocated globally and per VDOM
- Troubleshoot common VDOM issues

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

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

**DO NOT REPRINT****© FORTINET**

## System Resource Allocation

- Global resources limit: apply to resources that are shared by the whole FortiGate
- VDOM resources limit: per-VDOM resources are specific to each VDOM
  - Default per-VDOM resource settings are set to have **no limits**.
  - Guarantees a per-VDOM minimum resource allocation
  - No VDOM can starve the others of all the device resources



© Fortinet Inc. All Rights Reserved.

41

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

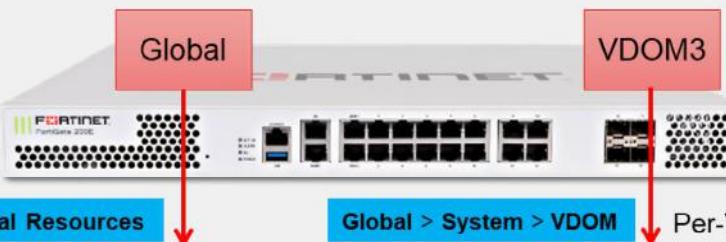
By default, all per-VDOM resource settings are set to have no limits. This means that any single VDOM can use all of the FortiGate device's resources. This could deprive other VDOMs of the resources that they require, to the point that could be unable to function.

Unlike FortiGate-VM, VDOMs are not allocated and balanced with weighted vCPU cores, vRAM, and other virtualized hardware.

To fine-tune performance, you can configure resource limits for each feature—IPsec tunnels, address objects, and so on—at the global level and at each VDOM level. This controls the ratio of the system resource usage of each VDOM to the total available resources.

**DO NOT REPRINT**  
**© FORTINET**

## Global and Per-VDOM Resource Limits



The diagram illustrates the configuration of resource limits on a FortiGate device. It shows a main FortiGate unit with two virtual domains (VDOM1 and VDOM3) connected to it. Red boxes highlight the 'Global' resources and the 'Per-VDOM resource limits' for VDOM3.

**Global > System > Global Resources**

Resource	Current Usage	Default Maximum	Override Maximum
Active Sessions	(289)	No Limit Set	<input checked="" type="checkbox"/>
<b>Policy &amp; Objects</b>			
Firewall Policies	(24)	21024	<input checked="" type="checkbox"/>
Firewall Addresses	(54)	11024	<input checked="" type="checkbox"/>
Firewall Address Groups	(10)	5000	<input checked="" type="checkbox"/>
Firewall Custom Services	(107)	No Limit Set	<input checked="" type="checkbox"/>
Firewall Service Groups	(8)	No Limit Set	<input checked="" type="checkbox"/>
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>
Firewall Recurring Schedules	(5)	No Limit Set	<input checked="" type="checkbox"/>
User & Device			

**Global > System > VDOM**

VDOM3 settings:

Resource	Current Usage	Global Maximum	Override Maximum	Guaranteed
Active Sessions	(0)	No Limit Set	<input checked="" type="checkbox"/>	
<b>Policy &amp; Objects</b>				
Firewall Policies	(0)	21024	<input checked="" type="checkbox"/>	
Firewall Address Groups	(0)	11024	<input checked="" type="checkbox"/>	
<b>VPN IPsec Phase1 Tunnels</b>				
Current Usage	(0)	2000	1900	1000
Firewall Service Groups	(4)	No Limit Set	<input checked="" type="checkbox"/>	
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>	

**Per-VDOM resource limits**

© Fortinet Inc. All Rights Reserved. 42

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

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

DO NOT REPRINT  
© FORTINET

## Monitoring VDOM Resources

- VDOM monitor displays:
  - CPU utilization
  - Memory utilization

Global > System > VDOM

Name	Management VDOM	NGFW Mode	Operation Mode	Status	CPU	Memory	Interfaces
customer	✗	Profile-based	NAT	Enabled	0%	7%	port3 SSL-VPN tunnel interface (ssl.customer)
root	✓	Profile-based	NAT	Enabled	0%	38%	port1 port2 port4 port5

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

**DO NOT REPRINT****© FORTINET**

## VDOM Administrator Has Difficulty Gaining Access

- Confirm the administrator VDOM
- Confirm the VDOM interfaces
- Confirm the VDOM administrator's access privileges
- Confirm trusted host and IP
- Best Practices
  - Create a VDOM-specific administrator account for each VDOM
  - Avoid giving **super\_admin** access



© Fortinet Inc. All Rights Reserved.

44

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

- Confirm the administrator's VDOM: each administrator account, other than the **super\_admin** account, is tied to one or more specific VDOMs. That administrator is not able to access any other VDOM. It may be possible they are trying to access the wrong VDOM (one that they do not have permissions for).
- Confirm the VDOM interfaces: an administrator can access their VDOM only through interfaces that are assigned to that VDOM. If interfaces on that VDOM are disabled or unavailable, there will be no method of accessing that VDOM by its local administrator. The **super\_admin** is required to either bring up the interfaces, fix the interfaces, or move another interface to that VDOM to restore access.
- Confirm the VDOM admin access: as with all FortiGate devices, administration access on the VDOM's interfaces must be enabled for the administrators of that VDOM to gain access. For example, if SSH is not enabled, that is not available to administrators. To enable admin access, the **super\_admin** clicks **Global > Network > Interfaces** and enables administrator access for the interface in question.
- Confirm trusted host and IP: if trusted hosts are enabled on the administrator account, ensure the user is connecting from the correct, specified host address, and that no intermediate devices are performing NAT functions on the connection.

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

**DO NOT REPRINT****© FORTINET**

## General VDOM Troubleshooting Tips

- Perform a sniffer trace

```
diagnose sniffer packet <interface_name> '<filter>' <verbose> <count>
```

- Perform a packet flow trace

```
diagnose debug enable
diagnose debug flow filter addr <PC1>
diagnose debug flow trace start 100
```



© Fortinet Inc. All Rights Reserved.

45

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

- Perform a sniffer trace: when troubleshooting networks, it helps to look inside the headers of packets to determine if they are traveling along the expected route. Packet sniffing can also be called a network tap, packet capture, or logic analyzing. The sniffer also indicates what traffic is entering or leaving the egress and ingress interfaces in all VDOMS. This makes it extremely useful for troubleshooting inter-VDOM routing issues.
- Debug the packet flow: traffic should enter and leave the VDOM. If you have identified that network traffic is not entering and leaving the VDOM as expected, debug the packet flow. You can debug only using CLI commands. This tool provides more granular details for help in troubleshooting inter-VDOM traffic because it gives details of routing selection, NAT, and policy selection.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Of these options, what is a possible reason why an administrator might not be able to gain access to a specific VDOM?  
 A. The administrator is using an IP address that is not specified as a trusted host.  
 B. The administrator is using the super\_admin profile.
  
2. Which troubleshooting tool is most suitable when trying to verify the firewall policy used by an inter-VDOM link?  
 A. Sniffer trace  
 B. Packet flow trace

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



VDOM Concepts



VDOM Administrators



Configuring VDOMs



Inter-VDOM Links



Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Define and describe VDOMs
- ✓ Create administrative accounts with access limited to one or more VDOMs
- ✓ Configure VDOMs to split FortiGate into multiple virtual devices
- ✓ Route traffic between VDOMs
- ✓ Limit the resources allocated globally and per VDOM



© Fortinet Inc. All Rights Reserved.

48

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

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

**DO NOT REPRINT**

© FORTINET



## FortiGate Infrastructure

Fortinet Single Sign-On (FSSO)



Last Modified: 13 June 2022

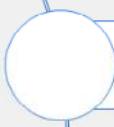
In this lesson, you will learn about Fortinet single sign-on (FSSO). When you use this feature, your users don't need to log on each time they access a different network resource.

**DO NOT REPRINT****© FORTINET**

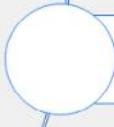
## Lesson Overview



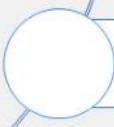
### FSSO Function and Deployment



### FSSO With Active Directory



### FSSO Settings



### Troubleshooting

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

**DO NOT REPRINT****© FORTINET**

## FSSO Function and Deployment

### Objectives

- Define single sign-on (SSO) and Fortinet single sign-on (FSSO)
- Understand FSSO deployment and configuration

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

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

**DO NOT REPRINT****© FORTINET**

## SSO and FSSO

- SSO is a process that allows identified users access to multiple applications without having to re-authenticate
- Users who are already identified can access applications without being prompted to provide credentials
  - FSSO software identifies a user's user ID, IP address, and group membership
  - FortiGate allows access based on membership in FSSO groups configured on FortiGate
  - FSSO groups can be mapped to individual users, user groups, organizational units (OUs), or a combination of them
- Each FSSO method gathers login events differently
- FSSO is typically used with directory services, such as Windows Active Directory or Novell eDirectory



© Fortinet Inc. All Rights Reserved.

4

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

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

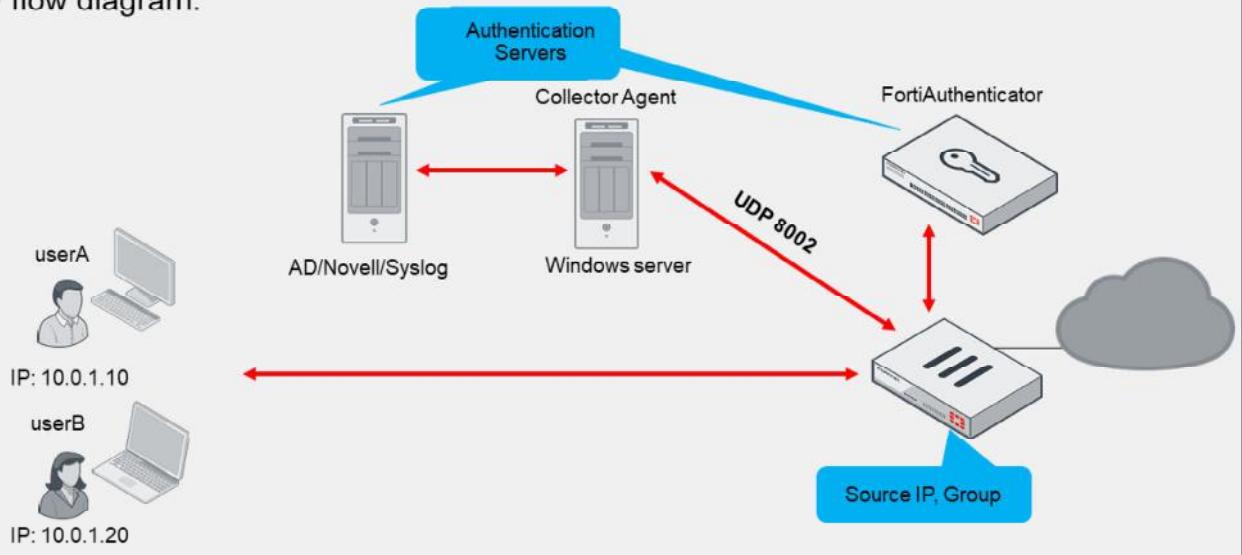
Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

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

**DO NOT REPRINT****© FORTINET**

## FSSO—Flow Chart

- FSSO flow diagram:



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

**DO NOT REPRINT****© FORTINET**

## FSSO Deployment and Configuration



Microsoft

Active Directory

### Microsoft Active Directory (AD)

- Domain controller (DC) agent mode
- Polling mode:
  - Collector agent-based
  - Agentless
- Terminal server (TS) agent
  - Enhances login capabilities of a collector agent or FortiAuthenticator
  - Gathers logins for Citrix and terminal servers where multiple users share the same IP address



### Novell eDirectory

- eDirectory agent mode
- Uses Novell API or LDAP setting

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. In FSSO, FortiGate allows network access based on \_\_\_\_\_.  
 A. Active user authentication with username and password  
 B. Passive user identification by user ID, IP address, and group membership
  
2. Which working mode is used for monitoring user sign-on activities in Windows AD?  
 A. Polling mode (collector agent-based or agentless)  
 B. eDirectory agent mode

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



FSSO Function and Deployment



FSSO With Windows Active Directory



FSSO Settings



Troubleshooting

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

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

**DO NOT REPRINT****© FORTINET**

## FSSO With Windows Active Directory

### Objectives

- Detect user login events in Windows AD using FSSO
- Identify FSSO modes for Windows AD

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

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

**DO NOT REPRINT****© FORTINET**

## DC Agent Mode

- DC agent mode is the most scalable mode and is, in most environments, the recommended mode for FSSO
- Requires one DC agent (`dcagent.dll`) installed on each Windows DC in the `Windows\system32` directory. The DC agent is responsible for:
  - Monitoring user login events and forwarding them to the collector agents
  - Handling DNS lookups (by default)
- Requires one or more collector agents installed on Windows servers. The collector agent is responsible for:
  - Group verification
  - Workstation checks
  - Updates of login records on FortiGate
  - Sending domain local security group, organizational units (OUs), and global security group information to FortiGate



© Fortinet Inc. All Rights Reserved.

10

DC agent mode is considered the recommended mode for FSSO.

DC agent mode requires:

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

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

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

In some configurations, double DNS resolution is a problem. In this case, you may configure a registry key on the domain controller that hosts the DC agent in order not to resolve the DNS:

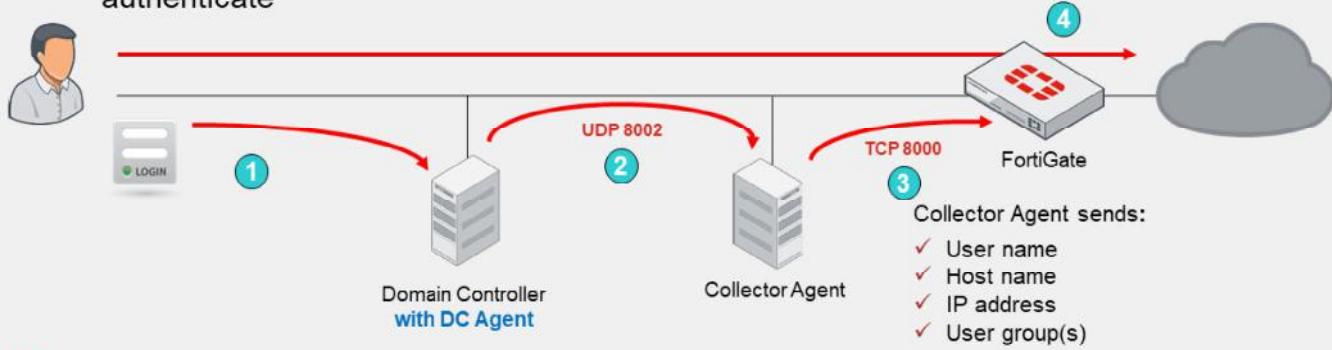
```
donot_resolve = (DWORD) 1 at HKLM\Software\Fortinet\FSAE/dcagent
```

**DO NOT REPRINT**

**© FORTINET**

## DC Agent Mode Process

1. The user authenticates against the Windows DC
2. The DC agent sees the login event and forwards it to the collector agent
3. The collector agent receives the event from the DC agent and forwards it to FortiGate
4. FortiGate knows the user based on their IP address, so the user does not need to authenticate



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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

1. When users authenticate with the DC, they provide their credentials.
2. The DC agent sees the login event, and forwards it to the collector agent.
3. The collector agent aggregates all login events and forwards that information to FortiGate. The information sent by the collector agent contains the user name, host name, IP address, and user group(s). The collector agent communicates with FortiGate over TCP port 8000 (default) and it listens on UDP port 8002 (default), for updates from the DC agents. The ports are customizable.
4. FortiGate learns from the collector agent who the user is, their IP address, and some of the AD groups that the user is a member of. When a user tries to access the internet, FortiGate compares the source IP address to its list of active FSSO users. Because the user in this case has already logged in to the domain, and FortiGate already has their information, FortiGate doesn't prompt the user to authenticate again. Rather it allows or denies the traffic based on the matching firewall policy.

**DO NOT REPRINT****© FORTINET**

## Collector Agent-Based Polling Mode

- A collector agent must be installed on a Windows server
  - No FSSO DC agent is required
- Every few seconds, the collector agent polls each DC for user login events. The collector agent uses:
  - SMB (TCP 445) protocol, by default, to request the event logs
  - TCP 135, TCP 139, and UDP 137 as fallbacks
- This mode requires a less complex installation, which reduces ongoing maintenance
- Three methods:
  - NetAPI
  - WinSecLog
  - WMI
- Event logging must be enabled on the DCs (except in NetAPI)



© Fortinet Inc. All Rights Reserved.

12

Polling mode can be collector agent-based or agentless.

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

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

**DO NOT REPRINT****© FORTINET**

## Collector Agent-Based Polling Mode Options

### WMI

- DC returns all requested login events every 3 seconds\*
  - Reads selected event logs
- Improves WinSec bandwidth usage
  - Reduces network load between collector agent and DC

### WinSecLog

- Polls all security events on DC every 10 seconds, or more\*
  - Log latency if network is large or system is slow
  - Requires fast network links
- Slower, but...
  - Sees all login events
  - Only parses known event IDs by collector agent

### NetAPI

- Polls the NetSessionEnum function on Windows every 9 seconds, or less\*
  - Authentication session table in RAM
- Retrieves login sessions, including DC login events
- Faster, but...
  - If DC has heavy system load, can miss some login events

Most recommended → Least recommended

\* The poll interval times are estimates. The interval times depend on the number of servers and network latency.

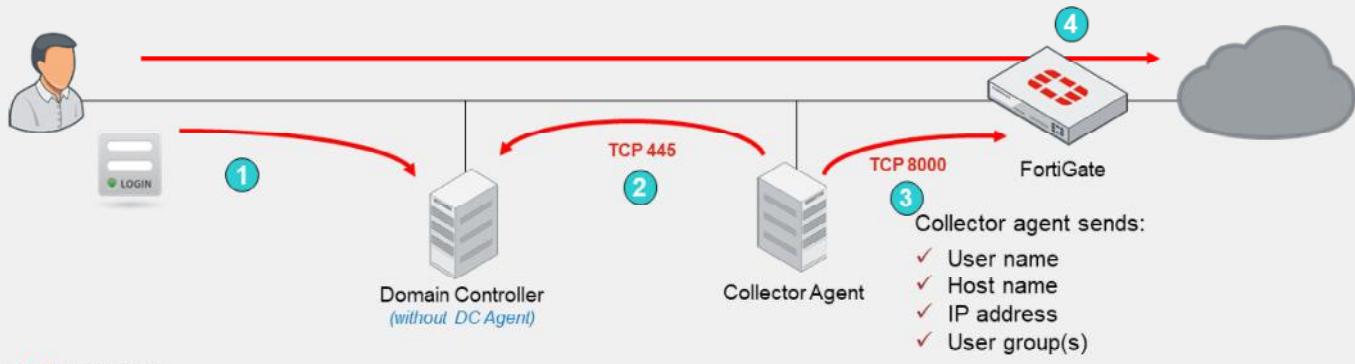
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **WMI:** is a Windows API that gets system information from a Windows server. The DC returns all requested login events. The collector agent is a WMI client and sends WMI queries for user login events to the DC, which, in this case, is a WMI server. The collector agent doesn't need to search security event logs on the DC for user login events; instead, the DC returns all requested login events. This reduces network load between the collector agent and DC.
- **WinSecLog:** polls all the security event logs from the DC. It doesn't miss any login events that have been recorded by the DC because events are not normally deleted from the logs. There can be some delay in FortiGate receiving events if the network is large and, therefore, writing to the logs is slow. It also requires that the audit success of specific event IDs is recorded in the Windows security logs. For a full list of supported event IDs, visit the Fortinet Knowledge Base (<http://kb.fortinet.com>).
- **NetAPI:** polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some login events if a DC is under heavy system load. This is because sessions can be quickly created and purged from RAM, before the agent has a chance to poll and notify FortiGate.

**DO NOT REPRINT**  
**© FORTINET**

## Collector Agent-Based Polling Mode Process

1. The user authenticates with the DC
2. The collector agent frequently polls the DCs to collect user login events
3. The collector agent forwards logins to FortiGate
4. The user does not need to authenticate



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

14

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

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

**DO NOT REPRINT****© FORTINET**

## Agentless Polling Mode

- Similar to agent-based polling, but FortiGate polls instead
- Doesn't require an external DC agent or collector agent
  - FortiGate collects the data directly
- Event logging must be enabled on the DCs
- More CPU and RAM required by FortiGate
- Support for polling option WinSecLog only
  - FortiGate uses the SMB protocol to read the event viewer logs
- Fewer available features than collector agent-based polling mode
- FortiGate doesn't poll workstation
  - Workstation verification is not available in agentless polling mode



© Fortinet Inc. All Rights Reserved.

15

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

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

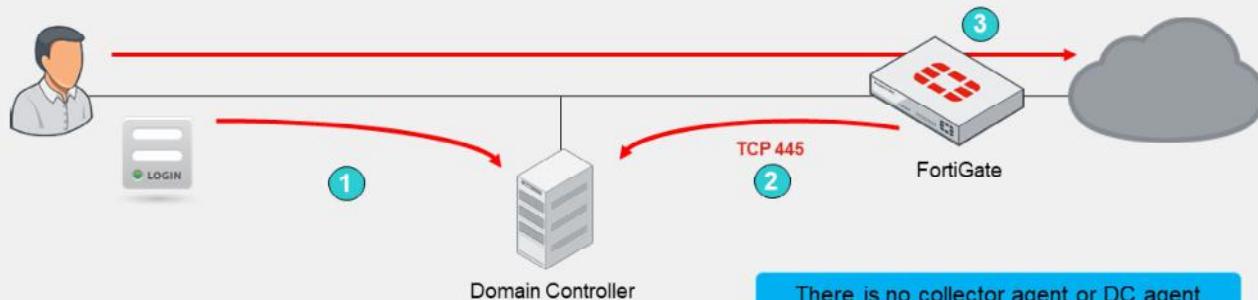
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

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

**DO NOT REPRINT**  
**© FORTINET**

## Agentless Polling Mode Process

1. FortiGate frequently polls DCs to collect user login events
2. The user authenticates with the DC
  - o FortiGate discovers the login event in next poll
3. The user does not need to authenticate
  - o FortiGate already knows whose traffic it is receiving



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

16

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

1. FortiGate polls the DC TCP port 445 to collect user login events.
2. After the user authenticates with the DC, FortiGate registers a login event during its next poll, obtaining the following information: the user name, the host name, and the IP address. FortiGate then queries for the user's user group(s).
3. When the user sends traffic, FortiGate already knows whose traffic it is receiving; therefore, the user does not need to authenticate.

**DO NOT REPRINT**

© FORTINET

## Comparing Modes

	DC agent mode	Polling mode
<b>Installation</b>	Complex—multiple installations (one per DC). Requires reboot.	Easy—one or no installations. No reboot required.
<b>DC agent required</b>	Yes	No
<b>Resources</b>	Shares with DC agents	Has own resources
<b>Scalability</b>	Higher	Lower
<b>Redundancy</b>	Yes	Yes
<b>Level of confidence</b>	Captures all logins	Might miss a login (NetAPI), or have a delay (WinSecLog)



© Fortinet Inc. All Rights Reserved.

17

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

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Additional FSSO AD Requirements

- The DNS server must be able to resolve all workstation names
  - Microsoft login events contain workstation names, but might not IP addresses
  - The collector agent uses a DNS server to resolve the workstation name to an IP address
- For full feature functionality, the collector agent must be able to poll workstations
  - This informs the collector agents whether or not the user is still logged in
  - TCP ports 445 (default) and 139 (backup) must be open between collector agents or FortiGate and all hosts
  - Remote registry service might be needed on each workstation



© Fortinet Inc. All Rights Reserved.

18

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

- Microsoft Windows login events have the workstation name and username, but not the workstation IP address. When the collector agent receives a login event, it queries a DNS server to resolve the IP address of the workstation. So, FSSO requires that you have your own DNS server. If a workstation IP address changes, DNS records must be updated immediately in order for the collector agent to be aware of the change and report them to FortiGate.
- For full feature functionality, collector agents need connectivity with all workstations. Since a monitored event log is not generated on logout, the collector agent (depending on the FSSO mode) must use a different method to verify whether users are still logged in. So, each user workstation is polled to see if users are still there.
- The DC agent, when the user logs in, intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which is the recommended mode for FSSO deployments?  
 A. DC agent mode  
 B. Polling mode: Agentless
  
2. Which FSSO mode requires more FortiGate system resources (CPU and RAM)?  
 A. Polling mode: Collector agent-based  
 B. Polling mode: Agentless

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



FSSO Function and Deployment



FSSO With Windows Active Directory



FSSO Settings



Troubleshooting

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

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

**DO NOT REPRINT**  
© FORTINET

## FSSO Settings

### Objectives

- Configure SSO settings on FortiGate
- Install FSSO agents
- Configure the Fortinet collector agent

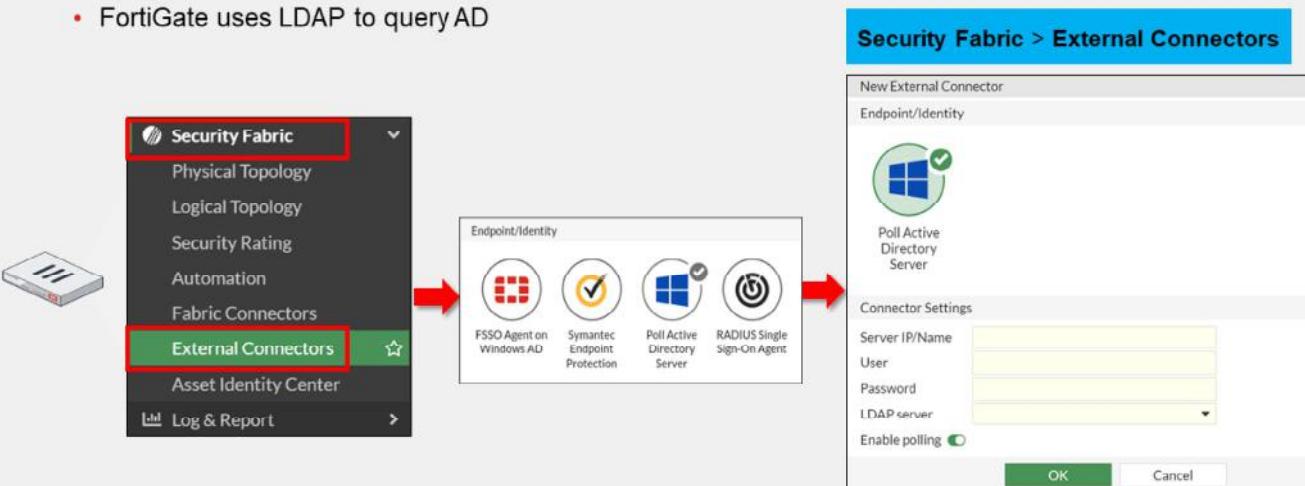
After completing this section, you should be able to achieve the objectives shown on this slide.

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

**DO NOT REPRINT**  
**© FORTINET**

## FSSO Configuration—Agentless Polling Mode

- Agentless polling mode:
  - FortiGate uses LDAP to query AD



FortiGate FSSO configuration is straightforward.

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

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

# DO NOT REPRINT

## © FORTINET

### FSSO Configuration—Collector Agent-Based Polling or DC Agent Mode

- Collector agent-based polling or DC agent mode:
  - The FSSO agent can monitor users' login information from AD, Exchange, Terminal, Citrix, and eDirectory servers

**Security Fabric > External Connectors**

Endpoint/Identity

- FSSO Agent on Windows AD
- Symantec Endpoint Protection
- Poll Active Directory Server
- RADIUS Single Sign-On Agent

New External Connector

FSSO Agent on Windows AD

User group source **Collector Agent Local**

LDAP server

Proactively retrieve from LDAP server

Connector Settings

Name

Primary FSSO agent

Server IP/Name

Password

Trusted SSL certificate

User group source **Collector Agent Local**

Users/Groups 0

Apply & Refresh OK Cancel

© Fortinet Inc. All Rights Reserved.

23

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

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

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

# DO NOT REPRINT

## © FORTINET

## FSSO Agent Installation

1. Visit the Fortinet support website:
  - <https://support.fortinet.com>
2. Click **Download > Firmware Images**
3. Select **FortiGate**, then click **Download**.
4. Click **v7.00 > 7.2 > 7.2.0 > FSSO**

Example image below:

The screenshot shows the Fortinet Support website interface. At the top, there's a navigation bar with links for Home, Asset Assistance, Download (which is highlighted in red), Feedback, FortiGuard Service Updates, Firmware Images (also highlighted in red), Firmware Image Checksums, and HQIP Images. Below this, a banner says "Welcome Please be a guest". On the left, there's a sidebar with "Home" and "Please be a guest". The main content area has a heading "Available agents:" followed by a list of agents. To the right, there's a "Select Product" dropdown set to "FortiGate", a "Release Notes" link, a "Download" button (which is blue and highlighted), an "Upgrade Path" link, and a "FortiGate Support Tool" link. Under "Image File Path", it shows "/FortiGate/v7.00/7.2/7.2.0/FSSO/". Below that is a table titled "Image Folders/Files" with a "Up to higher level directory" link. The table lists various files with their names, sizes, dates created, dates modified, and HTTPS checksums.

Name	Size (KB)	Date Created	Date Modified	HTTPS Checksum
DCAgent_Setup_5.0.0295.exe	3,445	2021-03-30 16:03:42	2021-03-30 16:03:43	HTTPS Checksum
DCAgent_Setup_5.0.0295.msi	3,112	2021-03-30 16:03:47	2021-03-30 16:03:48	HTTPS Checksum
DCAgent_Setup_5.0.0295_x64.exe	4,105	2021-03-30 16:03:53	2021-03-30 16:03:55	HTTPS Checksum
DCAgent_Setup_5.0.0295_x64.msi	3,772	2021-03-30 16:03:58	2021-03-30 16:03:59	HTTPS Checksum
FSSO_Setup_5.0.0295.exe	9,617	2021-03-30 16:03:36	2021-03-30 16:03:39	HTTPS Checksum
FSSO_Setup_5.0.0295_x64.exe	9,909	2021-03-30 16:03:04	2021-03-30 16:03:07	HTTPS Checksum
FSSO_Setup_x64directory_5.0.0295.exe	3,549	2021-03-30 16:03:56	2021-03-30 16:03:57	HTTPS Checksum
FSSO500WAT5_build0295.sum	1	2021-03-30 16:03:45	2021-03-30 16:03:45	HTTPS Checksum
TSAgent_Setup_5.0.0295.exe	4,465	2021-03-30 14:03:01	2021-03-30 14:03:03	HTTPS Checksum
TSAgent_Setup_5.0.0295.msi	4,132	2021-03-30 16:03:50	2021-03-30 16:03:52	HTTPS Checksum

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.

**DO NOT REPRINT**  
**© FORTINET**

## FSSO Collector Agent Installation Process

1. Run the installation process as Administrator
2. Enter the user name in the following format:
  - DomainName\UserName
3. Configure the collector agent for:
  - Monitoring logins
  - NTLM authentication
  - Directory access
4. Optionally, launch the DC agent installation wizard before exiting the collector agent installation wizard



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

25

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

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

**DO NOT REPRINT**  
**© FORTINET**

## DC Agent Installation Process

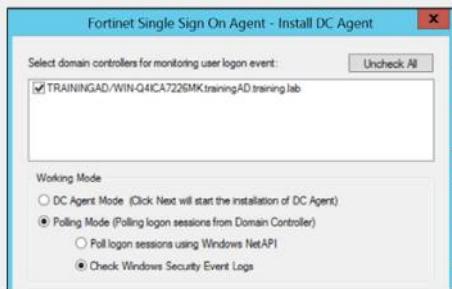
### 1 IP and port for collector agent



### 2 Domains to monitor



### 3 Remove users



4 Select domain controllers to install the DC agent

5 **DC Agent Mode** – to install DC agent on selected DC  
**Polling Mode** – DC agent will not be installed

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

26

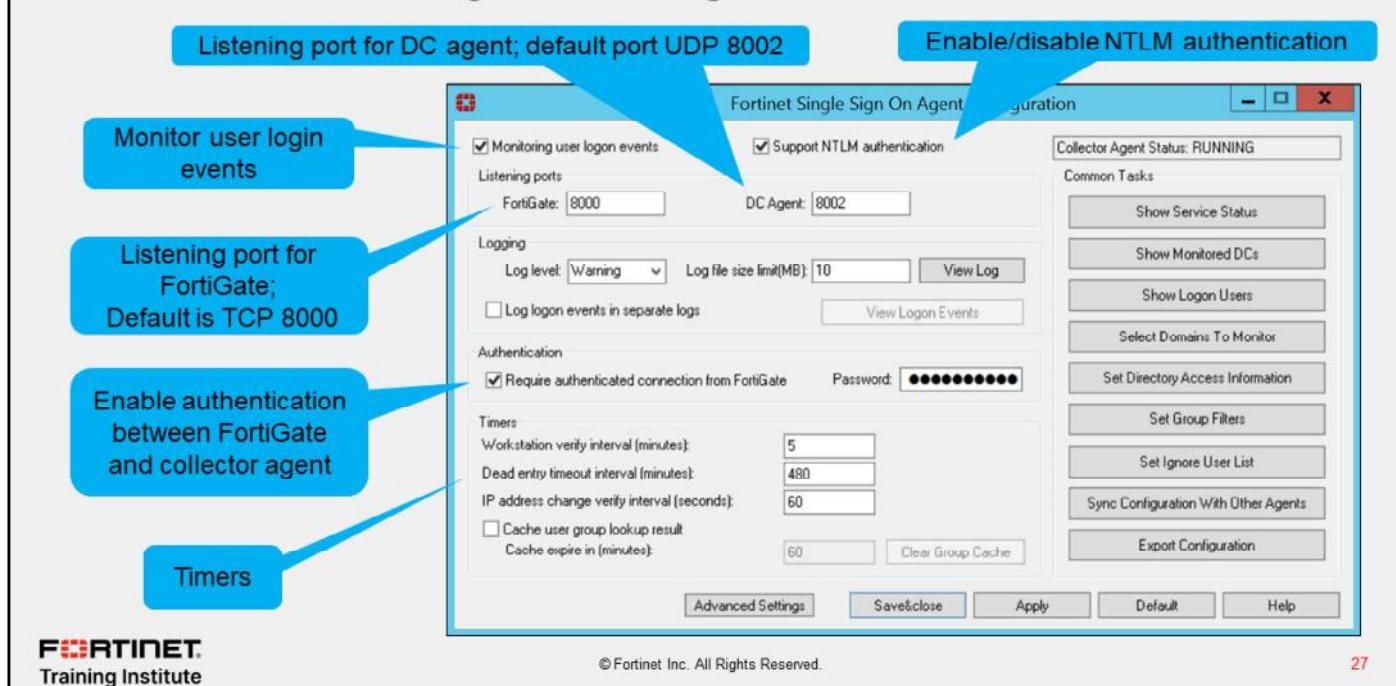
If you have just installed the collector agent and you selected **Launch DC Agent Install Wizard**, the installation process for domain controller agent automatically starts.

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

Finally, the wizard requests a system reboot.

**DO NOT REPRINT**  
**© FORTINET**

## FSSO Collector Agent Configuration



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

27

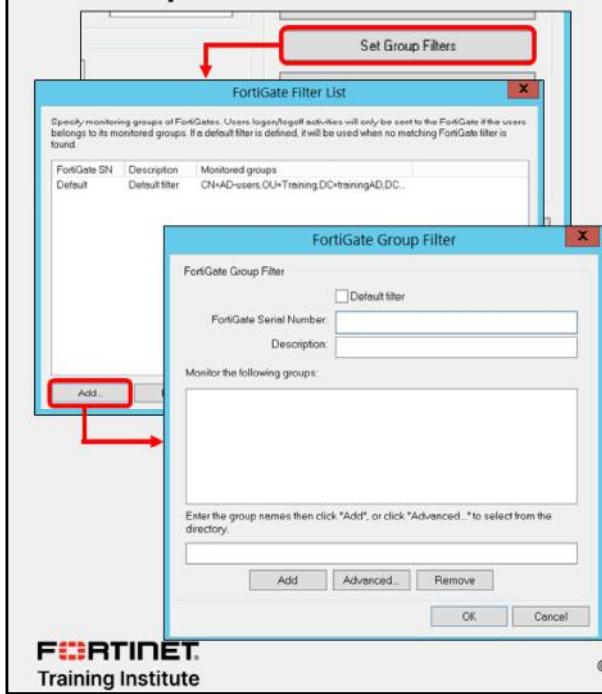
On the FSSO agent configuration GUI, you can configure settings such as:

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

# DO NOT REPRINT

## © FORTINET

### Group Filter



- The FSSO collector agent manages FortiGate group filters
- FortiGate group filters control which user's login information is sent to that FortiGate device
  - Filters are tied to the FortiGate serial number
- All FortiGate devices support at least 256 Windows AD user groups
  - The group filter support is for VDOMs
- If FortiGate FSSO is set up in user group source local mode (group filtering configured on FortiGate is pushed to Collector agent), FortiGate filter will take precedence over filter set on collector agent
- The default filter applies to any FortiGate device that does not have a specific filter defined in the list
- You can set filters for groups, OUs, users, or a combination

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

28

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

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

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

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

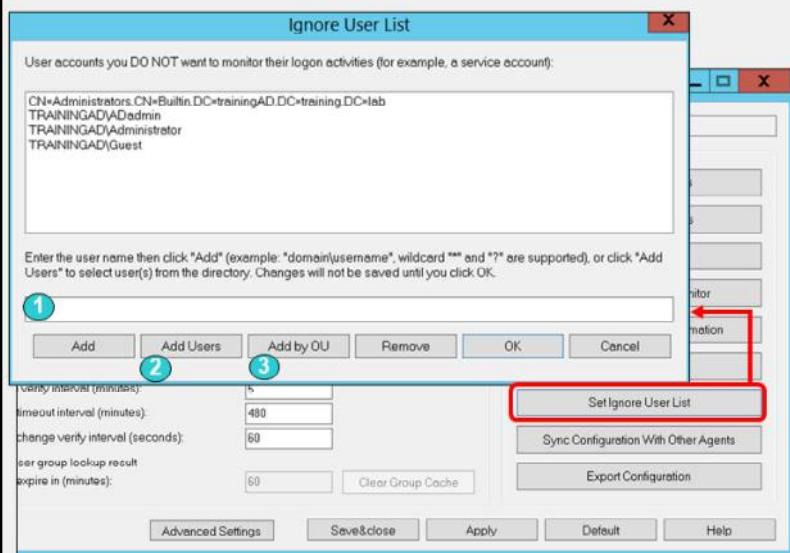
The filter list is initially empty. At a minimum, you should create a default filter that applies to all FortiGate devices without a defined filter.

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

# DO NOT REPRINT

## © FORTINET

### Ignored User List



- The collector agent ignores any login events that match the **Ignore User List** entries
  - Example: network service accounts
- User logins are not reported to FortiGate
- This helps to ensure users get the correct policies and profiles on FortiGate

To add users to the ignore list:

- Manual entry
- Add Users:** Select users you do not want to monitor
- Add by OU:** Select an OU from the directory tree
  - All users under the selected OU are added to the **Ignore User List**

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

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

You can add users to the **Ignore Users List** in the following ways:

- Manually enter the username.
- Click **Add Users**, and then choose the users you do not want to monitor.
- Click **Add by OU**, and then select an OU from the directory tree.

**DO NOT REPRINT****© FORTINET**

## Collector Agent Timers

### Workstation verify interval

- Verifies if a user is still logged on
- Uses remote registry service to verify
- Default: 5 minutes
- Disable: Set value to 0

Timers

Workstation verify interval [minutes]:	5
Dead entry timeout interval [minutes]:	480
IP address change verify interval [seconds]:	60
<input type="checkbox"/> Cache user group lookup result Cache expire in [minutes]:	60

### IP address change verify interval

- Important on DHCP or dynamic environments
- Default – 60 seconds

### Dead entry timeout interval

- Applies to unverified entries only
- Used to purge login information
- Default: 480 minutes (8h)
- Disable: Set value to 0

• Under the workstation verify interval

### Cache user group lookup result

- Collector agent remembers user group membership

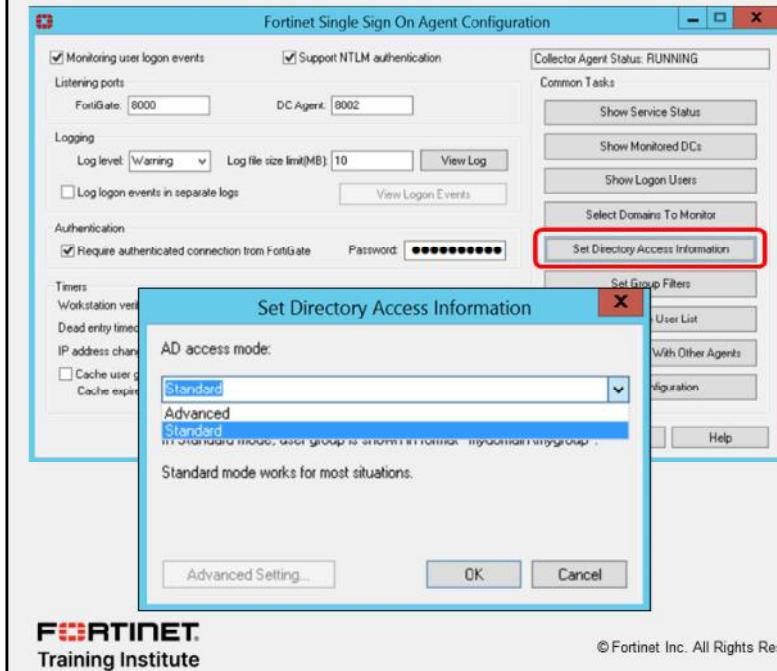
The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

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

- **Workstation verify interval.** This setting controls when the collector agent connects to individual workstations on port 139 (or port 445), and uses the remote registry service to verify if a user is still logged in to the same station. It changes the status of the user under **Show login User**, to **not verified** when it cannot connect to the workstation. If it does connect, it verifies the user and the status remains **OK**. To facilitate this verification process, you should set the remote registry service to auto start on all domain member PCs.
- **Dead entry timeout interval.** This setting applies only to entries with an unverified status. When an entry is not verified, the collector starts this timer. It's used to age out the entry. When the timer expires, the login is removed from the collector. From the perspective of FortiGate, there is no difference between entries that are **OK** and entries that are **not verified**. Both are considered valid.
- **IP address change verify interval.** This setting checks the IP addresses of logged in users and updates FortiGate when a user's IP address changes. This timer is especially important in DHCP or dynamic environments to prevent users from being locked out if they change IP address. The domain DNS server should be accurate; if the DNS server does not update the affected records promptly, the collector agent's IP information is inaccurate.
- **Cache user group lookup result.** This setting caches the user group membership for a defined period of time. It is not updated, even if the user changes group membership in AD.

**DO NOT REPRINT**  
**© FORTINET**

## AD Access Mode Configuration



### Standard Access Mode

- Windows convention:
  - Domain\groups
- UTM profiles to groups
  - Nested group is not supported
- Group filters at collector agent

### Advanced Access Mode

- LDAP convention user names:
  - CN=User, OU=Name, DC=Domain
- UTM profile to users, groups and OUs
  - Supports nested or inherited groups
- Group filtering:
  - FortiGate as an LDAP client, or group filter on collector agent
  - Filter groups defined on FortiGate

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

The main difference between modes is the naming convention used:

- **Standard** mode uses the Windows convention, NetBios: Domain\groups, while
- **Advanced** mode uses the LDAP convention: CN=User, OU=Name, DC=Domain.

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

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

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

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

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

**DO NOT REPRINT**

**© FORTINET**

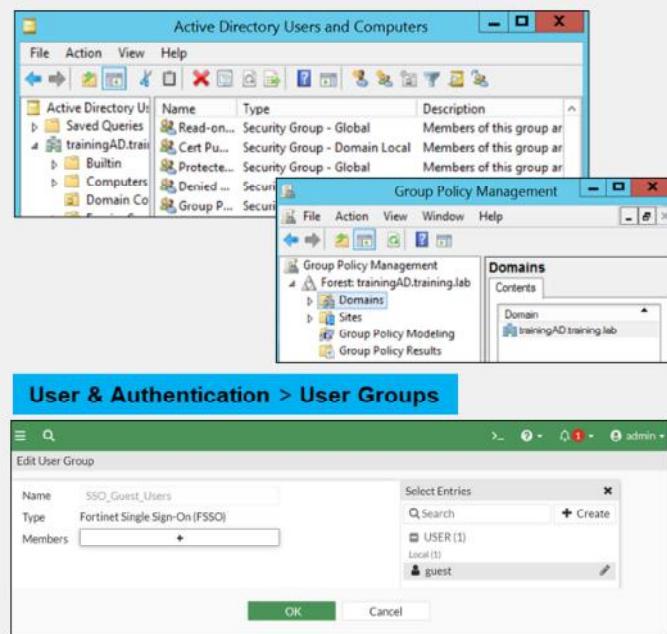
## AD Group Support

### Group type supported:

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

### If the user is not part of an FSSO group:

- For passive FSSO authentication:
  - User is part of **SSO\_Guest\_Users**
- For passive and active FSSO authentication:
  - User is prompted to log in



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

32

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

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

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## Advanced Settings

**Citrix/Terminal Server**

- Terminal server (TS) agent mode: monitors user logins in real time
- Requires a collector agent
  - No polling support from FortiGate

**RADIUS Accounting**

- Notify the firewall upon login and logout events

**Syslog Servers**

- Notify the firewall upon login and logout events

**Exchange Server**

- Monitor MS Exchange Server
- Allow users access to emails through the domain account
  - Accessing from the domain or not

© Fortinet Inc. All Rights Reserved. 33

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

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

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

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. If you have collector agents using either the DC agent mode or the collector agent-based polling mode, which fabric connector should you select on FortiGate?
  - A. Poll Active Directory Server
  - B. Fortinet Single Sign-On Agent
  
2. Which naming conventions does the FSSO collector agent use to access the Windows AD in **Standard** access mode?
  - A. Windows convention - NetBios: Domain\groups
  - B. LDAP convention: CN=User,OU=Name,DC=Domain

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



FSSO Function and Deployment



FSSO With Active Directory



FSSO Settings



Troubleshooting

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

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

**DO NOT REPRINT****© FORTINET**

## Troubleshooting

### Objectives

- Recognize and monitor FSSO-related log messages
- Perform basic FSSO troubleshooting

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

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

**DO NOT REPRINT**  
**© FORTINET**

## FSSO Log Messages on FortiGate

- FSSO logs are generated from authentication events, such as user login and logout events and NTLM authentication events
  - To log all events, set the minimum log level to **Notification** or **Information**

The screenshot shows the FortiGate Log & Report interface. At the top, there's a navigation bar: **Log & Report > System Events > User Events**. Below this is a table of log entries:

User	Action	Message
ADUSER1	authentication	User ADUSER1 succeeded in logout
ADUSER1	FSSO-logoff	FSSO-logoff event from TrainingDomain: user ADUSER1 logged off 10.0.1.10
ADUSER1	FSSO-logon	FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10

Below the table, there's a detailed view of the last log entry (FSSO-logon). It shows:

- Event:** Message: FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10
- Other:** Destination: TrainingDomain, Log ID: **43014**, Sub Type: user, roll: 65533

On the right, there's a table of log messages with columns: **Message ID**, **Severity**, and **Description**:

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication successful
43013	Notification	FSSO authentication failed
<b>43014</b>	<b>Notification</b>	<b>FSSO user logged on</b>
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication successful
43017	Notification	NTLM authentication failed

A red arrow points from the Log ID '43014' in the event details to the corresponding row in the message log table.

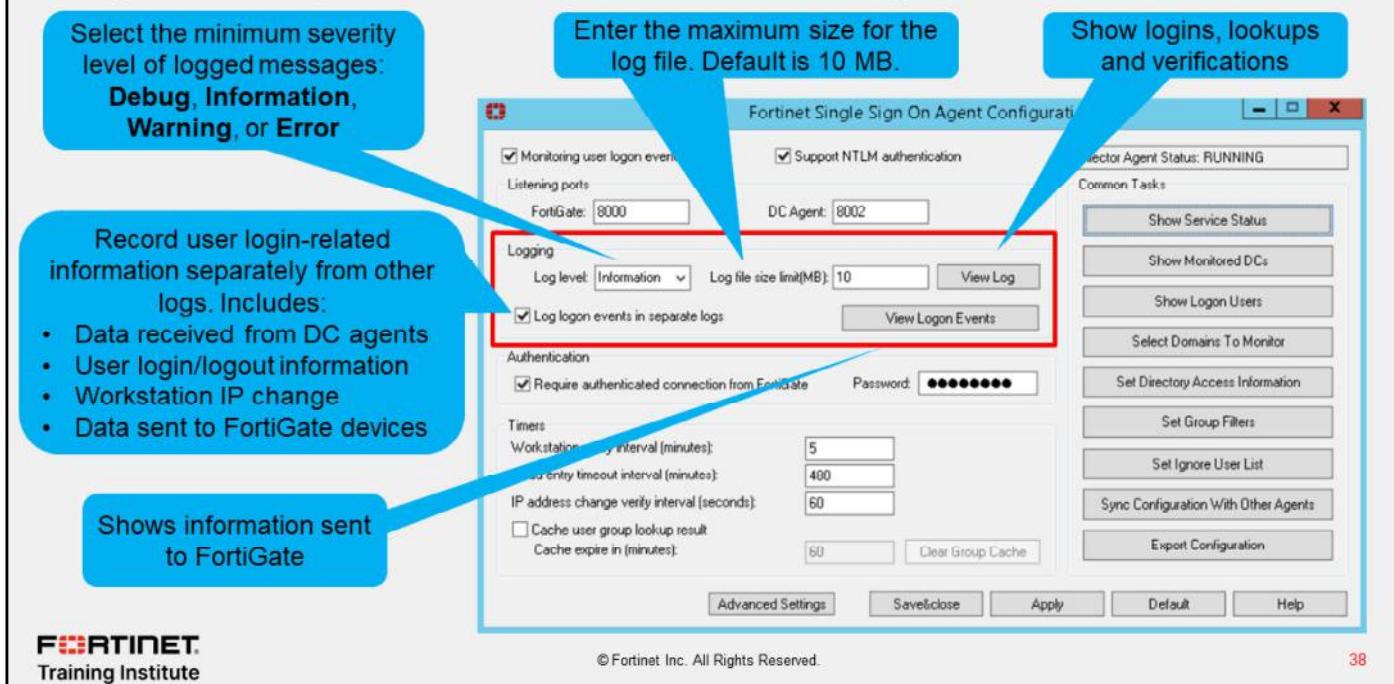
At the bottom left is the **FORTINET Training Institute** logo. At the bottom center is the text: © Fortinet Inc. All Rights Reserved. At the bottom right is the number 37.

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Log Messages on FSSO Collector Agent



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

38

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

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

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

# DO NOT REPRINT

## © FORTINET

### Troubleshooting Tips for FSSO

1. Ensure all firewalls allow the FSSO required ports
  - For example: ports 139 (workstation verification), 445 (workstation verification and event log polling), 389 (LDAP), 445, 636 (LDAPS), and 3268, 3269 (TLS)
2. Guarantee at least 64 Kbps bandwidth between FortiGate and domain controllers
  - Configure traffic shaping to ensure the minimum bandwidth is always available
3. Configure the timeout timer to flush inactive sessions after a shorter time
  - Alternatively, encourage users to log out of one machine before logging in to another machine
4. Ensure DNS is configured and updating IP addresses if the host IP address changes
5. Never set the timer workstation verify interval to 0
  - This prevents the collector agent from aging out stale entries. They can be removed only by a new event overwriting them
  - This can be dangerous in environments where FSSO and non-FSSO users share the same DHCP pool
6. Include all FSSO groups in the firewall policies when using passive authentication
  - Even add the SSO\_Guest\_Users to an identity-based security policy to allow traffic
  - If active authentication is used as a backup, ensure that SSO\_Guest\_User is not added to policies



© Fortinet Inc. All Rights Reserved.

39

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Currently Logged-On Users

The screenshot illustrates the integration of Fortinet Single Sign-On (FSSO) with FortiGate. It shows both command-line interface (CLI) output and a graphical user interface (GUI) dashboard.

**CLI Output:**

```
# diagnose debug authd fssso list
----FSSO logins----
IP: 10.0.1.10 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training
IP: 192.168.131.5 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training

Total number of logins listed: 2, filtered: 0
----end of FSSO logins----
```

Annotations for the CLI output:

- IP address:** Points to the IP address 10.0.1.10.
- User name:** Points to the user name ADUSER1.
- User group:** Points to the user group TRAININGAD/AD-USERS.
- Workstation name:** Points to the workstation name WIN-INTERNAL.
- Group created on FortiGate:** Points to the entry "MemberOf: Training".

**Dashboard > Users & Devices > Firewall Users:**

The dashboard shows two users:

- Method:** Fortinet Single Sign-On
- User Group:** Training (green), TRAININGAD/AD-USERS (orange)
- Users:** 1 (green circle), 2 (orange circle)

Annotations for the GUI:

- # execute fssso refresh**: A blue box containing the CLI command to manually refresh user group information.
- User Group:** Training
- Members:** TRAININGAD/AD-USERS
- Group Type:** Fortinet Single Sign-On (FSSO)

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Connection to FortiGate

- Check connectivity between collector agent and FortiGate

```
# diagnose debug enable
# diagnose debug authd fssso server-status

  Server Name      Connection Status      Version          Address
-----  -----  -----
TrainingDomain    connected           FSAE server 1.1    10.0.1.10
```



© Fortinet Inc. All Rights Reserved.

41

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

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

**DO NOT REPRINT****© FORTINET**

## Additional Commands

# diagnose debug authd fss0 <...>	
filter	Filters used for list or clear logins
list	Show currently logged on users
refresh-groups	Refresh group mapping
summary	Summary of currently logged on users
clear-logins	Delete cached login status
refresh-logins	Resynchronize login database
server-status	Show status of FSSO server connection
# diagnose firewall auth clear	Clears all filtered users
# diagnose firewall auth filter	Filter specific group, id, and so on
# diagnose firewall auth list	List authenticated users

Also, available under `diagnose debug authd fss0` are commands for clearing the FortiGate cache of all currently logged in users, filtering the display of the list of logged in users, and refreshing the login and user group information.

# DO NOT REPRINT

## © FORTINET

### Polling Mode

```
diagnose debug fssso-polling detail
AD Server Status:
ID=1, name(10.0.1.10),ip=10.0.1.10,source(security),users(0)
port=auto username=administrator
read log offset=251636, latest login timestamp: Wed Feb 4 09:47:31 2015
polling frequency: every 10 second(s) success(246), fail(0)
LDAP query: success(0), fail(0)
LDAP max group query period(seconds): 0
most recent connection status: connected
```

Status of polls by FortiGate to DC

```
diagnose debug fssso-polling refresh-user
refresh completes. All login users are obsolete. Please re-login to make them available.
```

Active FSSO users

```
diagnose sniffer packet any 'host ip address and tcp port 445'
```

```
diagnose debug application fssod -1
```

Sniff polls



© Fortinet Inc. All Rights Reserved.

43

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which logging level shows the login events on the collector agent?  
 A. Information  
 B. Warning
  
2. The command diagnose debug fssso-polling detail displays information for which mode of FSSO?  
 A. Agentless polling  
 B. Collector agent-based polling

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Fortinet FSSO Function and Deployment



FSSO with Active Directory



FSSO Settings



Troubleshooting

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Define SSO and FSSO
- ✓ Understand FSSO deployment and configuration
- ✓ Detect user login events in Windows AD using FSSO
- ✓ Identify FSSO modes for Windows AD
- ✓ Configure SSO settings on FortiGate
- ✓ Install FSSO agents
- ✓ Configure a Fortinet collector agent
- ✓ Recognize and monitor FSSO-related messages
- ✓ Perform basic FSSO troubleshooting



© Fortinet Inc. All Rights Reserved.

46

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

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

DO NOT REPRINT

© FORTINET



## FortiGate Infrastructure

ZTNA



Last Modified: 23 August 2022

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

DO NOT REPRINT

© FORTINET

## Lesson Overview

ZTNA Introduction

Comparing ZTNA to SSL and IPSec VPN

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

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

**DO NOT REPRINT**

**© FORTINET**

## ZTNA

### Objectives

- Understand the benefits of using ZTNA
- Understand the fundamentals of ZTNA
- Understand how to establish device identity and trust
- Understand SSL certificate-based authentication
- Configure ZTNA access on FortiOS
- Describe types of ZTNA configuration

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

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

# DO NOT REPRINT

© FORTINET

## What is ZTNA?

- Access control method that provides role-based application access
- ZTNA method uses:
  - Client device identification
  - Authentication
  - Zero-trust tags
- Provides flexibility to manage both on-net and off-net users
- ZTNA has two modes:
  - ZTNA access proxy
  - IP/MAC-based access control (on-fabric, devices for IT compliances, and rules enforcement)



© Fortinet Inc. All Rights Reserved.

4

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

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

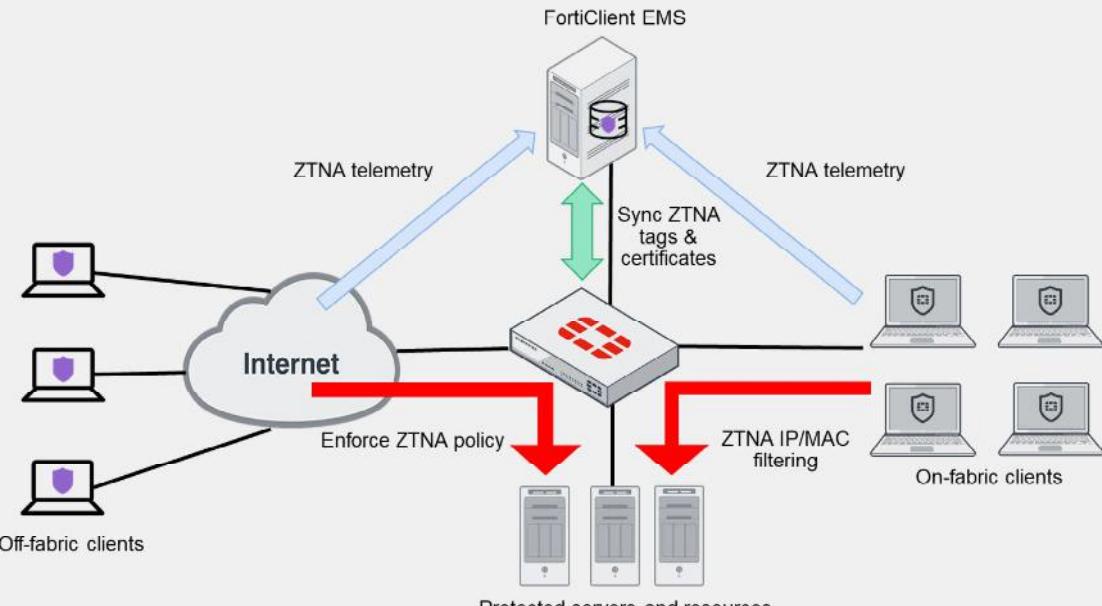
ZTNA has two modes:

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

# DO NOT REPRINT

## © FORTINET

### ZTNA Workflow



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

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

# DO NOT REPRINT

## © FORTINET

### Device Roles

- Device identity and trust are integral to ZTNA
- Identity is established through client certificates
- Trust is established between:
  - FortiClient
    - Provides endpoint information (device information, logged on users, and security posture)
    - Obtains client certificate from FortiClient EMS
  - FortiClient EMS
    - Issues and signs the client certificate
    - Synchronizes certificate to FortiGate
    - Uses tagging rules to tag endpoints
  - FortiGate
    - Maintains continuous connection to FortiClient EMS to synchronize endpoint information
    - When device information changes, FortiClient EMS updates FortiGate
    - FortiGate WAD daemon uses this information when processing ZTNA traffic



© Fortinet Inc. All Rights Reserved.

6

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

FortiClient provides the following information to FortiClient EMS when it registers:

- Device information (network details, operating system, model, and so on)
- Logged in user information
- Security posture (on-fabric and off-fabric, antivirus software, vulnerability status, and so on)

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

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

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

**DO NOT REPRINT****© FORTINET**

## FortiClient

- Provides a comprehensive network security solution for endpoints while improving your visibility and control
  - Allows you to manage security of multiple endpoints from the FortiClient EMS
  - Allows you to manage endpoints locally or remotely, stationary or mobile, using FortiClient EMS
  - Supports multiple platform protection:
    - Windows devices
    - Mac OS devices
    - Linux OS devices
    - iOS devices
    - Android mobile devices
    - Chromebook



© Fortinet Inc. All Rights Reserved.

7

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

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

**DO NOT REPRINT****© FORTINET**

## FortiClient (Contd)

- FortiClient is used with EMS to use all APT and security features
- FortiClient must connect to FortiClient EMS to activate the license
- You can change FortiClient configurations only from the management device
- FortiClient is either used with FortiClient EMS only or in the Security Fabric
- Enforces endpoint compliance and provides endpoint awareness
- Automates prevention of known and unknown threats
- Provides secure remote access



© Fortinet Inc. All Rights Reserved.

8

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## FortiClient EMS

- FortiClient EMS is a security management solution that enables:
  - Scalable and centralized management of multiple endpoints (computers)
  - Efficient and effective administration of endpoints running FortiClient
- Provides visibility across the network to securely share information and assign security profiles to endpoints
- Works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users
- Designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users



© Fortinet Inc. All Rights Reserved.

9

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

FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:

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

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

# DO NOT REPRINT

## © FORTINET

## FortiGate and FortiClient EMS Connectivity

- FortiGate uses FortiClient EMS fabric connector to connect
- FortiGate must verify the FortiClient EMS server certificate
  - Need to install CA certificate on FortiGate, otherwise certificate is not trusted
- FortiClient EMS must authorize the FortiGate as fabric device

**Security Fabric > Fabric Connectors**

**Administration > Fabric Devices**

**FortiClient EMS GUI**

**Fabric connector status**

**Fortinet Training Institute**

© Fortinet Inc. All Rights Reserved.

10

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

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

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

# DO NOT REPRINT

## © FORTINET

### Zero-Trust Tagging Rules

- You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android
- When using tagging rules with EMS and FortiClient
  - EMS sends zero-trust tagging rules to endpoints
  - FortiClient checks endpoints using the provided rules and sends the results to EMS
  - EMS dynamically groups endpoints together using the tag configured for each rule
  - You can view the dynamic endpoint groups in **Zero Trust Tags > Zero Trust Tag Monitor**

Endpoint	User	OS	IP	Tagged on
Remote-Client	Administrator	Microsoft Windows Ser ...	10.0.2.20	2021-08-26 02:43:06

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## FortiClient EMS Certificate Management

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

The screenshot shows the 'EMS Settings' page under 'System Settings > EMS Setting'. The 'EMS CA certificate (ZTNA)' section is highlighted with a red box. It displays two certificates: 'FCTEMS0000101875.1' (valid until 2030-01-19) and 'default\_ZTNARootCA.pem' (valid until 2046-07-16). A refresh button is visible next to the second certificate.

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

12

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

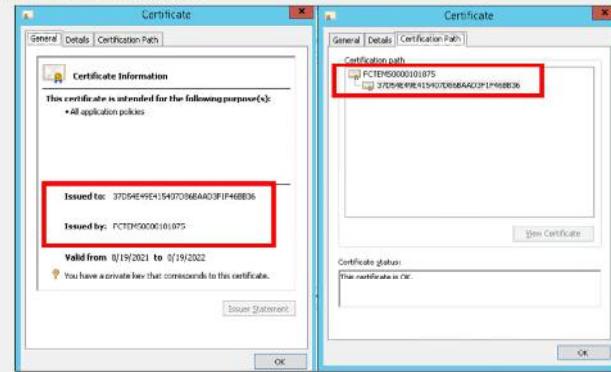
Do not confuse the FortiClient EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by FortiClient EMS for HTTPS access and fabric connectivity to the FortiClient EMS server.

**DO NOT REPRINT**  
**© FORTINET**

## FortiClient EMS Certificate Management (Contd)

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

```
FG-Fortigate # diagnose endpoint record list
Record #1:
  IP Address = 10.0.1.100
  MAC Address = 00:50:56:a1:1b:15
  MAC list = 00:50:56:a1:19:7e,00:50:56:a1:1b:15;
  VDOM = root (0)
  EMS serial number: FCTEM60000101875
  Client cert SN: 64415C90D00FFA3EAA50A22DAB07255FB45B9
  Pub. IP address: 206.47.132.124
  Quarantined: no
  Online status: online
  Registration status: registered
  On-net status: on-net
  Gateway Interface: port3
  FortiClient version: 7.0.0
  AVDB version: 88.336
  FortiClient app signature version: 10.143
  FortiClient app compatibility mode engine version: 2.31
  FortiClient URL: 370542498114070685A03F1740BB36
  Host Name: AD-Server
  OS Type: WIN84
  OS Version: Microsoft Windows Server 2012 R2 Standard Edition, 6
  4-bit (Build 9600)
  Host Description:
  Domain: trainingAD.training.lab
  Last Login User: Administrator
  Owner:
  Host Model: VMware Virtual Platform
  Host Manufacturer: VMware, Inc.
```



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

13

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## SSL Certificate-Based Authentication

- An endpoint obtains a client certificate when it registers to FortiClient EMS
- FortiClient automatically submits CSR request
- FortiClient EMS signs and returns the client certificate
- Certificate is stored in OS certificate store
- By default:
  - Client certificate authentication is enabled on access proxy
  - Empty certificate response is set to block
  - Options can be configured on CLI only

```
config firewall access-proxy
    edit <name>
        set client-cert enable
        set empty-cert-action block
    end
```

- Currently, ZTNA supports the Microsoft Edge and Google Chrome browsers



© Fortinet Inc. All Rights Reserved.

14

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

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

If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:

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

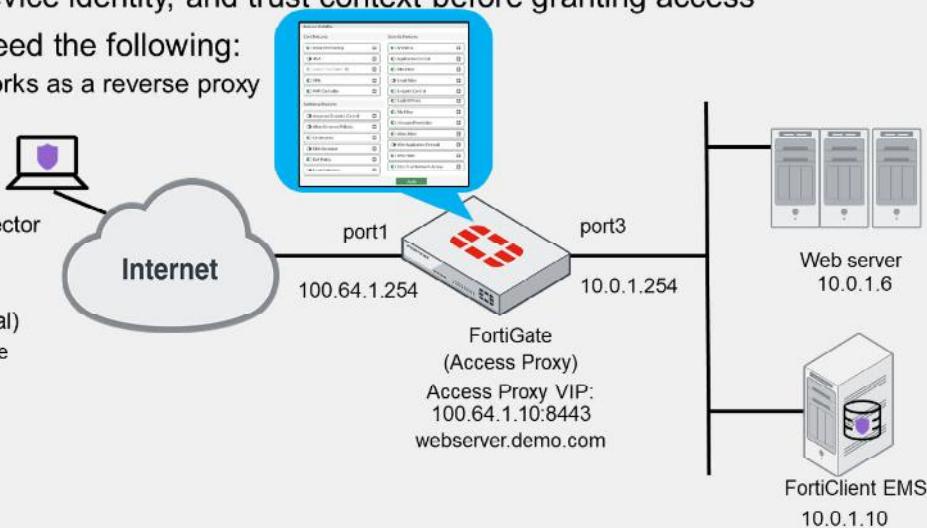
If the client cancels and responds with an empty client certificate, the client is allowed to continue with ZTNA proxy rule processing when you can set `empty-cert-action` to `accept`. If `empty-cert-action` is set to `block`, FortiGate blocks the client from further ZTNA proxy rule processing.

# DO NOT REPRINT

## © FORTINET

### ZTNA HTTPS Access Proxy

- HTTPS access proxy works as a reverse proxy
- Verifies user identity, device identity, and trust context before granting access
- To deploy ZTNA, you need the following:
  - HTTPS access proxy works as a reverse proxy
  - FortiClient endpoint
  - FortiClient EMS
  - FortiGate
    - FortiClient EMS connector
    - ZTNA server
    - ZTNA rule
    - Authentication (optional)
      - Explicit proxy enable



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

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

ZTNA configuration on FortiGate requires the following configuration:

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

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

**DO NOT REPRINT**  
**© FORTINET**

## ZTNA HTTPS Access Proxy (Contd)

- ZTNA server

**Policy & Objects > ZTNA > ZTNA Servers**

**ZTNA Server Configuration:**

- Name: ZTNA-webserver
- Comments:
- Network:
- Service: HTTPS
- External Interface: **SSL-VPN**
- External IP: 100.64.1.250
- External port: 9463
- Server/Service Mappings:
  - + Create New
  - Service # URL #
  - HTTPS www.example2.com/map1

**Virtual host matching rules:**

- Virtual Host: Any Host, Specify
- Match by: Substring
- Host: www.example2.com
- Use certificate: Fortinet\_CA\_SSL
- Match path by: Substring, Wildcard, Regular Expression
- Path: /map1

**Real server IP address and port:**

IP:	10.0.1.250
Port:	443
Status:	Active

- ZTNA rule

**Policy & Objects > ZTNA > ZTNA Rules**

**ZTNA Rule Configuration:**

- Name: ZTNA-Deny-Malicious
- Source: all
- ZTNA Tag: Malicious-File-Detected
- ZTNA Server: ZTNA-webserver
- Action: **ACCEPT** (checkbox checked)

**Denying access based on malicious tag:**

Comments: Write a comment... 0/4093

Enable this policy:

**FORTINET.**  
 Training Institute

16

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

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

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

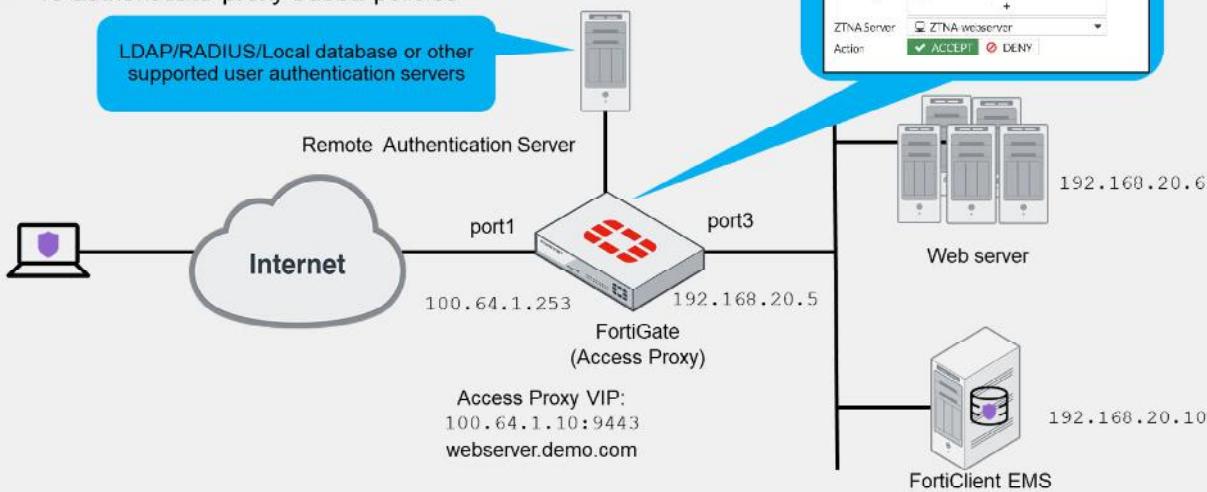
# DO NOT REPRINT

## © FORTINET

### ZTNA HTTPS Access Proxy With Basic Authentication

- You can add authentication to the access proxy
- Requires authentication scheme and authentication rule
  - To authenticate proxy-based policies

LDAP/RADIUS/Local database or other supported user authentication servers



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

17

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

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

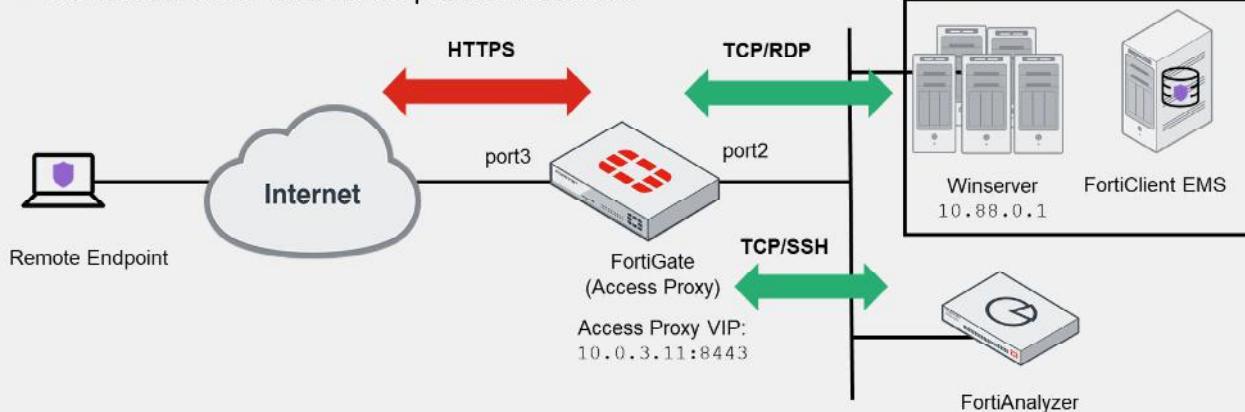
The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they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

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

**DO NOT REPRINT**  
**© FORTINET**

## ZTNA TCP Forwarding Access Proxy

- TCP forwarding access proxy demonstrates an HTTPS reverse proxy that forwards TCP traffic to the resource
- TCP forwarding access proxy:
  - Tunnels TCP traffic between the client and FortiGate over HTTPS
  - Forwards the TCP traffic to the protected resource



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

18

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

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

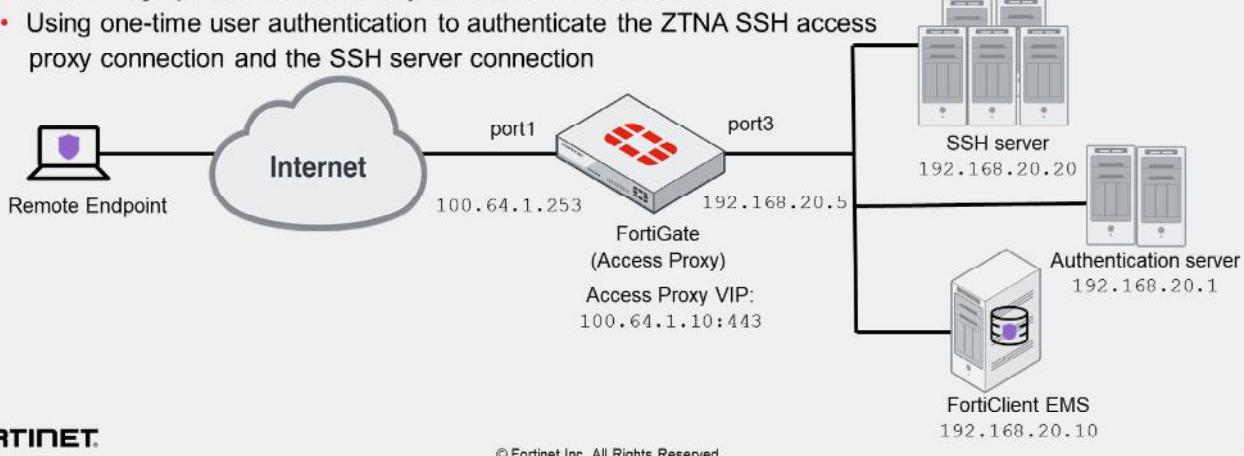
You can also add authentication and a security posture check for TCP Forwarding Access Proxy, which you learned about earlier in this lesson.

**DO NOT REPRINT**

**© FORTINET**

## ZTNA SSH Access Proxy

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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

19

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

Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:

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

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

**DO NOT REPRINT**  
**© FORTINET**

## ZTNA IP/MAC-Based Access Control

- ZTNA IP/MAC-based access control enhances security when endpoints are physically on the corporate network
  - Use ZTNA tags to control access
- IP/MAC-based access control focuses on access for fabric users
- This mode does not require the use of the access proxy, and only uses ZTNA tags for access control

**ZTNA IP/MAC-based firewall policy**

Name:	Block-Malicious
Incoming Interface:	port3
Outgoing Interface:	port1
Source:	all
IP/MAC Based Access Control:	FCTEMS_ALL_FORTICLOUD_SEI
Destination:	all
Schedule:	always
Service:	ALL
Action:	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
<input checked="" type="checkbox"/> Log Violation Traffic	
Comments:	Write a comment... 0/1023
<input checked="" type="checkbox"/> Enable this policy	

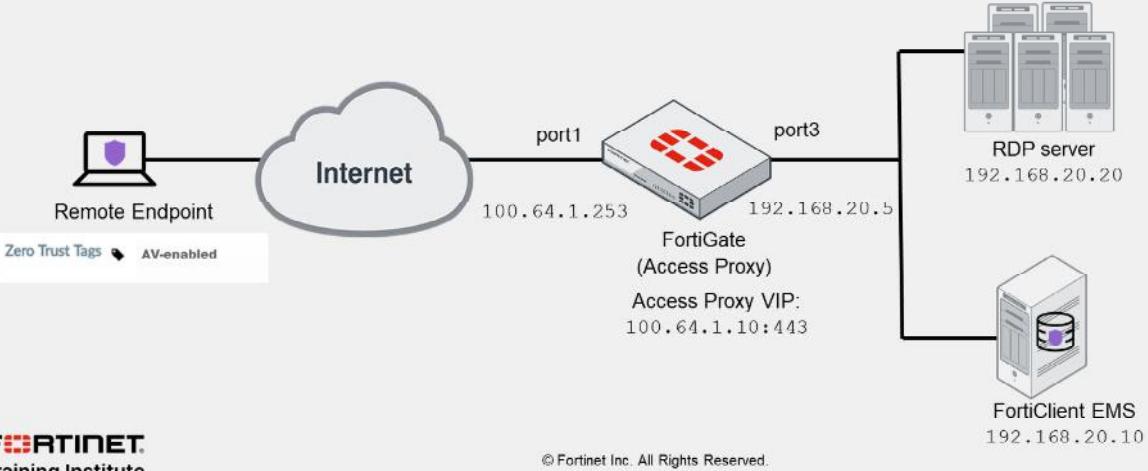
ZTNA IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for fabric users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check, to implement role-based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

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

**DO NOT REPRINT**  
**© FORTINET**

## Posture Check Verification for Active ZTNA Session

- Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified
  - Terminates session if the endpoint is no longer compliant with the ZTNA policy
- FortiGate monitors changes to the endpoint tags, when FortiGate detects change:
  - The endpoint's active session must reevaluate again to match the ZTNA policy before a data can pass



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

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

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which component issues and signs the client certificate?

- A. FortiClient EMS
- B. FortiClient

2. Which internet browser supports Fortinet ZTNA?

- A. Firefox
- B. Chrome

DO NOT REPRINT

© FORTINET

## Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPsec VPN

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

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

**DO NOT REPRINT**

**© FORTINET**

## Comparing ZTNA to SSL and IPsec VPN

### Objectives

- Describe the differences between SSL VPN, IPsec VPN, and ZTNA access
- Understand the evolution of teleworker remote access with ZTNA

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

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

**DO NOT REPRINT**

**© FORTINET**

## Comparing SSL VPN, IPsec VPN, and ZTNA Access

	IPsec VPN	SSL VPN	ZTNA
Tunnel type:	IPsec tunnel only	Session-based OR tunnel	Session-based only
Configured between:	FortiClient and FortiGate FortiGate and FortiGate FortiGate and compatible third-party IPsec VPN gateway FortiGate and compatible third-party IPsec VPN clients	Browser and FortiGate FortiClient and FortiGate FortiGate (SSL Client) and FortiGate (SSL Server)	Browser and FortiGate FortiClient and FortiGate (TCP forwarding access)
Log in through:	IPsec client	HTTPS web page on FortiGate FortiClient FortiGate (SSL Client)	HTTPS hostname or IP and port number FortiClient (TCP forwarding access)



© Fortinet Inc. All Rights Reserved.

25

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

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

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

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

# DO NOT REPRINT

## © FORTINET

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

	IPsec VPN	SSL VPN	ZTNA
Category:	Industry standard	Vendor specific	Vendor specific
<b>Ease of use (Configuration):</b>	<ul style="list-style-type: none"> <li>Requires installation</li> <li>Flexible setup               <ul style="list-style-type: none"> <li>Mesh and star topologies</li> <li>For clients or peer gateways</li> <li>Performance based: IPsec cryptography is faster in FortiOS</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Does not require installation</li> <li>Simpler setup               <ul style="list-style-type: none"> <li>Client-to-FortiGate</li> <li>FortiGate-to-FortiGate</li> <li>No user-configured settings</li> <li>Technical support less requested</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Does not require installation</li> <li>Simpler setup               <ul style="list-style-type: none"> <li>Only client-to-FortiGate</li> <li>No user-configured settings</li> <li>Technical support less requested</li> </ul> </li> </ul>
<b>Better for:</b>	Office-to-office traffic Data centers	Provides flexibility tunnel-mode or session-based access	Session-based access only
<b>Attack surface protection</b>	<ul style="list-style-type: none"> <li>Traditional perimeter protection:               <ul style="list-style-type: none"> <li>Defends against external threats only</li> <li>Doesn't address threat inside the network</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Traditional perimeter protection:               <ul style="list-style-type: none"> <li>Defends against external threats only</li> <li>Doesn't address threat inside the network</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>zero-trust philosophy               <ul style="list-style-type: none"> <li>No one inside or outside should be trusted</li> <li>Based on identity authentication</li> </ul> </li> </ul>

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

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.

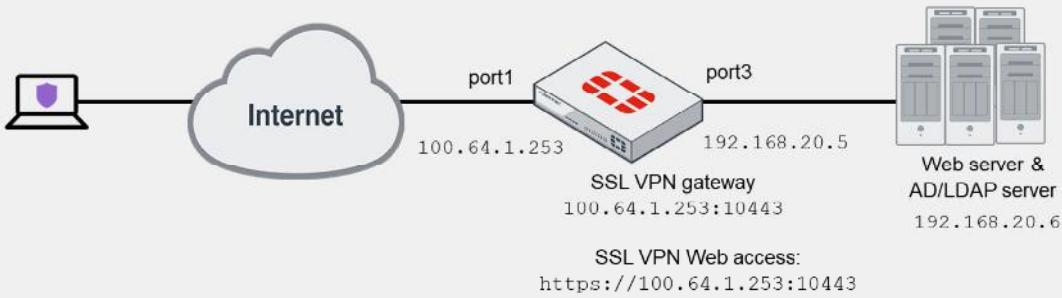
ZTNA follows the zero-trust philosophy to protect the attack surface that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. zero-trust also assumes that every attempt to access the network or an application is a threat.

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.

**DO NOT REPRINT****© FORTINET**

## Moving to ZTNA From SSL VPN

- You can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy



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

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

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

- A. ZTNA
- B. IPSec

2. What does FortiClient EMS integration ensure?

- A. Device identification
- B. User identification

DO NOT REPRINT

© FORTINET

## Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPSec  
VPN

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

29

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Understand the benefits and fundamentals of ZTNA
- ✓ Understand how to establish device identity and trust
- ✓ Understand SSL certificate-based authentication
- ✓ Configure ZTNA access on FortiOS
- ✓ Describe types of ZTNA configuration



© Fortinet Inc. All Rights Reserved.

30

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

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

**DO NOT REPRINT**

© FORTINET



**FORTINET**  
Training Institute



## FortiGate Infrastructure

### SSL VPN

 FortiOS 7.2

Last Modified: 13 June 2022

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

DO NOT REPRINT

© FORTINET

## Lesson Overview



### SSL VPN Deployment Modes



### Configuring SSL VPNs



### Monitoring and Troubleshooting

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT  
© FORTINET

## SSL VPN Deployment Modes

### Objectives

- Describe the differences between SSL VPN modes

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

**DO NOT REPRINT****© FORTINET**

## SSL VPN Deployment Modes

- Tunnel mode
  - Accessed through a FortiClient
  - Requires a virtual adapter on the client host
  
- Web mode
  - Requires only a web browser
  - Supports a limited number of protocols:
    - FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, Telnet, VNC, and Ping

The screenshot shows the 'Edit SSL-VPN Portal' configuration page. It includes fields for 'Name' (set to 'full-access'), 'Limit Users to One SSL-VPN Connection at a Time' (unchecked), 'Tunnel Mode' (checked), 'Tunnel Mode Client Options' (checkboxes for 'Allow client to save password', 'Allow client to connect automatically', 'Allow client to keep connections alive', and 'DNS Split Tunneling' are all unchecked), 'Restrict to Specific OS Versions' (unchecked), and 'Web Mode' (checked). The 'Tunnel Mode' and 'Web Mode' checkboxes are highlighted with red boxes.

```
config vpn ssl web portal
  edit <portal-name>
    set tunnel-mode [enable|disable]
    set web-mode [enable|disable]
  end
```

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

Which should you choose?

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

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

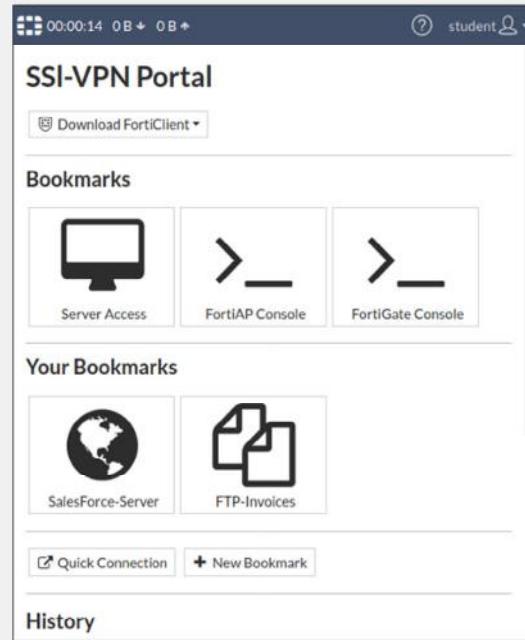
Web mode requires only a web browser, but supports a limited number of protocols.

# DO NOT REPRINT

## © FORTINET

### Web Mode

- Connect to the FortiGate SSL VPN portal from any browser
  - The web portal displays the status of SSL VPN
  - The SSL VPN stays up only while the SSL VPN portal page is open
- Access internal network resources easily using:
  - Bookmarks
  - Quick connection
- Disadvantages:
  - Interaction with the internal network exclusively by browser
    - Through the SSL VPN portal
    - External network applications cannot send data across the VPN
  - Limited number of protocols supported



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

Web mode is the simplest SSL VPN mode.

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

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

Web mode has two main disadvantages:

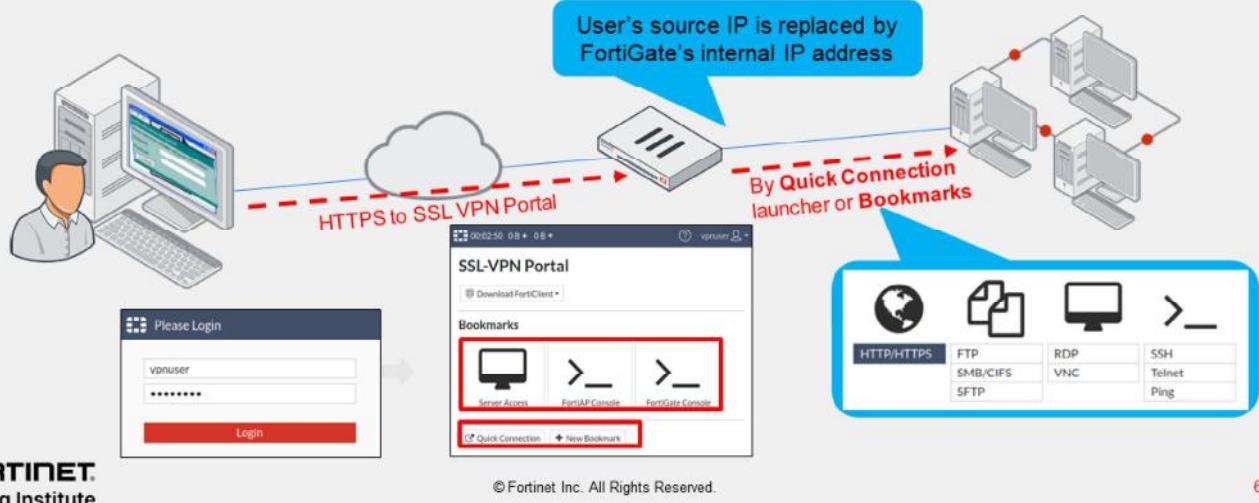
- All interaction with the internal network must be done using the browser exclusively (through the web portal). External network applications running on the user's PC cannot send data across the VPN.
- This a secure HTTP/HTTPS gateway mechanism that doesn't work for accessing everything, but just few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

# DO NOT REPRINT

## © FORTINET

### Web Mode (Contd)

1. Remote users connect to the SSL VPN portal—HTTPS web page on FortiGate
2. Users authenticate
3. Users access resources through the **Quick Connection** launcher or **Bookmarks**



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

6

How does web mode work?

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

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

**DO NOT REPRINT****© FORTINET**

## Tunnel Mode

- Connect to FortiGate through FortiClient
  - Tunnel is up only while the SSL VPN client is connected
  - FortiClient adds a virtual network adapter called `fortissl`
- FortiGate establishes the tunnel
  - Assigns a virtual IP address to the client from a pool of reserved addresses
  - All traffic is encapsulated with SSL/TLS
- Advantage:
  - Any IP network application on the client can send traffic through the tunnel
- Disadvantage:
  - Requires the installation of a VPN client

<http://www.forticlient.com/>



# FortiClient

Next Generation Endpoint Protection

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

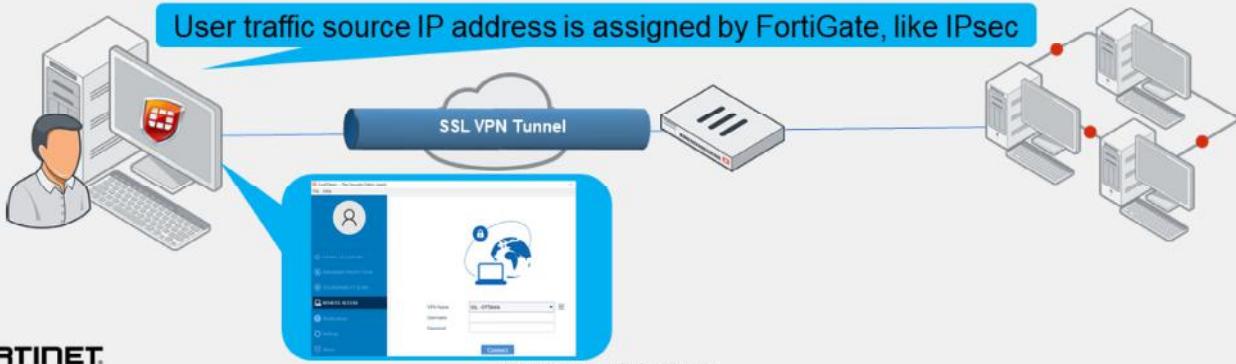
Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as `fortissl` to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is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

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

**DO NOT REPRINT****© FORTINET**

## Tunnel Mode (Contd)

1. Remote users connect to the SSL VPN gateway through the SSL VPN client
2. Users authenticate
3. The virtual adapter creates the tunnel
4. Users access resources through an encrypted tunnel (SSL/TLS)



8

How does tunnel mode work?

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

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

# DO NOT REPRINT

© FORTINET

## Tunnel Mode—FortiGate as Client

- Connect to server FortiGate device as SSL VPN client
  - Use SSL VPN *Tunnel* interface type
  - Devices connect to client FortiGate device can access the resources behind server FortiGate
- Tunnel establishes between two FortiGate devices
  - Hub-and-spoke topology
  - Client FortiGate dynamically adds route to remote subnets
  - Assigns a virtual IP address to the client FortiGate device from a pool of reserved addresses
- Advantage:
  - Any IP network application on the user machines connect to client FortiGate device can send traffic through the tunnel
  - Useful to avoid issues caused by intermediate devices, such as:
    - ESP packets being blocked.
    - UDP ports 500 or 4500 being blocked.
    - Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.
- Disadvantage:
  - Requires proper CA certificate on SSL VPN Server FortiGate
  - SSL VPN Client FortiGate user uses PSK and PKI client certificate to authenticate



© Fortinet Inc. All Rights Reserved.

9

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

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

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

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

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