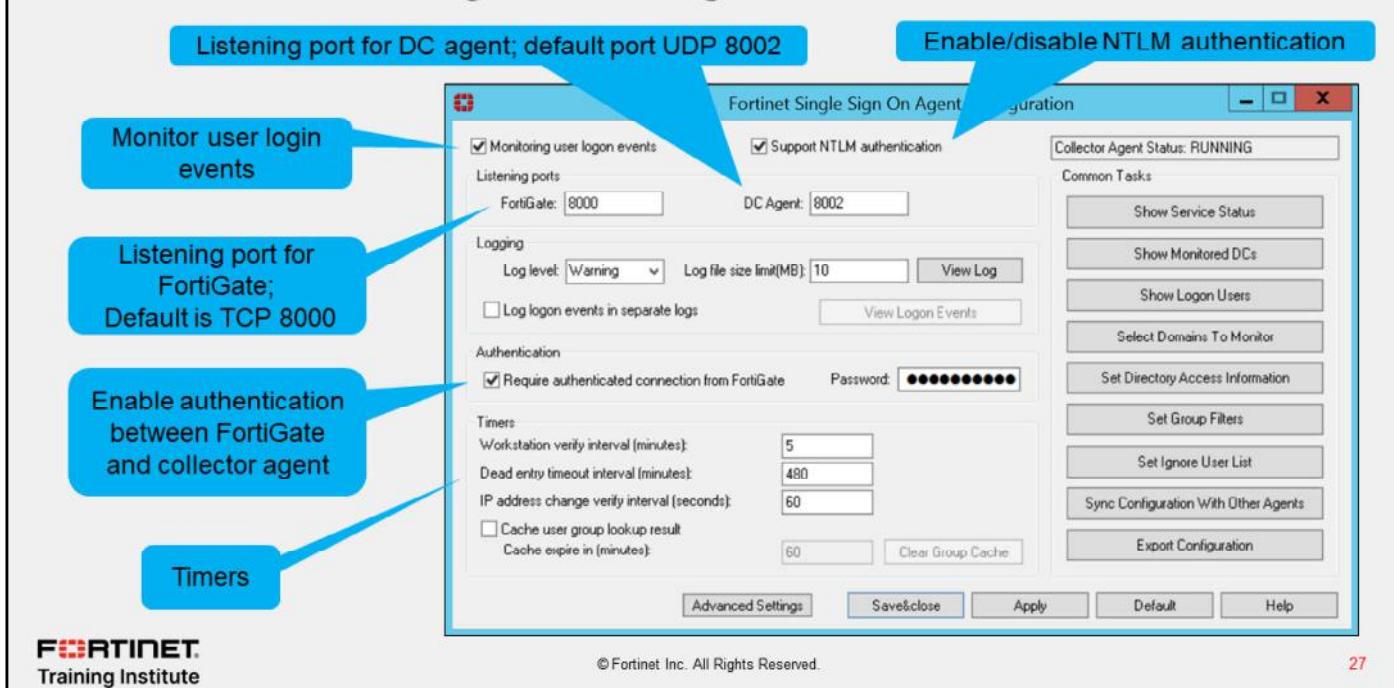


DO NOT REPRINT
© FORTINET

FSSO Collector Agent Configuration



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

27

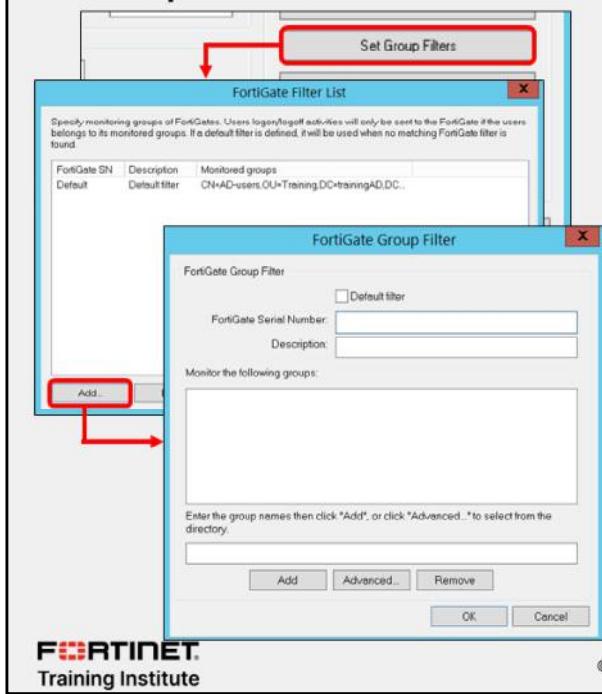
On the FSSO agent configuration GUI, you can configure settings such as:

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

DO NOT REPRINT

© FORTINET

Group Filter



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

© Fortinet Inc. All Rights Reserved.

28

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

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

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

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

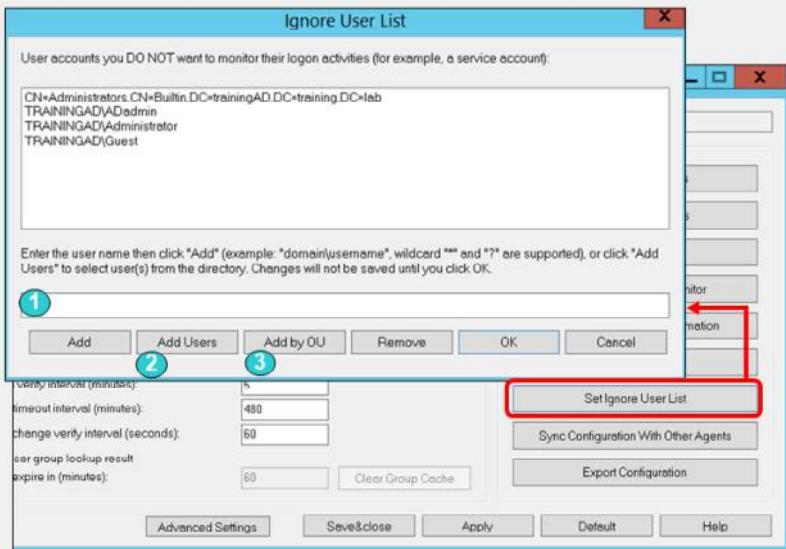
The filter list is initially empty. At a minimum, you should create a default filter that applies to all FortiGate devices without a defined filter.

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

DO NOT REPRINT

© FORTINET

Ignored User List



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

To add users to the ignore list:

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

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

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

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

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

DO NOT REPRINT**© FORTINET**

Collector Agent Timers

Workstation verify interval

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

Timers

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

IP address change verify interval

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

Dead entry timeout interval

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

• Under the workstation verify interval

Cache user group lookup result

- Collector agent remembers user group membership

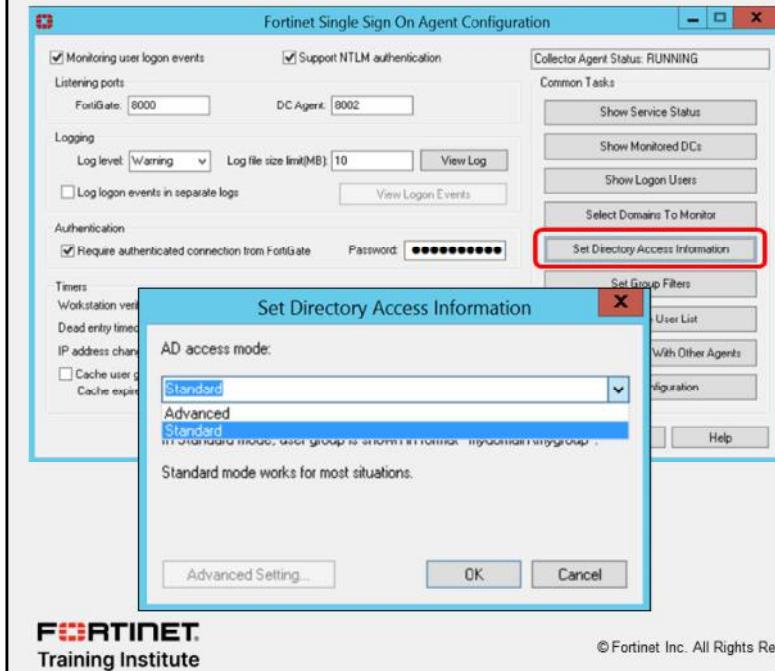
The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

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

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

DO NOT REPRINT
© FORTINET

AD Access Mode Configuration



Standard Access Mode

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

Advanced Access Mode

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

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

31

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

The main difference between modes is the naming convention used:

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

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

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

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

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

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

DO NOT REPRINT**© FORTINET**

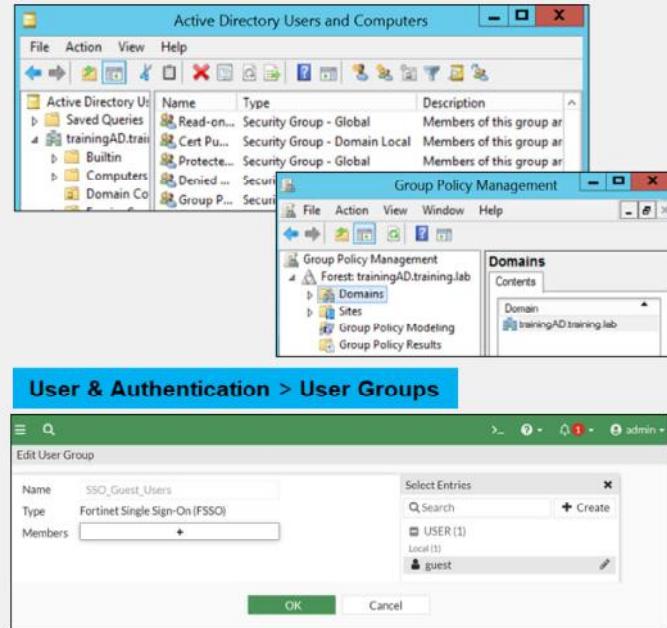
AD Group Support

Group type supported:

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

If the user is not part of an FSSO group:

- For passive FSSO authentication:
 - User is part of **SSO_Guest_Users**
- For passive and active FSSO authentication:
 - User is prompted to log in



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

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

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

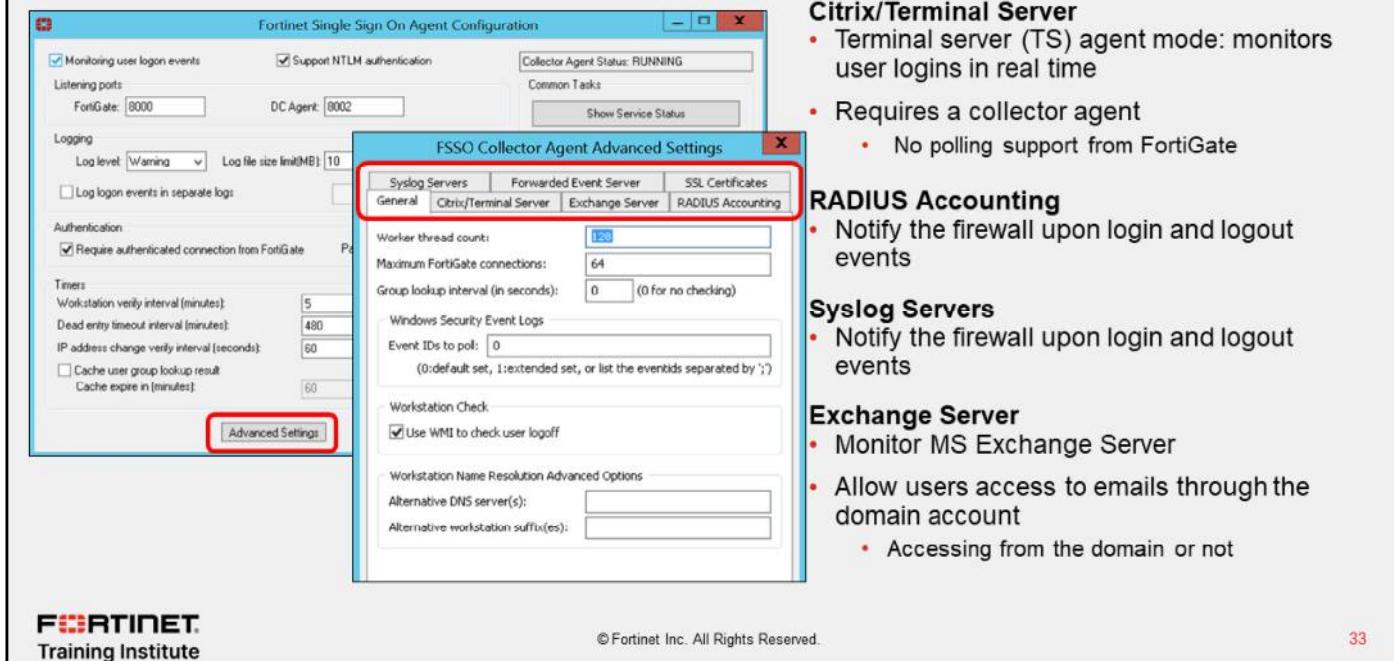
This allows an administrator to configure limited network access to guest users that do not belong to the Windows AD domain.

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

DO NOT REPRINT

© FORTINET

Advanced Settings



The screenshot shows the Fortinet Single Sign-On Agent Configuration interface. A modal dialog box titled 'FSSO Collector Agent Advanced Settings' is open, with the 'Citrix/Terminal Server' tab selected. The 'Advanced Settings' button in the main window is highlighted with a red box. The configuration window includes sections for Monitoring user login events, Support NTLM authentication, and various logging and authentication parameters. The 'FSSO Collector Agent Advanced Settings' dialog contains tabs for Syslog Servers, Forwarded Event Server, SSL Certificates, General, Citrix/Terminal Server (selected), Exchange Server, and RADIUS Accounting. It also includes sections for Worker thread count, Maximum FortiGate connections, Group lookup interval, Windows Security Event Logs, and Workstation Check.

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

FOURINET Training Institute

© 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, a table lists log messages. One message for 'ADUSER1 FSSO-logon' is highlighted. Below this, a 'Details' box shows an 'Event' message and an 'Other' section. The 'Other' section includes fields: Destination (TrainingDomain), Log ID (43014), Sub Type (user), and roll (65533). A red arrow points from the 'Log ID' field in the 'Other' section to the '43014' entry in a list of log entries on the right. The list includes:

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

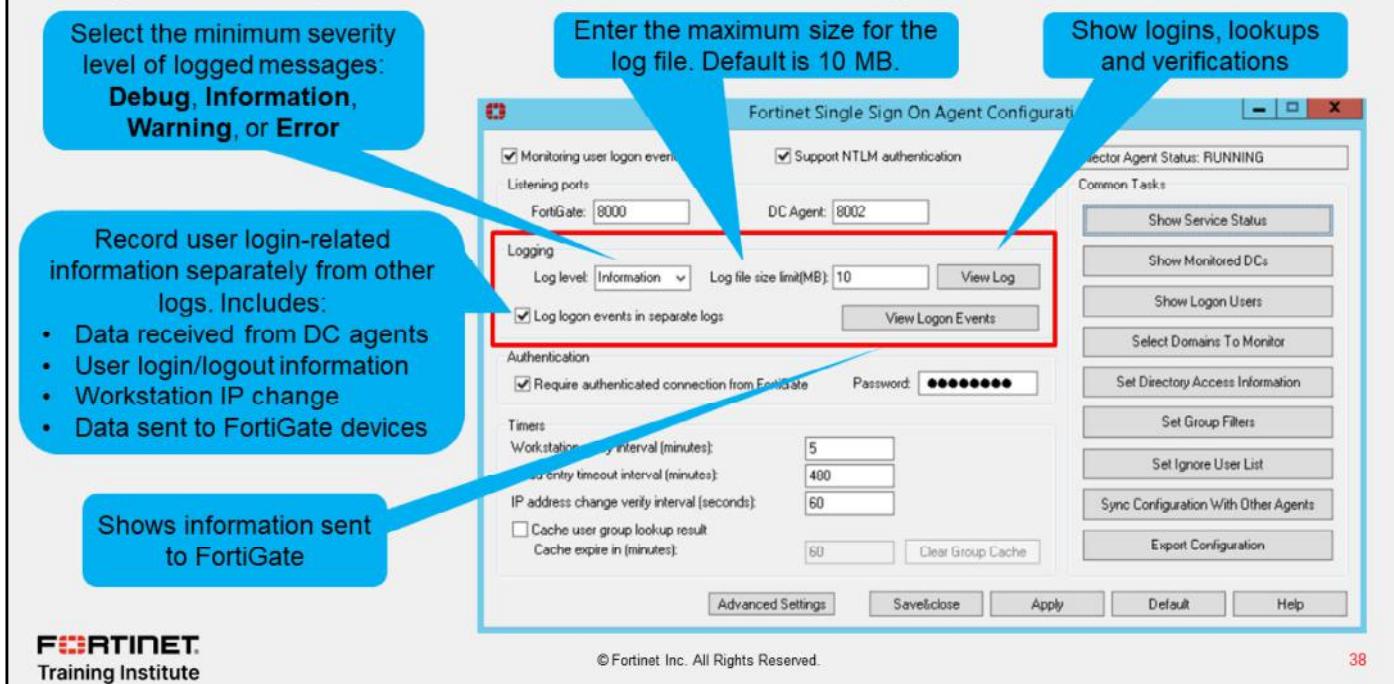
© Fortinet Inc. All Rights Reserved. 37

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

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

DO NOT REPRINT
© FORTINET

Log Messages on FSSO Collector Agent



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

38

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

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

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

DO NOT REPRINT

© FORTINET

Troubleshooting Tips for FSSO

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



© Fortinet Inc. All Rights Reserved.

39

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

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

DO NOT REPRINT
© FORTINET

Currently Logged-On Users

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

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

IP address: 10.0.1.10

Workstation name: WIN-INTERNAL

User name: ADUSER1

User group: TRAININGAD/AD-USERS

Group created on FortiGate: Training

Dashboard > Users & Devices > Firewall Users

User Name	IP Address	User Group	Duration	Traffic Volume	Method
ADUSER1	10.0.1.10	Training	1 minute(1s)	217.40	Fortinet Single Sign-On
		TRAININGAD/AD-USERS			

© Fortinet Inc. All Rights Reserved.

execute fssso refresh

User Group: Training
 Members: TRAININGAD/AD-USERS
 Group Type: Fortinet Single Sign-On (FSSO)

FORTINET
 Training Institute

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

FORTINET
Training Institute



FortiGate Infrastructure

ZTNA

FortiOS 7.2

Last Modified: 23 August 2022

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

DO NOT REPRINT

© FORTINET

Lesson Overview

ZTNA Introduction

Comparing ZTNA to SSL and IPSec VPN

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

ZTNA

Objectives

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

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

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

DO NOT REPRINT**© FORTINET**

What is ZTNA?

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



© 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.

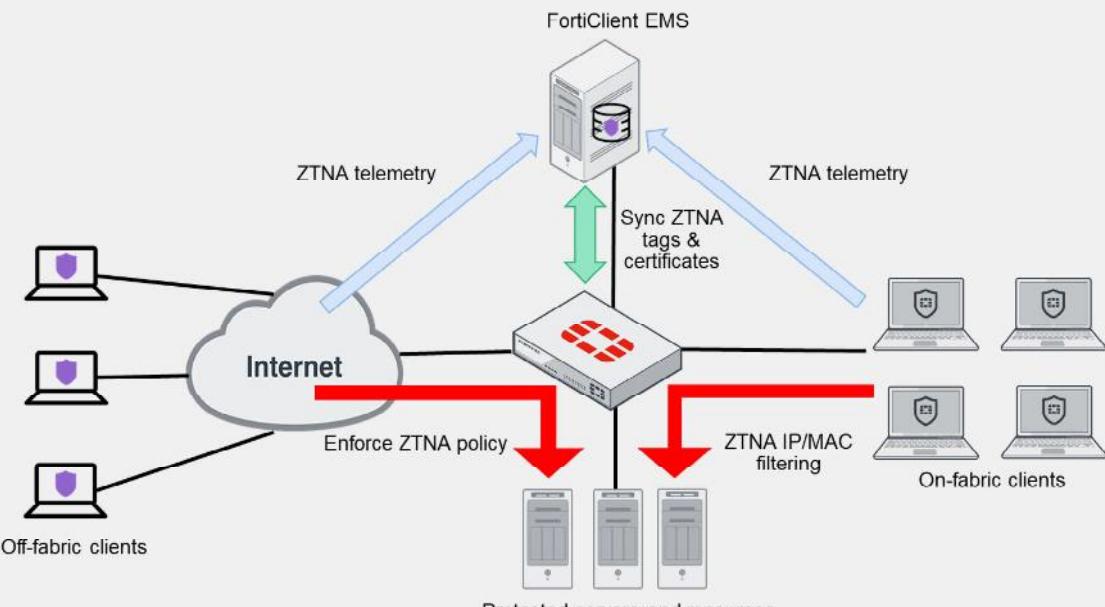
Traditionally, a user and a device have different sets of rules for on-fabric access and off-fabric VPN access to company resources. With a distributed workforce, and access that spans company networks, data centers, and the cloud, managing the rules can be complex. User experience is also affected when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

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

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

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

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

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

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

DO NOT REPRINT**© FORTINET**

FortiClient

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



© Fortinet Inc. All Rights Reserved.

7

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

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

DO NOT REPRINT**© FORTINET**

FortiClient (Contd)

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



© Fortinet Inc. All Rights Reserved.

8

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

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

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

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

DO NOT REPRINT**© FORTINET**

FortiClient EMS

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



© Fortinet Inc. All Rights Reserved.

9

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

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

The benefits of deploying FortiClient EMS include:

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

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

DO NOT REPRINT
© FORTINET

FortiGate and FortiClient EMS Connectivity

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

The screenshot displays the FortiGate GUI and FortiClient EMS interface. On the left, the 'Security Fabric > Fabric Connectors' screen shows the configuration of a 'FortiClient EMS' connector. A blue callout labeled 'FortiGate GUI' points to this screen. On the right, the 'Administration > Fabric Devices' screen shows a 'Fabric Device Authorization Request' for a 'FortiGate' device. A blue callout labeled 'Fabric connector status' points to this screen. The FortiClient EMS GUI is also shown in a separate window at the top right.

Security Fabric > Fabric Connectors

Administration > Fabric Devices

FortiClient EMS GUI

Fabric connector status

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved.

10

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

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

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

DO NOT REPRINT

© FORTINET

Zero-Trust Tagging Rules

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

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

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

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

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

DO NOT REPRINT
© FORTINET

FortiClient EMS Certificate Management

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

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 the certificate name as 'default_ZTNARootCA.pem' and its creation date as '2018-07-16'. A note below states 'Certificate was created on 2017-07-21 12:09:07 UTC'.

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

12

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

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

**DO NOT REPRINT
© FORTINET**

FortiClient EMS Certificate Management (Contd)

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

- diagnose endpoint record list <optional IP address>

三

```
MQ-FortiGate # diagnose endpoint record list  
Record #1:
```

IP Address = 10.0.1.100
MAC Address = 00:50:56:a1:1b:15

MAC list = 00:50:56:a1:19:7a,00:50:56:a1:1b:15;
VDOM = root (0)
MAC denied sessions: 8C00000000010195

```
        Queueing discipline: pfifo_fast
        Online status: online
        Registration status: registered
        On-net status: on-net
        Gateway Interface: port3
        Fcificlient version: 7.0.0
        AVDB version: 89.336
        Fcificlient app signature version: 10.143
        Fcificlient app signature engine running version: 2.31
        Fcificlient HID: 3704E49F1144707863A3D0717F46B36
        Host Name: AD-Server
        OS Type: WIN64
        OS Version: Microsoft Windows Server 2012 R2 Standard Edition
4-bit (build 9600)
        Host Description:
        Hostname: training00.training.lab
        Last Login User: Administrator
        Owner:
        Host Model: VMware Virtual Platform
        Host Manufacturer: VMware, Inc.
```

The screenshot shows the 'Certificate Information' tab of a certificate properties dialog. It includes sections for certificate details, purpose, and issuer information, along with a note about a private key and a 'View Certificate' button.

The screenshot shows the 'Certification Path' tab selected in the 'Certificate' window. The path consists of two certificates: 'FCD160000101075' and '37259E494139070056A4C0311968836'. A red box highlights the second certificate in the list. At the bottom right, there is a 'View Certificate' button.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

13

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

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

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

DO NOT REPRINT**© FORTINET**

SSL Certificate-Based Authentication

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

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

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

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

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

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

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

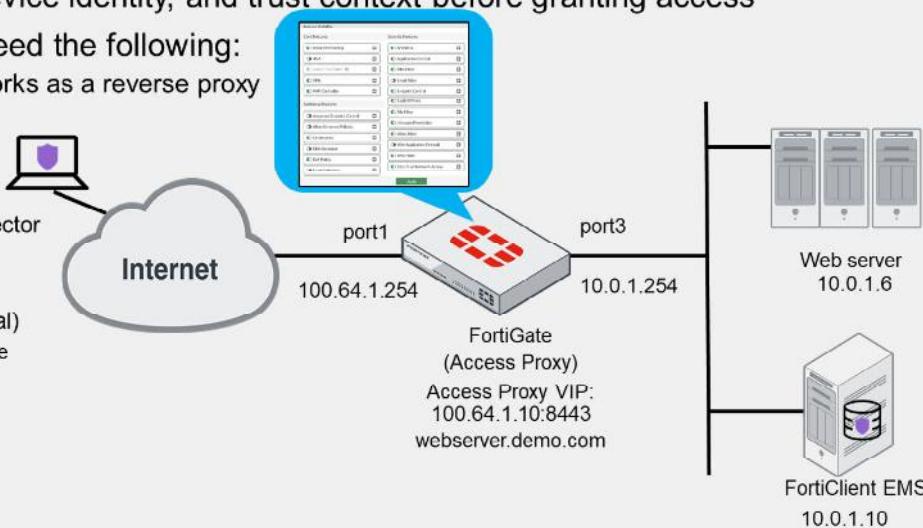
If the client cancels and responds with an empty client certificate, the client is allowed to continue with ZTNA proxy rule processing when you can set `empty-cert-action` to `accept`. If `empty-cert-action` is set to `block`, FortiGate blocks the client from further ZTNA proxy rule processing.

DO NOT REPRINT

© FORTINET

ZTNA HTTPS Access Proxy

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



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

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

ZTNA configuration on FortiGate requires the following configuration:

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

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

DO NOT REPRINT
© FORTINET

ZTNA HTTPS Access Proxy (Contd)

- ZTNA server

Policy & Objects > ZTNA > ZTNA Servers

ZTNA Servers

Virtual host matching rules

Real server IP address and port

- ZTNA rule

Policy & Objects > ZTNA > ZTNA Rules

ZTNA Rules

Denying access based on malicious tag

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

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

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

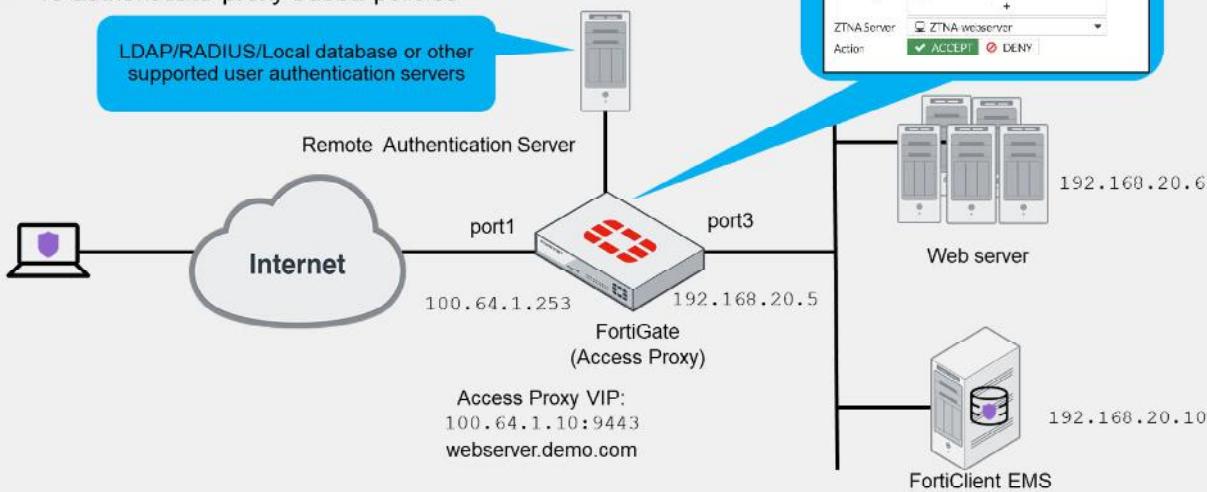
DO NOT REPRINT

© FORTINET

ZTNA HTTPS Access Proxy With Basic Authentication

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

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

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

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

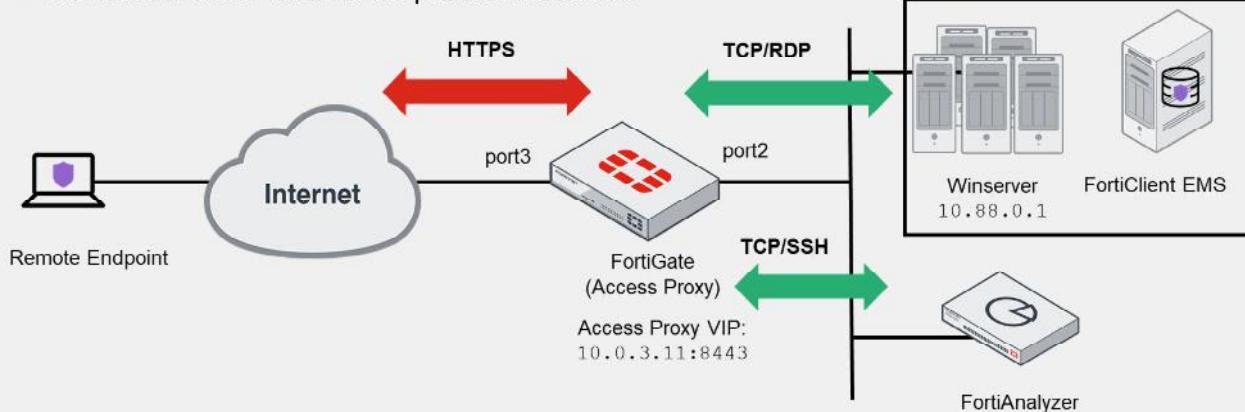
The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they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

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

DO NOT REPRINT
© FORTINET

ZTNA TCP Forwarding Access Proxy

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



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

18

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

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

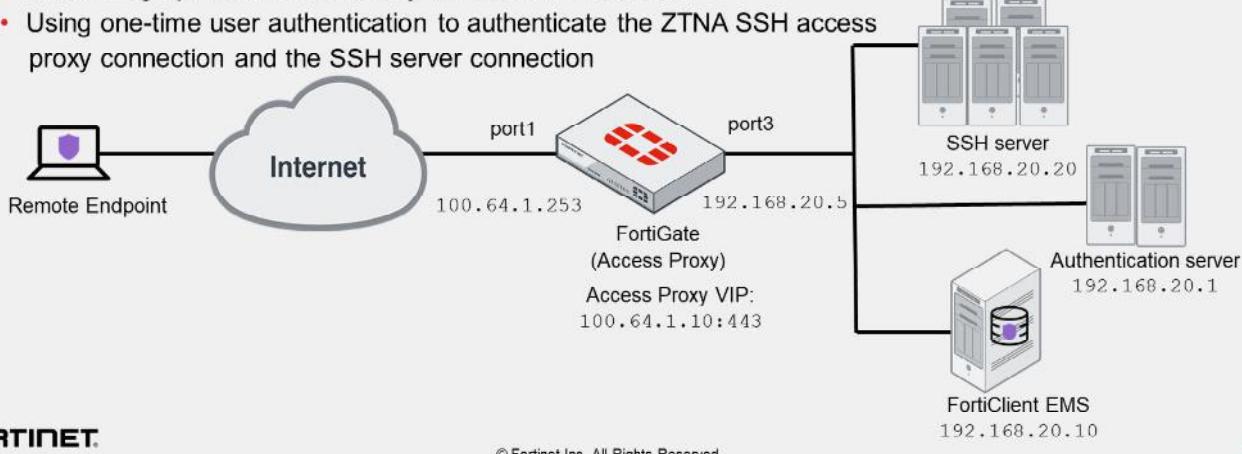
You can also add authentication and a security posture check for TCP Forwarding Access Proxy, which you learned about earlier in this lesson.

DO NOT REPRINT

© FORTINET

ZTNA SSH Access Proxy

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

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

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

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

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

DO NOT REPRINT
© FORTINET

ZTNA IP/MAC-Based Access Control

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

ZTNA IP/MAC-based firewall policy

Name: Block-Malicious

Incoming Interface: port3

Outgoing Interface: port1

Source: all

IP/MAC Based Access Control: FCTEMS_ALL_FORTICLOUD_SEI

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy

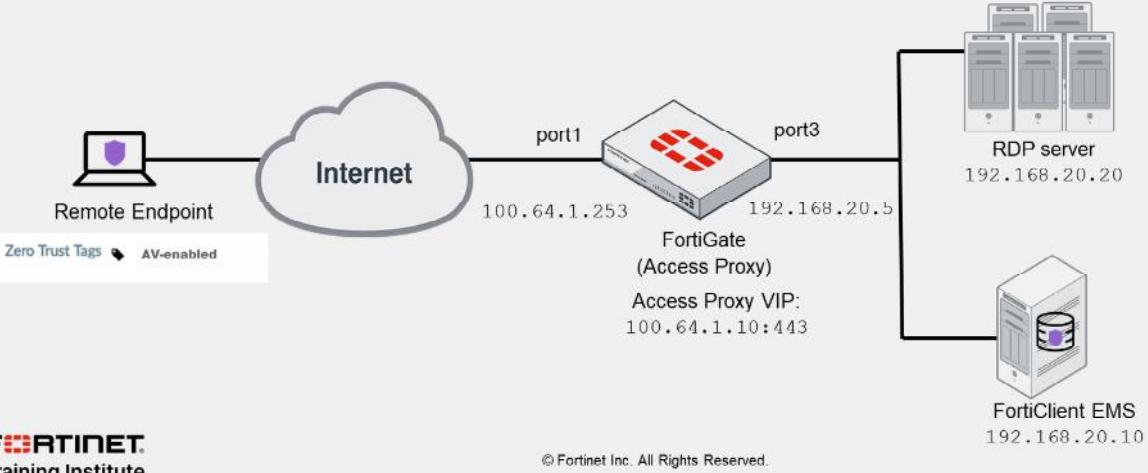
ZTNA IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for fabric users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check, to implement role-based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

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

DO NOT REPRINT
© FORTINET

Posture Check Verification for Active ZTNA Session

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



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

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

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

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which component issues and signs the client certificate?

- A. FortiClient EMS
- B. FortiClient

2. Which internet browser supports Fortinet ZTNA?

- A. Firefox
- B. Chrome

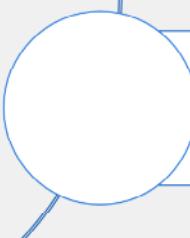
DO NOT REPRINT

© FORTINET

Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPsec VPN

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

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

DO NOT REPRINT

© FORTINET

Comparing ZTNA to SSL and IPsec VPN

Objectives

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

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

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

DO NOT REPRINT

© FORTINET

Comparing SSL VPN, IPsec VPN, and ZTNA Access

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



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

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

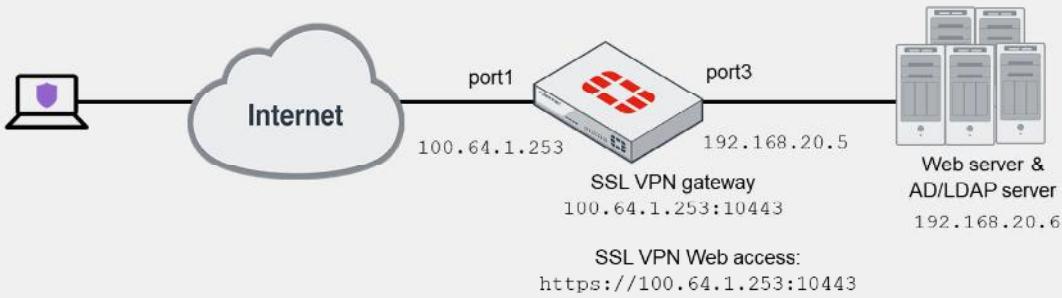
ZTNA follows the zero-trust philosophy to protect the attack surface that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. zero-trust also assumes that every attempt to access the network or an application is a threat.

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

DO NOT REPRINT**© FORTINET**

Moving to ZTNA From SSL VPN

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



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

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

DO NOT REPRINT

© FORTINET

Knowledge Check

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

- A. ZTNA
- B. IPSec

2. What does FortiClient EMS integration ensure?

- A. Device identification
- B. User identification

DO NOT REPRINT

© FORTINET

Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPSec
VPN

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

29

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

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



© Fortinet Inc. All Rights Reserved.

30

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

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

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

SSL VPN

FortiOS 7.2

Last Modified: 13 June 2022

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

DO NOT REPRINT

© FORTINET

Lesson Overview



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

SSL VPN Deployment Modes

Objectives

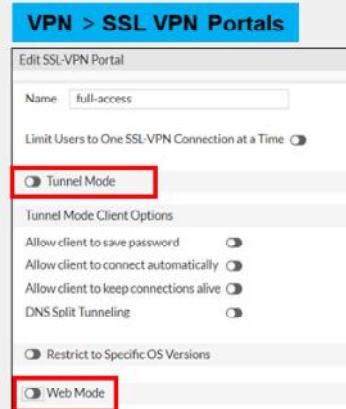
- Describe the differences between SSL VPN modes

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

DO NOT REPRINT**© FORTINET**

SSL VPN Deployment Modes

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



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

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

Which should you choose?

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

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

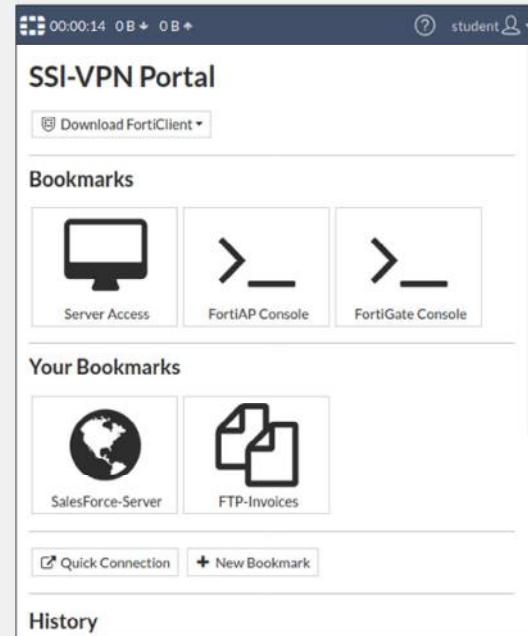
Web mode requires only a web browser, but supports a limited number of protocols.

DO NOT REPRINT

© FORTINET

Web Mode

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



Web mode is the simplest SSL VPN mode.

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

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

Web mode has two main disadvantages:

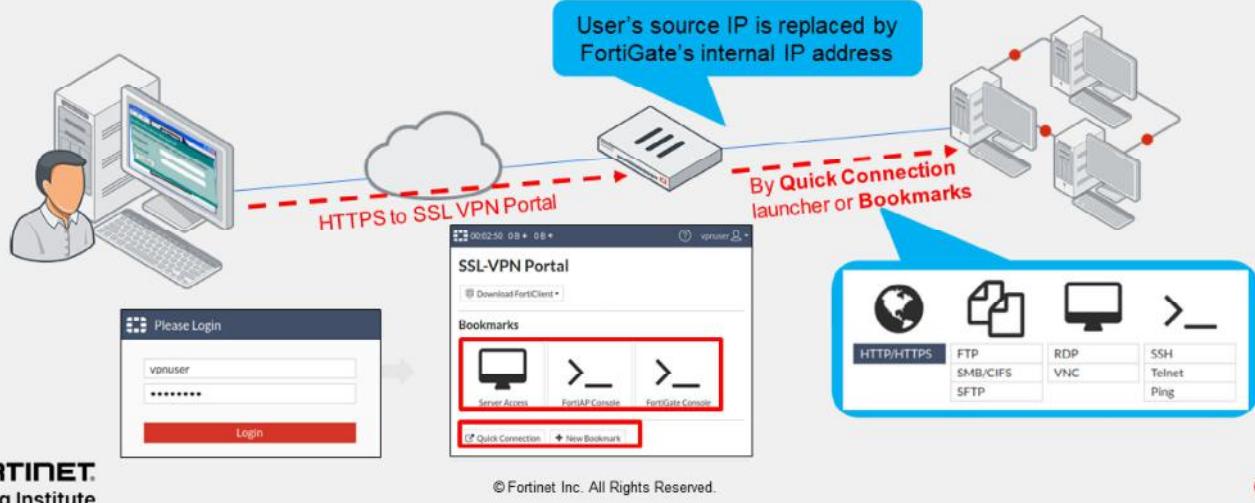
- All interaction with the internal network must be done using the browser exclusively (through the web portal). External network applications running on the user's PC cannot send data across the VPN.
- This a secure HTTP/HTTPS gateway mechanism that doesn't work for accessing everything, but just few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

DO NOT REPRINT

© FORTINET

Web Mode (Contd)

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



FORTINET
Training Institute

6

How does web mode work?

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

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

DO NOT REPRINT**© FORTINET**

Tunnel Mode

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

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



FortiClient

Next Generation Endpoint Protection

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

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

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

DO NOT REPRINT**© FORTINET**

Tunnel Mode (Contd)

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



How does tunnel mode work?

1. Users connect to FortiGate through FortiClient.
2. Users provide credentials to successfully authenticate.
3. FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter (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.

DO NOT REPRINT

© FORTINET

Tunnel Mode—FortiGate as Client (Contd)

1. SSL VPN client FortiGate initiates connection to SSL VPN server FortiGate
2. SSL VPN client FortiGate uses PSK(local user account) and PKI client to authenticate
3. The virtual *SSL VPN tunnel* interface creates the tunnel
 - IP address assigned from SSL VPN server FortiGate
 - Route is added to client to access subnets on remote FortiGate
4. User's devices access resources through an encrypted tunnel (SSL/TLS)



© Fortinet Inc. All Rights Reserved.

10

How does tunnel mode work when FortiGate is configured as client?

1. Client FortiGate connects to server FortiGate using SSL/TLS
2. Client FortiGate provides credentials to successfully authenticate. It includes both PSK (local or remote user account) and PKI (certificate) accounts.
3. Server FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter. This is the client's source IP address for the duration of the connection.
4. Then, users can access services and network resources through the encrypted tunnel behind client FortiGate.

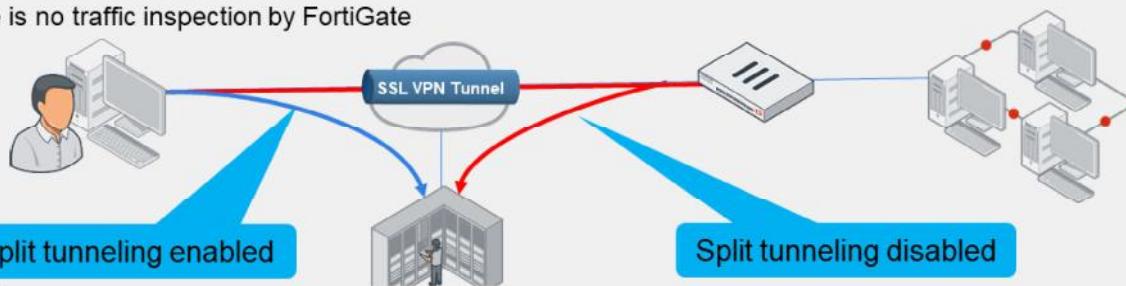
SSL VPN client FortiGate device encrypts all traffic from the remote computer and sends it over the SSL VPN tunnel. SSL VPN server FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

DO NOT REPRINT

© FORTINET

Tunnel Mode—Split Tunneling

- **Disabled:**
 - All traffic routes through an SSL VPN tunnel to a remote FortiGate, then to the destination. This includes internet traffic
 - An egress firewall policy is required
 - Traffic inspection and security features can be applied
- **Enabled:**
 - Only traffic destined for the private network is routed through the remote FortiGate
 - Internet traffic uses the local gateway; unencrypted route
 - Conserves bandwidth and alleviates bottlenecks
 - There is no traffic inspection by FortiGate



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

Tunnel mode also supports split tunneling.

When split tunneling is disabled, all IP traffic generated by the client's computer—including internet traffic—is routed across the SSL VPN tunnel to FortiGate. This sets up FortiGate as the default gateway for the host. You can use this method in order to apply security features to the traffic on those remote clients, or to monitor or restrict internet access. This adds more latency and increases bandwidth usage.

In a FortiGate (client) to FortiGate (server) setup, a default route is effectively dynamically created on the SSL VPN client FortiGate, and the new default route is added to the existing default route in the form of ECMP. The following options are available to configure routing:

- To make all traffic default to the SSL VPN server and still have a route to the server's listening interface, on the SSL VPN client, set a lower distance for the default route that is learned from the server.
- To include both default routes in the routing table, with the route learned from the SSL VPN server taking priority, on the SSL VPN client, set a lower distance for the route learned from the server. If the distance is already zero, then increase the priority on the default route.

When split tunneling is enabled, only traffic that is destined for the private network behind the remote FortiGate is routed through the tunnel. All other traffic is sent through the usual unencrypted route. There is no traffic inspection by FortiGate.

Split tunneling helps to conserve bandwidth and alleviates bottlenecks.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. A web-mode SSL VPN user connects to a remote web server. What is the source IP address of the HTTP request the web server receives?
 - A. The remote user IP address
 - B. The FortiGate device internal IP address
2. Which statement about tunnel-mode SSL VPN is correct?
 - A. It supports split tunneling.
 - B. It requires bookmarks.
3. A web-mode SSL VPN user uses _____ to access internal network resources.
 - A. bookmarks
 - B. FortiClient

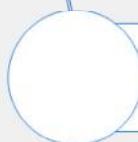
DO NOT REPRINT

© FORTINET

Lesson Progress



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

Good job! You now understand the SSL VPN operation modes supported by FortiGate.

Now, you will learn about how to configure SSL VPNs.

DO NOT REPRINT

© FORTINET

Configuring SSL VPNs

Objectives

- Define authentication for SSL VPN users
- Configure SSL VPN portals
- Configure SSL VPN settings
- Define firewall policies for SSL VPNs
- Configure client integrity check

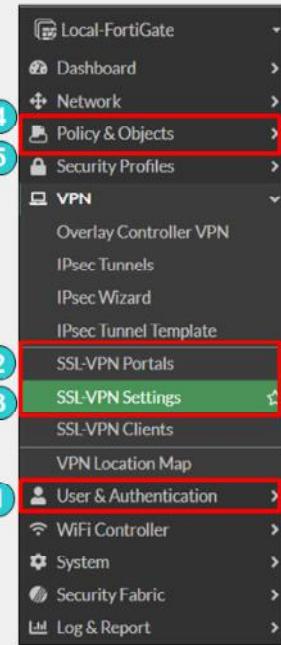
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring the SSL VPN settings on FortiGate, you will be able to better design the architecture of your SSL VPN tunnels.

DO NOT REPRINT**© FORTINET**

Configuring SSL VPN—User as Client

1. Set up user accounts and groups for remote SSL VPN users
2. Configure SSL VPN portals
3. Configure SSL VPN settings
4. Create a firewall policy to and from the SSL VPN interface
 - Accepts and decrypts packets
 - Allows traffic from SSL VPN clients to the internal network and the reverse
5. Optionally:
 - Create a firewall policy to allow SSL VPN traffic to the internet:
 - Useful to allow all clients' traffic through FortiGate to Internet when split tunneling is disabled
 - FortiGate can be used to apply security profiles



To configure SSL VPN, you must take these steps:

1. Configure user accounts and groups.
2. Configure the SSL VPN portal.
3. Configure SSL VPN settings.
4. Create a firewall policy to accept and decrypt packets. This policy is also used to provide access to internal networks.
5. Optionally, configure a firewall policy to allow traffic from the SSL VPN client to the internet and apply security profiles. User traffic will go to the internet through FortiGate, where you can monitor or restrict client access to the internet.

The first step is to create the accounts and user groups for the SSL VPN clients.

All FortiGate authentication methods, with the exception of remote password authentication using the Fortinet Single Sign-On (FSSO) protocol, can be used for SSL VPN authentication. This includes local password authentication and remote password authentication (using the LDAP, RADIUS, and TACACS+ protocols).

Some steps can be configured in a different order than what is shown on this slide.

DO NOT REPRINT

© FORTINET

Configure the SSL VPN Portal

VPN > SSL VPN Portals

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

- SSL VPN portals determine the access profiles
 - Configure portals for different user or groups
- SSL VPN portals can operate in:
 - Tunnel mode
 - Activate split tunneling in the **Enable Split Tunneling** option
 - Assign an IP address to the end user virtual network adapter in **Source IP Pool: fortissl**
 - Web mode
 - Use direct connection or bookmarks to several applications such as: FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, TELNET, VNC

Tunnel Mode

Web Mode

Administrator-defined bookmarks

© Fortinet Inc. All Rights Reserved.

16

The next step is to configure the SSL VPN portal(s). An SSL VPN portal contains tools and resource links for the users to access.

In tunnel mode, when you enable split tunneling, you need to select either **Enabled Based on Policy Destination** or **Enabled for Trusted Destination** setting, which usually specifies networks behind the FortiGate for the SSL VPN users to access. **Enabled Based on Policy Destination** allows client traffic in which destination is matched with the destination configured on the SSL VPN firewall policy where as **Enabled for Trusted Destination** allows client traffic that does not match the explicitly trusted destination.

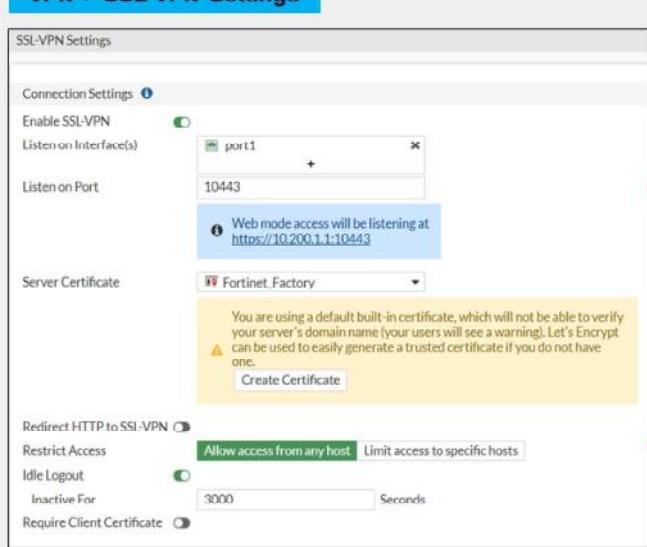
Also, for tunnel mode you need to select an IP pool for users to acquire an IP address when connecting. There is a default pool available within the address objects if you do not create your own.

If you enable web mode, you can customize the SSL VPN portal and preconfigure bookmarks to appear for all users who log in to the SSL VPN portal. Also, you can individually configure and link each portal to a specific user or user group, so they have access to only required resources.

DO NOT REPRINT

© FORTINET

Configure SSL VPN Settings



- FortiGate interface for SSL VPN portal:
 - Default port is 443
 - By default, the admin GUI interface and the SSL VPN portal use same HTTPS port
 - Advised to use different interfaces for admin GUI access and SSL VPN portal
 - If both services use the same interface and port, only the SSL VPN portal appears

- Restrict access to known hosts
- SSL VPN time out:
 - Default idle: 300 sec (5 min)
- Digital server certificate:
 - Self-signed certificate used by default
 - To avoid browser security warnings, use a certificate issued by a public CA, generate a trusted certificate or install the self-signed certificate on all clients

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

After you configure the SSL VPN portal, the next step is to configure the SSL VPN settings.

Let's start with the **Connection Settings** section. Here, you need to map a FortiGate interface to the SSL VPN portal. The default port for the SSL VPN portal is 443. This means users need to connect to the IP address of the FortiGate interface mapped to the SSL VPN portal, using port443 HTTPS. If you enable **Redirect HTTP to SSL VPN**, users who connect using HTTP (TCP port 80) will be redirected to HTTPS.

Port 443 is the standard default port for administration of the HTTPS protocol. This is convenient because users do not need to specify the port in their browsers. For example, <https://www.example.com/> automatically uses port443 in any browser. This is considered a valid setup on FortiGate because you usually don't access the SSL VPN login through every interface. Likewise, you generally don't enable administrative access on every interface of your FortiGate. So, even though the ports may overlap, the interfaces that each one uses to access may not. However, if the SSL VPN login portal and HTTPS admin access both use the same port, and are both enabled on the same interface, only the SSL VPN login portal will appear. To have access to both portals on the same interface, you need to change the port number for one of the services. If you change the administrator access port, this will affect the port number for that service on all interfaces.

Also, an inactive SSL VPN is disconnected after 300 seconds (5 minutes) of inactivity. You can change this timeout using the **Idle Logout** setting on the GUI.

Finally, like other HTTPS websites, the SSL VPN portal presents a digital certificate when users connect. By default, the portal uses a self-signed certificate, which triggers the browser to show a certificate warning. To avoid the warning, you should use a digital certificate signed by a publicly known certificate authority (CA). You can also generate a certificate for interface. Alternatively, you can load the FortiGate self-signed digital certificate into the browser as a trusted authority.

DO NOT REPRINT**© FORTINET**

Configure SSL VPN Settings (Contd)

- Define the IP range for the SSL VPN

- IPs are assigned to clients' virtual adapters while joined to VPN
- IP allocation has two methods:

- First-available (default) or Round robin
- CLI only

```
conf vpn ssl settings
  set tunnel-addr-assigned-method first-available/round-robin
end
```

- Resolve names by DNS server

- Use internal DNS if resolving internal domain names
- Optionally, resolve names by WINS servers

- Specify authentication portal mapping

- Specify portals for each user or group
- Define portal for all other users or groups
 - It cannot be deleted

Users/Groups	Portal
All Other Users/Groups	full access

Define the tunnel-mode client settings and the authentication rules that map users to the appropriate portal.

When users connect, the tunnel is assigned an IP address. You can choose to use the default range or create your own range. The IP range determines how many users can connect simultaneously. There are two IP allocation methods and only available in CLI as shown in the slide:

- First-available (default setting)
- Round robin

Please note when round-robin is used, address pools defined in web portal is ignored, and the `tunnel-ip-pools` or `tunnel-ipv6-pools` under `ssl vpn` setting must be set. Only one set of IP pool address is allowed.

DNS server resolution is effective only when the DNS traffic is sent over the VPN tunnel. Generally, this will be the case only when split tunnel mode is disabled and all traffic is being sent from the user's computer across the tunnel.

Finally, you can allow different groups of users to access different portals. In the example shown on this slide, teachers have access only to the web portal. Accountants can use FortiClient to connect in tunnel mode.

DO NOT REPRINT

© FORTINET

Firewall Policies to and from SSL VPN Interface

- Listens for connections to the SSL VPN portal
- **ssl.<vdom_name>** policy enables portal with user authentication
- The selected **Incoming Interface** is the SSL VPN virtual interface
 - Example: **ssl.root** for root VDOM
- Passes decrypted traffic to the selected **Outgoing Interface**

The fourth, and last, mandatory step involves creating firewall policies for logging on.

SSL VPN traffic on FortiGate uses a virtual interface called `ssl.<vdom_name>`. Each virtual domain (VDOM) contains a different virtual interface based on its name. By default, if VDOMs are not enabled, then the device operates with a single VDOM called `root`.

To activate and successfully log in to the SSL VPN, there must be a firewall policy from the SSL VPN interface to the interface to which you want to allow access for the SSL VPN users, including all of the users and groups that can log in as the source. Without a policy like this, no login portal is presented to users.

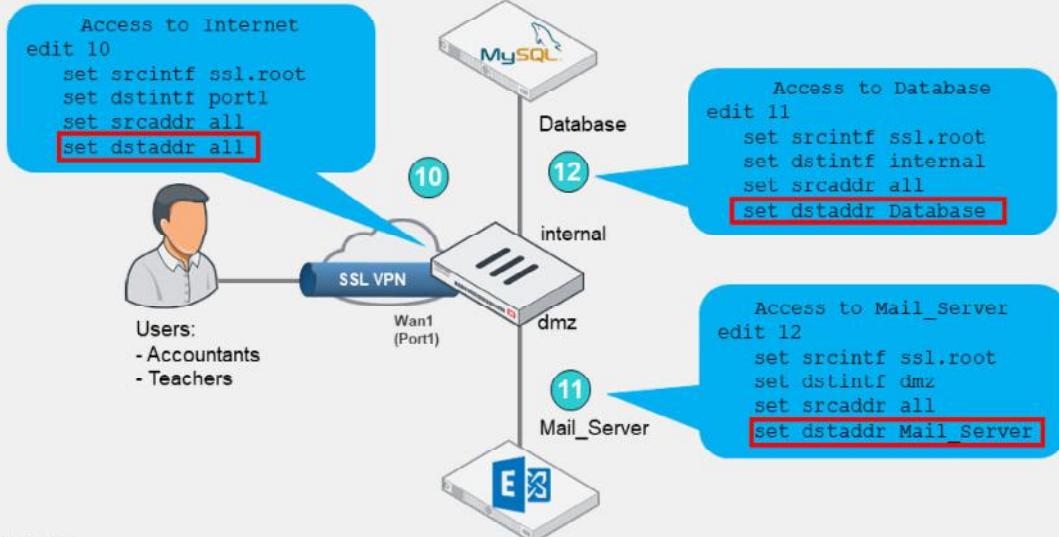
If there are resources behind other interfaces that users need access to, then you need to create additional policies that allow traffic from `ssl.root` to exit those interfaces.

DO NOT REPRINT

© FORTINET

Example: Access to Resources

- All traffic generated by the user exits through the `ssl.<vdom_name>` interface
 - Applies to both web and tunnel mode



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

20

Any traffic from SSL VPN users, whether in web portal or tunnel mode, exits from the `ssl.<vdom_name>` interface.

This slide shows an example of firewall policies that are configured to allow access to resources behind other interfaces that users need access to when connected through SSL VPN.

Optionally, if split tunneling is disabled, you need to create an additional firewall policy from `ssl.root` to the egress interface to allow clients access to the internet.

You can also apply security profiles to this firewall policy to restrict user access to the internet.

DO NOT REPRINT

© FORTINET

Configuring SSL VPN—FortiGate as Server

- SSL VPN Server FortiGate

- Set up user accounts and groups for remote SSL VPN users
 - Create two accounts: local/remote and PKI
 - Require clients to authenticate using their certificates as well as username and password
- Configure SSL VPN portals
- Configure SSL VPN settings
 - Authentication rules include both accounts using CLI
- Create a firewall policy to and from the SSL VPN interface
- Create a firewall policy to allow SSL VPN traffic to the internet (optional)

Use CLI to create first PKI user to get PKI menu on GUI

User & Authentication > User Definition

Edit User	
Username	clientfortigate
User Account Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
User Type	Local User
Password	*****
User Group	<input checked="" type="radio"/> SSL-VPN-Users <input type="radio"/> +
<input type="checkbox"/> Two-factor Authentication	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

User & Authentication > PKI

Edit PKI User	
Name	pki
Subject	
CA	CA.Cert.1
<input type="checkbox"/> Two-factor authentication	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

```
config user peer
  edit pki
    set ca "CA_Cert_1"
    set cn "FGVM01TM905"
  end
```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

21

To configure SSL VPN, you must take these steps:

SSL VPN server FortiGate:

- Set up user accounts and groups for remote SSL VPN users.
 - Create two accounts: local/remote and PKI. The PKI menu is only available in the GUI after a PKI user has been created using the CLI, and a CN can only be configured in the CLI. If no CN is specified, then any certificate that is signed by the CA will be valid and matched.
 - Require clients to authenticate using their certificates as well as username and password.
- Configure SSL VPN portals.
- Configure SSL VPN settings.
 - Authentication rules include both accounts using CLI.
- Create a firewall policy to and from the SSL VPN interface.
- Create a firewall policy to allow SSL VPN traffic to the internet (optional).

DO NOT REPRINT

© FORTINET

Configuring SSL VPN—FortiGate as Client

• SSL VPN Client FortiGate

1. Create PKI user
 - Select CA certificate that allows the FortiGate to complete the certificate chain and verify the server's certificate
2. Create SSL VPN tunnel interface using `ssl.<vdom>` interface
3. Create and configure the SSL VPN Client settings on **VPN > SSL-VPN Clients**
4. Create a firewall policy from internal interface to the SSL VPN interface

The image shows two screenshots of the FortiGate Management Interface. The left screenshot, titled 'Network > Interface > Create New', shows the configuration of a new interface named 'sslclient_port'. It is set as an 'SSL-VPN Tunnel' type, connected to 'port4', and assigned to 'VRF ID 0'. The 'Client Name' is 'sslclient_port'. The right screenshot, titled 'VPN > SSL-VPN Clients > Create New', shows the configuration of a new SSL-VPN client named 'SSLClienttoHQ'. It is connected to 'sslclient_port' and 'VRF ID 0'. The 'Client Name' is 'SSLClienttoHQ'. The 'Virtual SSLInterface' is 'sslclient_port'. The 'Server' is '10.200.1.1' and the 'Port' is '10443'. The 'Username' is 'ClientFortigate'. The 'Peer' is 'pkd'. The 'Administrative Distance' is '10' and the 'Priority' is '0'. The 'Status' is 'Enabled'. The 'Comments' field is empty. A red box highlights the 'Username' field, and blue callout boxes explain the 'Client Name', 'Virtual SSLInterface', 'Server FortiGate IP Address and SSL Port', 'Local and PKI user details including local cert to identify this client', and 'Dynamic route priority and distance settings'.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

22

To configure SSL VPN, you must take these steps:

SSL VPN Client FortiGate:

1. Create PKI user:
 - Set the same CN using CLI if PKI user on server FortiGate has CN configured.
 - Select CA certificate that allows the FortiGate to complete the certificate chain and verify the server's certificate.
2. Create SSL VPN tunnel interface using `ssl.<vdom>` interface.
3. Create and configure the SSL VPN client settings on **VPN > SSL-VPN Clients**, it includes:
 - Client name
 - Virtual SSL VPN interface
 - SSL VPN server FortiGate IP address and SSL port number
 - Local username and password and PKI(Peer) user. The **Client Certificate** is the local certificate that is used to identify this client, and is assumed to already be installed on the FortiGate. The SSL VPN server requires it for authentication.
 - When split tunnel is disabled, new default route is added and priority and distance plays an important role.
4. Create a firewall policy to allow traffic from internal interface to the SSL VPN interface.

DO NOT REPRINT**© FORTINET**

Client Integrity Checking

- SSL-VPN gateway checks client integrity
 - Requires Microsoft Windows
 - Supported in SSL VPN tunnel mode only
- Detects client security applications recognized by the Windows Security Center
 - Antivirus and firewall software
 - Security attributes recorded on the client's computer
- Checks the status of applications through their globally unique identifier (GUID)
 - Custom host checks
- Determines the state of the applications
 - Active/inactive
 - Current version number
 - Signature updates

**FORTINET**
Training Institute

© Fortinet Inc. All Rights Reserved.

23

When a user connects to your network through an SSL-VPN, a portal is established between your network and the user's PC. The VPN session is secured natively in two ways: the connection is encrypted and the user must log in with their credentials, such as a username and password. However, you can configure additional checks to increase the security of the connection.

One method of increasing your security is by using client integrity checking. Client integrity ensures that the connecting computer is secure by checking whether specific security software, such as antivirus or firewall software, is installed and running. This feature supports only Microsoft Windows clients, because it accesses the Windows Security Center to perform its checks. Alternatively, you can customize this feature to check the status of other applications using their GUIDs. A GUID is a unique ID in the Windows Configuration Registry that identifies each Windows application. Client integrity can also check the current software and signature versions for the antivirus and firewall applications.

Client integrity checking is applicable to tunnel mode only.

DO NOT REPRINT

© FORTINET

Configure the Client Integrity Check

- Uses external vendor software to ensure client integrity:
FortiClient, AVG, CA, F-Secure, Kaspersky, McAfee, Norton, Symantec, Panda, Sophos, Trend-Micro, Zone Alarm,...
- Checks whether the software is installed on host client:
 - Configure through CLI or GUI
 - Software must be updated and recognized by Windows Security Center
 - None – No host checking
 - av – Verify if there is any antivirus software
 - fw – Verify if there is any firewall software
 - av-fw – Verify if there is both antivirus and firewall software
 - Custom – Verify custom or proprietary software
 - If the software is not installed, FortiGate rejects SSL-VPN connection attempt

```
config vpn ssl web host-check-software
show
```

VPN > SSL-VPN Portals > portal-name

<input checked="" type="radio"/> Host Check	Realtime AntiVirus	Firewall	Enable both
Restrict to specific OS versions <input type="checkbox"/>			

```
config vpn ssl web portal
edit <portal_name>
  set host-check [none|av|fw|av-fw|custom]
  set host-check-interval <seconds>
end
```

Administrators should have in-depth knowledge of the Windows OS to use and maintain this feature

FortiGate performs the client integrity check while the VPN is still establishing, just after user authentication has finished. If the required software is not running on the user's PC, FortiGate rejects the VPN connection attempt, even with valid user credentials. You enable client integrity for each web portal, and you configure it using CLI commands or the FortiGate GUI.

The list of recognized software, along with the associated registry key value, is available on the CLI only. Software is split into three categories: antivirus (av), firewall (fw), and custom. Custom is used for customized or proprietary software that an organization may require. Administrators can configure av, fw, or both settings on the GUI or CLI, but the custom setting is available only on the CLI.

Administrators can also configure OS versions and patch settings to allow or deny VPN connections from specific OS versions.

The disadvantage of enabling client integrity checking is that it can result in a lot of administrative overhead because of the following factors:

- All users must have their security software up to date in order to successfully establish a connection.
- Software updates can result in a change to the registry key values, which can also prevent a user from successfully connecting.

As such, administrators must have in-depth knowledge of the Windows operating system and subsequent registry behavior in order to properly make extended use of and maintain this feature.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which step is necessary to configure SSL VPN connections?
 A. Create a firewall policy from the SSL VPN interface to the resource's interface.
 B. Enable event logs for SSL VPN traffic: users, VPN, and endpoints.

2. Which action may allow internet access in tunnel mode, if the remote network does not allow internet access to SSL VPN users?
 A. Enable split tunneling
 B. Configure the DNS server to use the same DNS server as the client system DNS

DO NOT REPRINT

© FORTINET

Lesson Progress



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

Good job! You now understand how to configure FortiGate for SSL VPN connections.

Now, you'll learn how to monitor SSL VPN sessions, review logs, configure SSL VPN timers, and troubleshoot common issues.

DO NOT REPRINT

© FORTINET

Monitoring and Troubleshooting

Objectives

- Monitor SSL VPN-connected users
- Review SSL VPN logs
- Configure SSL VPN timers
- Troubleshoot common SSL VPN issues
- Identify hardware acceleration components for SSL VPN

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

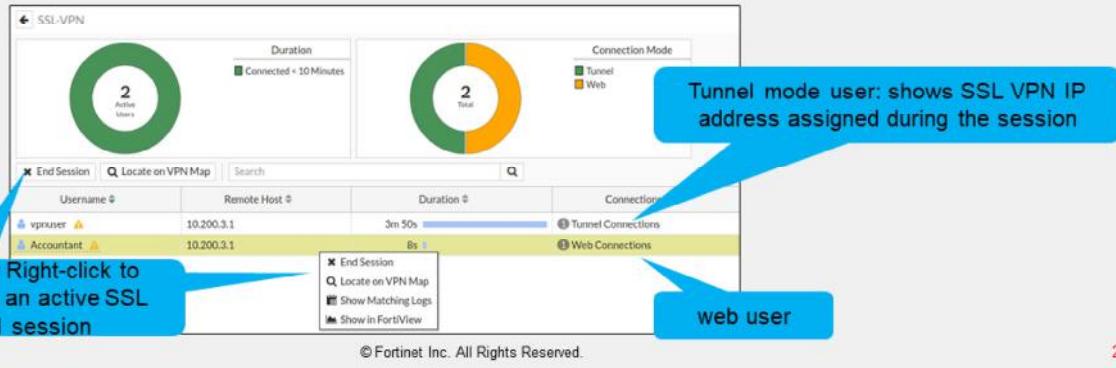
By demonstrating competence in SSL VPN monitoring and troubleshooting, you will be able to avoid, identify, and solve common issues and misconfigurations.

DO NOT REPRINT
© FORTINET

Monitoring SSL VPN Sessions

- Monitor which SSL VPN users are connected
 - GUI: Dashboard > Network > SSL VPN
- Shows SSL VPN user names, connection times, and IP addresses
 - For tunnel mode, **Active Connections** displays IP address assigned to `fortissl` virtual adapter
- Force end user disconnection
 - Right-click the user name and select **End Session**

Dashboard > Network > SSL VPN



FOR
NET
 Training Institute

28

You can monitor which SSL VPN users are connected on the **SSL VPN** widget. This shows the names of all SSL VPN users that are currently connected to FortiGate, their IP addresses (both inside the tunnel and outside), and connection times.

When a user connects using tunnel model, the **Active Connections** column shows the IP address assigned by FortiGate to the `fortissl` virtual adapter on the client's computer. Otherwise, the user is connected only to the web portal page.

DO NOT REPRINT

© FORTINET

SSL VPN Logs

The screenshot shows the FortiGate Log & Report interface. The left sidebar has a 'Log & Report' dropdown and a list of traffic types. The 'System Events' item is highlighted with a red box and has a red arrow pointing to it from the main content area. The main content area shows two widgets: 'VPN Events' and 'User Events'. Each widget has a blue callout box with a table of log entries. The 'VPN Events' table shows SSL tunnel status changes, and the 'User Events' table shows authentication actions for a user named 'Student'.

Date/Time	Level	Action	Status	Message
2020/01/21 04:50:...	ssl-new-con	ssl-new-con	SSL tunnel established	SSL new connection
2020/01/21 04:50:...	tunnel-down	tunnel-down	SSL tunnel shutdown	SSL tunnel statistics
2020/01/21 04:49:...	tunnel-stats	tunnel-stats	SSL tunnel statistics	SSL tunnel established
2020/01/21 04:39:...	tunnel-up	tunnel-up	SSL tunnel established	SSL new connection
2020/01/21 04:39:...	ssl-new-con	ssl-new-con	SSL tunnel established	SSL new connection

Date/Time	Level	User	Action	Message
2020/01/21 04:50:33	info	Student	auth-logout	User Student removed from auth logon
2020/01/21 04:39:02	info	Student	auth-logon	User Student added to auth logon

- Review if the SSL VPN tunnel is established or closed
- Review the authentication action related to SSL VPN users
- Review SSL VPN connections in tunnel mode with FortiClient

You can also review SSL VPN logs. On **Log & Report > System Events**:

- Select **VPN Events** widget to show new connection requests, and if the SSL VPN tunnel is established or closed.
- Select **User Events** widget to see the authentication action related to SSL VPN users.

DO NOT REPRINT

© FORTINET

SSL VPN Idle Timeout vs. Authentication Session

- Firewall policy authentication session is associated with SSL VPN tunnel session
 - Firewall policy authentication session is forced to end when SSL VPN tunnel session ends
 - Prevents reuse of authenticated SSL VPN firewall sessions (not yet expired) by a different user, after the initial user terminates the SSL VPN tunnel session
- SSL VPN authentication is not subject to the firewall authentication timeout setting
 - It has a separate idle setting: default 300 seconds

The screenshot shows the 'VPN > SSL VPN Settings' configuration page. It includes sections for 'Redirect HTTP to SSL-VPN', 'Restrict Access' (with 'Allow access from any host' selected), 'Idle Logout' (selected), and 'Inactive For' (set to 300 seconds). A blue arrow points from the 'Idle Logout' section to a command line interface (CLI) command on the right. The CLI command is:

```
config vpn ssl settings
  set idle-timeout <0-259200>
end
```

When an SSL VPN is disconnected, either by the user or through the SSL VPN idle setting, all associated sessions in the FortiGate session table are deleted. This prevents the reuse of authenticated SSL VPN sessions (not yet expired) after the initial user terminates the tunnel.

The SSL VPN user idle setting is not associated with the firewall authentication timeout setting. It is a separate idle option specifically for SSL VPN users. A remote user is considered idle when FortiGate does not see any packets or activity from the user within the configured timeout period.

DO NOT REPRINT**© FORTINET**

SSL VPN Timers

- Set up timers to avoid logouts when SSL VPN users are connected over high latency connections

- DTLS hello timeout—default 10 seconds
- Login timeout—default 30 seconds

```
config vpn ssl settings
    set login-timeout <10-180>
    set dtls-hello-timeout <10-60>
    set http-request-header-timeout <1-60>
    set http-request-body-timeout <1-60>
end
```

- Timers can also help to mitigate DoS attacks within SSL VPN caused by partial HTTP requests, such as Slowloris and R-U-Dead-Yet

When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under `config vpn ssl settings` have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections.

Also, timers can help you to mitigate vulnerabilities such as Slowloris and R-U-Dead-Yet, that allow remote attackers to cause a denial of service through partial HTTP requests.

DO NOT REPRINT**© FORTINET**

Best Practices for Common SSL VPN Issues

- For web mode connections, make sure that:
 - Cookies are enabled and the internet privacy options are set to high in your web browser
 - SSL VPN clients are following the proper URL structure: <https://<FortiGateIP>:<port>>
- For tunnel mode connections, make sure that:
 - The FortiClient version is compatible with the FortiOS firmware
 - Refer to release notes for product compatibility and integration
 - Split tunneling is enabled to allow internet access without backhauling all user's data to the remote network, or
 - Split tunneling is disabled and an egress firewall policy is created for SSL VPN connections
- For general SSL VPN connections, make sure that:
 - Users are connecting to the correct port number
 - To check SSL VPN port assignment, click **VPN > SSL VPN Settings**
 - Firewall policies include SSL VPN groups or users, and the destination address
 - The timeout timer is configured to flush inactive sessions after a short time
 - Users are encouraged to log out if they are not using the network resources only accessible by SSL VPN



© Fortinet Inc. All Rights Reserved.

32

The following are some best practices to keep in mind when using SSL VPNs. These best practices can also be helpful in many SSL VPN troubleshooting situations:

- Enable cookies in your web browser
- Set internet privacy options to high in your web browser
- Use a FortiClient version that is compatible with your FortiOS firmware
- Enable split tunneling or create an egress firewall policy for SSL VPN connections in order to allow access for external resources
- Connect to the correct port number
- Add SSL VPN groups, SSL VPN users, and destination addresses to the firewall policies
- Flush inactive sessions by timeout

DO NOT REPRINT**© FORTINET**

Useful Troubleshooting Commands

```
# diagnose debug enable
# diagnose vpn ssl <...>
  list      → Show current connections
  info      → General SSL VPN information
  statistics → Show statistics about memory usage on FortiGate, maximum and
                current connections
  debug-filter → Debug message filter for SSL VPN
  hw-acceleration-status → Display the status of SSL hardware acceleration
  tunnel-test → Enable/disable SSL VPN old tunnel mode IP allocation method
  web-mode-test → Enable/disable random session ID in proxy URL for testing
```

```
# diagnose debug application sslvpn -1
# diagnose debug enable
```

Display debug messages for SSL VPN; -1 debug level
produces detailed results

- Check debug logs on the FortiClient



© Fortinet Inc. All Rights Reserved.

33

There are several useful troubleshooting commands available under `diagnose vpn ssl`. They include:

- `list`: Lists logged-on users
- `info`: Shows general SSL VPN information
- `statistics`: Shows statistics about memory usage on FortiGate
- `hw-acceleration-status`: Displays the status of SSL hardware acceleration
- `tunnel-test`: Enables or disables SSL VPN old tunnel mode IP allocation method
- `web-mode-test`: Enables or disables random session ID in proxy URL for testing

The command `diagnose debug application sslvpn` shows the entire list of debug messages for SSL VPN connections.

Remember, to use the commands listed above, you must first run the `diagnose debug enable` command. Also, check SSL VPN debug logs on FortiClient.

DO NOT REPRINT**© FORTINET**

Hardware Acceleration for SSL VPN

- FortiGate devices with content processors (CP8 or CP9), which offload specific CPU-intensive operations, support high-performance SSL VPN bulk data engines
 - SSL/TLS protocol processor
- Administrators can disable CP offloading through firewall policies
 - For example: test purposes

```
config firewall policy
  edit 1
    set auto-asic-offload [enable | disable]
  end
```

- To view the status of SSL VPN acceleration, use the following command:

```
get vpn status ssl hw-acceleration-status
```

```
Acceleration hardware detected: kxp-on      No acceleration hardware detected
cipher=on
```

FortiGate devices that have CP8 or CP9 content processors, which accelerate many common resource-intensive, security-related processes, can offload SSL VPN traffic to a high-performance VPN bulk data engine.

This specialized IPsec and SSL/TLS protocol processor processes most of the latest well-known algorithms for encryption.

By default, the offloading process is set up. If, for testing purposes you want to disable it, you can do it using the CLI only at the firewall policy configuration level.

You can also view the status of SSL VPN acceleration using the CLI.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What does the SSL VPN monitor feature allow you to do?
 A. Monitor SSL VPN user actions, such as authentication
 B. Force SSL VPN user disconnections

2. Which statement about SSL VPN timers is correct?
 A. SSL VPN timers can prevent logouts when SSL VPN users experience long network latency.
 B. The login timeout is a non-customizable hard value.

DO NOT REPRINT

© FORTINET

Lesson Progress



SSL VPN Deployment Modes



Configuring SSL VPNs



Monitoring and Troubleshooting

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

36

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe the differences between SSL VPN modes
- ✓ Define authentication for SSL VPN users
- ✓ Configure SSL VPN portals
- ✓ Configure SSL VPN settings
- ✓ Define firewall policies for SSL VPN
- ✓ Configure the client integrity check
- ✓ Monitor SSL VPN connected users
- ✓ Review SSL VPN logs
- ✓ Configure SSL VPN timers
- ✓ Troubleshoot common SSL VPN issues



© Fortinet Inc. All Rights Reserved.

37

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

By mastering the objectives covered in this lesson, you learned how to configure and use SSL VPNs to give remote users access to your private network.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

IPsec VPN

FortiOS 7.2

Last Modified: 23 August 2022

In this lesson, you will learn about the architectural components of IPsec VPN and how to configure them.

DO NOT REPRINT

© FORTINET

Lesson Overview



IPsec Introduction



IPsec Configuration



Routing and Firewall Policies



Redundant VPNs



Monitoring and Logs

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

IPsec Introduction

Objectives

- Describe the benefits of IPsec VPN
- Be familiar with the IPsec protocol
- Understand how IPsec works
- Select an appropriate VPN topology

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

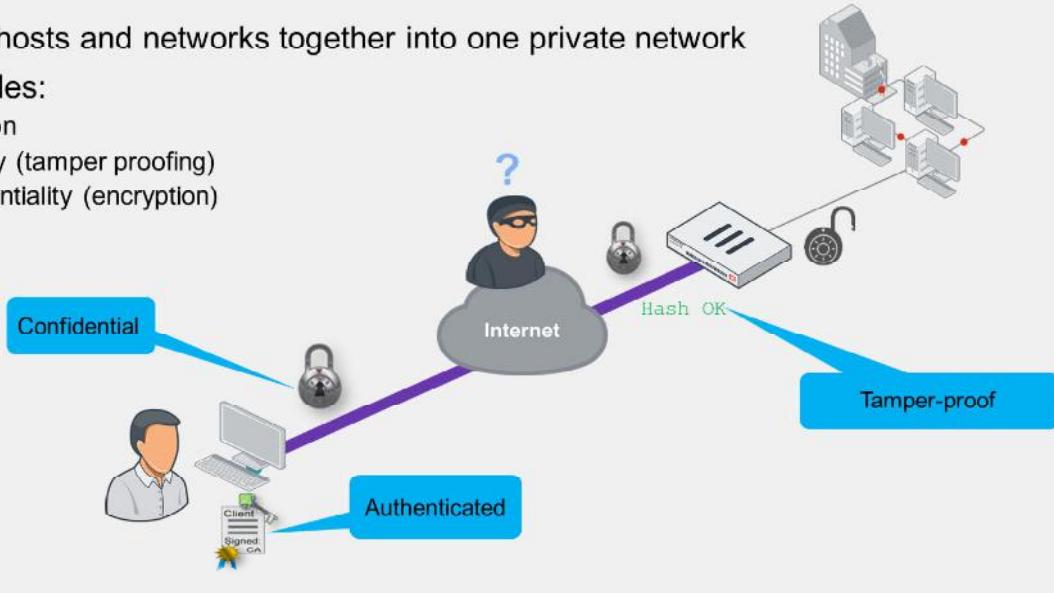
By demonstrating competence in IPsec basics, you will be able to understand IPsec concepts and benefits.

DO NOT REPRINT

© FORTINET

What Is IPsec?

- Joins remote hosts and networks together into one private network
- Usually provides:
 - Authentication
 - Data integrity (tamper proofing)
 - Data confidentiality (encryption)



What is IPsec? When should you use it?

IPsec is a vendor-neutral set of standard protocols that is used to join two physically distinct LANs. The LANs are joined as if they were a single logical network, despite being separated by the internet.

In theory, IPsec *does* support null encryption—that is, you can make VPNs that don't encrypt traffic. IPsec also supports null data integrity. But does that provide any advantages over plain traffic? No. No one can trust traffic that may have had an attack injected by an attacker. Rarely do people want data sent by an unknown source. Most people also want private network data, such as credit card transactions and medical records, to remain private.

Regardless of the vendor, IPsec VPNs almost always have settings that allow them to provide three important benefits:

- Authentication: to verify the identity of both ends
- Data integrity (or HMAC): to prove that encapsulated data has not been tampered with as it crosses a potentially hostile network
- Confidentiality (or encryption): to make sure that only the intended recipient can read the message

DO NOT REPRINT

© FORTINET

What Is the IPsec Protocol?

- Multiple protocols that work together
 - Authentication Header (AH) provides integrity but not encryption
 - AH is defined in the RFC, but FortiGate does not use it
- Port numbers and encapsulation vary by network address translation (NAT)

Protocol	NAT Traversal (NAT-T)	No NAT
IKE RFC 2409 (IKEv1) RFC 4306 (IKEv2)	IP protocol 17: UDP port 500 (UDP 4500 for rekey, quick mode, mode-cfg)	IP protocol 17: UDP port 500
ESP RFC 4303	IP protocol 17: UDP port 4500 (encapsulated)	IP protocol 50

- If required, set a custom port for both IKE and IKE NAT-T (initiator and responder)*:

```
config system settings
  set ike-port <port>
end
```

* Custom port range: 1024–65535. FortiGate always listens on UDP port 4500 (responder only)

If you're passing your VPN through firewalls, it helps to know which protocols to allow.

IPsec is a suite of separate protocols, which includes:

- Internet Key Exchange (IKE): used to authenticate peers, exchange keys, and negotiate the encryption and checksums that will be used—essentially, it is the *control channel*
- AH: contains the authentication header—the checksums that verify the integrity of the data
- Encapsulating Security Payload (ESP): the encapsulated security payload—the encrypted payload, which is essentially the *data channel*

So, if you must pass IPsec traffic through a firewall, remember that allowing only one protocol or port number is usually not enough.

Note that the IPsec RFC mentions AH, however, AH does not offer encryption, which is an important benefit. Therefore, FortiGate does not use AH. As a result, you don't need to allow the AH IP protocol (51).

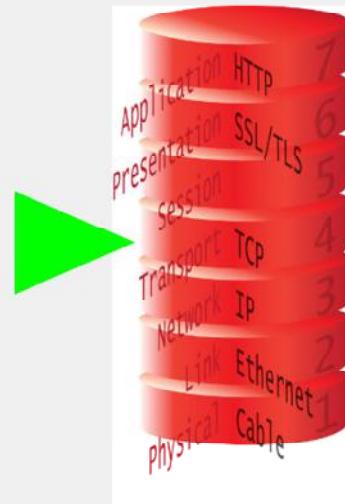
To set up a VPN, you must configure matching settings on both ends of the VPN—whether the VPN is between two FortiGate devices, FortiGate and FortiClient, or a third-party device and FortiGate. If the settings don't match, the tunnel setup fails.

The default ports for standard IKE traffic and IKE NAT-T traffic is UDP 500 and UDP 4500, respectively. You can use the CLI command shown on this slide to configure a custom port for both IKE and IKE NAT-T. The custom port is used to initiate and respond to tunnel requests. If NAT is detected, then the custom port can be used for both IKE and UDP-encapsulated ESP traffic. Note that FortiGate always listens for port UDP 4500 regardless of the custom port settings. This enables FortiGate to negotiate NAT-T tunnels on custom and standard ports.

DO NOT REPRINT**© FORTINET**

How Does IPsec Work?

- Encapsulation
 - Other protocols wrapped inside IPsec
 - What's inside? Varies by mode:
 - Transport mode—TCP/UDP
 - Tunnel mode—additional IP layer, then TCP/UDP
- Negotiation
 - Authentication
 - Handshake to exchange keys, settings

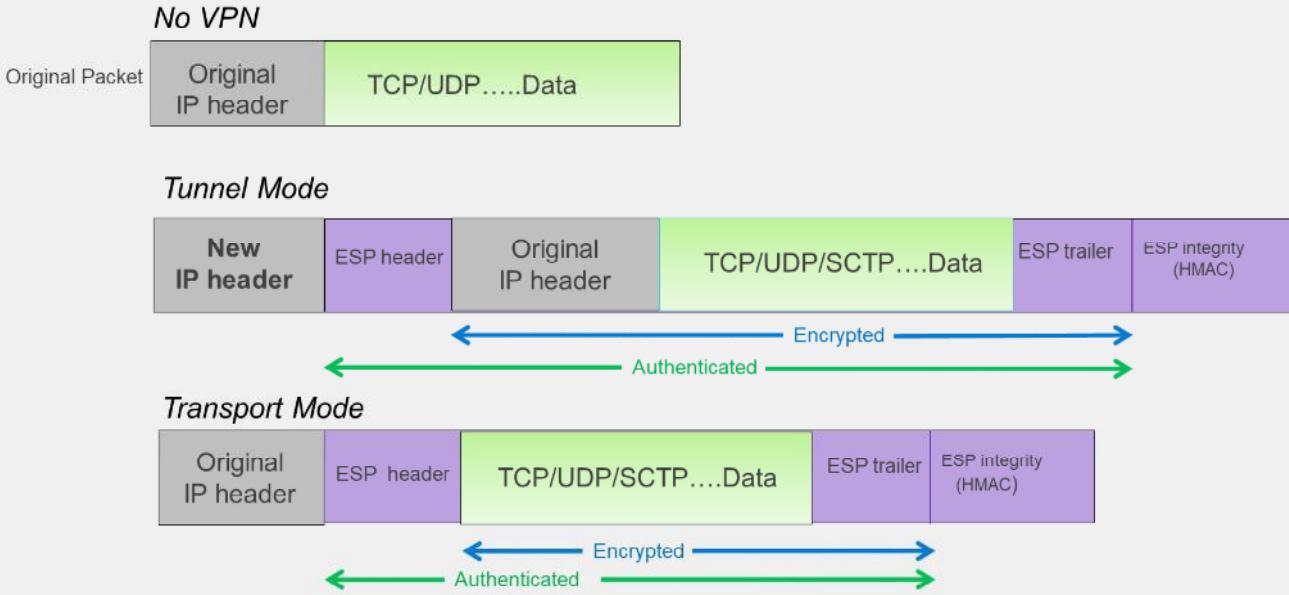


IPsec provides services at the IP (network) layer. During tunnel establishment, both ends negotiate the encryption and authentication algorithms to use.

After the tunnel has been negotiated and is up, data is encrypted and encapsulated into ESP packets.

DO NOT REPRINT
© FORTINET

ESP Encapsulation—Tunnel or Transport Mode



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

7

What's encapsulated? It depends on the encapsulation mode being used. IPsec can operate in two modes: transport mode and tunnel mode.

- Transport mode directly encapsulates and protects the fourth layer (transport) and above. The original IP header is not protected and no additional IP header is added.
- Tunnel mode is a true tunnel. The whole IP packet is encapsulated and a new IP header is added at the beginning. After the IPsec packet reaches the remote LAN and is unwrapped, the original packet can continue on its journey.

Note that after you remove the VPN-related headers, a transport mode packet can't be transmitted any further; it has no second IP header inside, so it's not routable. For that reason, this mode is usually used only for end-to-end (or client-to-client) VPNs.

DO NOT REPRINT

© FORTINET

What Is IKE?

- Default ports: UDP port 500 (and UDP port 4500 when crossing NAT)
- Negotiates a tunnel's private keys, authentication, and encryption
- Phases:
 - Phase 1
 - Phase 2
- Versions
 - IKEv1 (legacy, wider adoption)
 - IKEv2 (new, simpler operation)



© Fortinet Inc. All Rights Reserved.

8

IKE uses UDP port 500. If NAT-T is enabled in a NAT scenario, IKE uses UDP port 4500.

IKE establishes an IPsec VPN tunnel. FortiGate uses IKE to negotiate with the peer and determine the IPsec security association (SA). The IPsec SA defines the authentication, keys, and settings that FortiGate uses to encrypt and decrypt that peer's packets. It is based on the Internet Security Association and Key Management Protocol (ISAKMP).

IKE defines two phases: phase 1 and phase 2.

There are two IKE versions: IKEv1 and IKEv2. Even though IKEv2 is a newer version and features a simpler protocol operation, this lesson focuses on IKEv1 only, because of its much wider adoption.

DO NOT REPRINT

© FORTINET

IKEv1 vs. IKEv2

Feature	IKEv1	IKEv2
Exchange modes	<ul style="list-style-type: none"> Main <ul style="list-style-type: none"> Total messages: 9 (6 for phase 1, 3 for phase 2) Aggressive <ul style="list-style-type: none"> Total messages: 6 (3 for phase 1, 3 for phase 2) 	<ul style="list-style-type: none"> One exchange procedure only Total messages: 4 (one child SA only)
Authentication methods	<p>Symmetric:</p> <ul style="list-style-type: none"> Pre-shared key (PSK) Certificate signature Extended authentication (XAuth) 	<p>Asymmetric:</p> <ul style="list-style-type: none"> PSK Certificate signature EAP (pass-through—no client support)
NAT-T	Supported as extension	Native support
Reliability	Unreliable—messages are not acknowledged	Reliable—messages are acknowledged
Dial-up phase 1 matching by ID	<ul style="list-style-type: none"> Peer ID + aggressive mode + PSK Peer ID + main mode + certificate signature 	<ul style="list-style-type: none"> Peer ID Network ID
Traffic selector narrowing	Not supported	Supported

This slide shows a table comparing some of the IKEv1 and IKEv2 features that FortiOS supports. IKEv2 provides a simpler operation, which is the result of using a single exchange mode and requiring less messages to bring up the tunnel.

Authentication-wise, both versions support PSK and certificate signature. Although only IKEv1 supports XAuth, IKEv2 supports EAP, which is equivalent to XAuth. However, the FortiOS IKEv2 EAP implementation is pass-through only. That is, FortiOS doesn't support EAP as a client, which means that you cannot revoke access to peers using IKEv2 unless you use a certificate signature. With IKEv1, you can deny access to VPN peers without having to use a certificate signature by using XAuth. IKEv2 also supports asymmetric authentication, which enables you to configure each peer to use a different authentication method.

Both IKE versions support NAT-T. However, IKEv2 supports NAT-T natively, while IKEv1 supports NAT-T as an extension. Also, IKEv2 is a more reliable protocol than IKEv1 because, like TCP, peers must acknowledge the messages exchanged between them. IKEv1 doesn't support such a mechanism.

When you configure multiple dial-up IPsec VPNs, IKEv2 makes it simpler to match the intended gateway by peer ID. With IKEv2, you can either use the standard peer ID attribute or the Fortinet proprietary network ID attribute to indicate the phase 1 gateway to match on the dial-up server, regardless of the authentication mode in use. However, with IKEv1, you can use the peer ID only, and then combine it with aggressive mode and pre-shared key authentication, or with main mode and certificate signature authentication.

Finally, IKEv2 allows the responder to choose a subset of the traffic the initiator proposes. This is called traffic selector narrowing and enables you to have more flexible phase 2 selector configurations. Traffic selector narrowing enables a peer to automatically narrow down its traffic selector addresses, so it agrees with the traffic selector the remote peer proposes.

DO NOT REPRINT**© FORTINET**

Negotiation—Security Association (SA)

- IKE allows the parties involved in a transaction to set up their Security Associations (SAs)
 - SAs are the basis for building security functions into IPsec
 - In normal two-way traffic, the exchange is secured by a pair of SAs
 - IPsec administrators decide the encryption and authentication algorithms that can be used in the exchange
- IKE uses two distinct phases:
 - Phase 1 → Outcome: IKE SA
 - Phase 2 → Outcome: IPsec SA



© Fortinet Inc. All Rights Reserved.

10

In order to create an IPsec tunnel, both devices must establish their SAs and secret keys, which are facilitated by the IKE protocol.

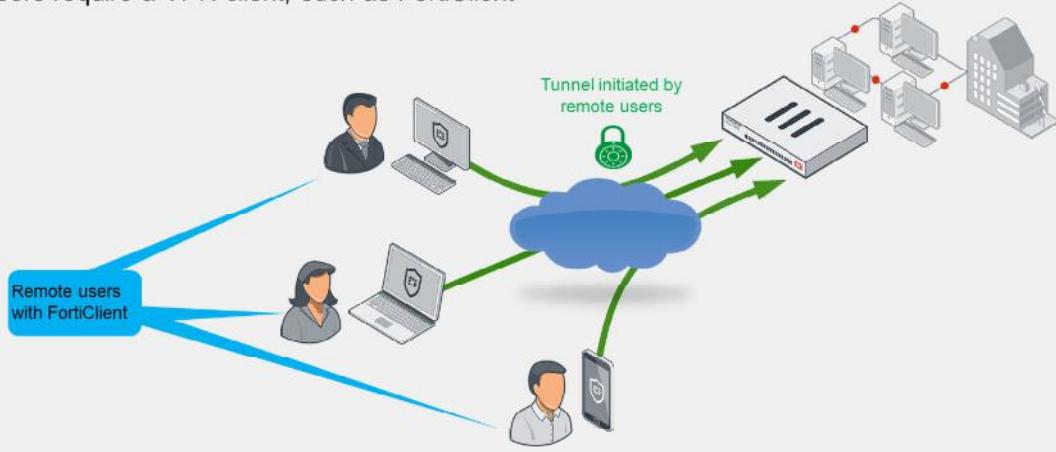
The IPsec architecture uses SAs as the basis for building security functions into IPsec. An SA is the bundle of algorithms and parameters being used to encrypt and authenticate data travelling through the tunnel. In normal two-way traffic, this exchange is secured by a pair of SAs, one for each traffic direction. Essentially, both sides of the tunnel must agree on the security rules. If both sides cannot agree on the rules for sending data and verifying each other's identity, then the tunnel is not established. SAs expire and need to be renegotiated by the peers after they have reached their lifetime.

IKE uses two distinct phases: phase 1 and phase 2. Each phase negotiates different SA types. The SA negotiated during phase 1 is called IKE SA, and the SA negotiated during phase 2 is called IPsec SA. FortiGate uses IKE SAs for setting up a secure channel to negotiate IPsec SAs. FortiGate uses IPsec SAs for encrypting and decrypting the data sent and received, respectively, through the tunnel.

DO NOT REPRINT
© FORTINET

VPN Topologies—Remote Access

- Remote users connect to corporate resources
 - FortiGate is configured as dial-up server—only clients can initiate the VPN
 - Users require a VPN client, such as FortiClient



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

Use remote access VPNs when remote internet users need to securely connect to the office to access corporate resources. The remote user connects to a VPN server located on the corporate premises, such as FortiGate, to establish a secure tunnel. After the user is authenticated, FortiGate provides access to network resources, based on the permissions granted to that user.

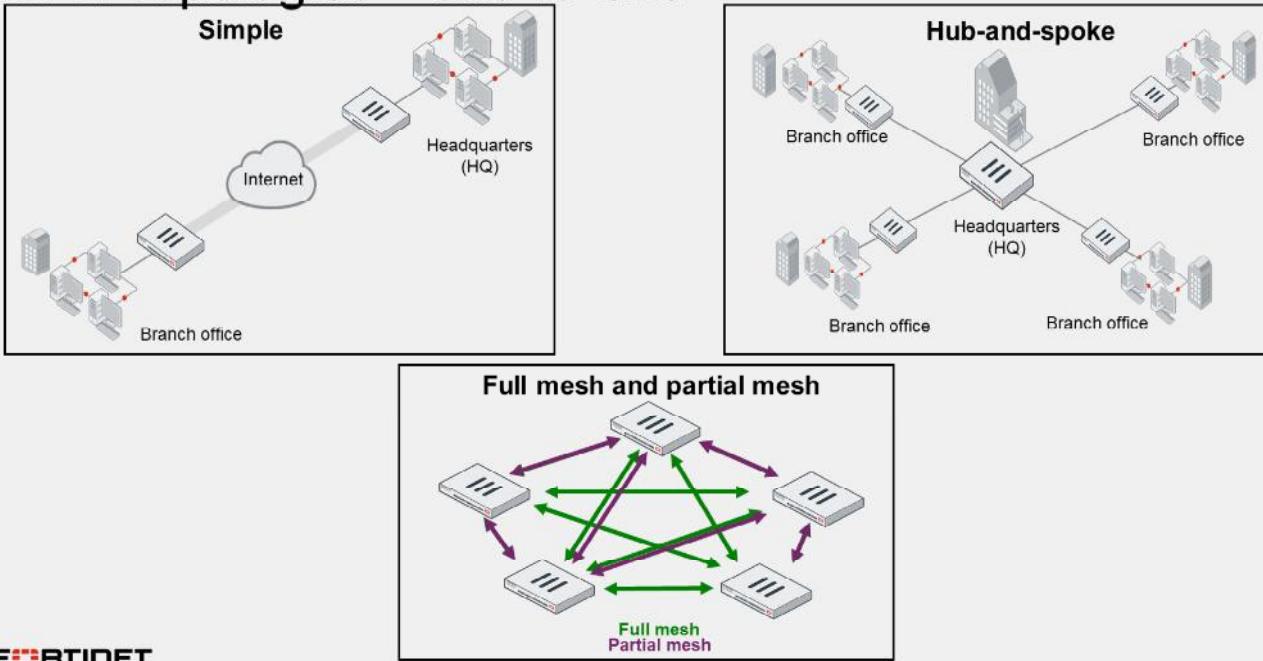
In a remote access VPN, FortiGate is usually configured as a dial-up server. You will learn more about dial-up VPNs in this lesson. The IP address of the remote internet user is usually dynamic. Because FortiGate does not know the IP address of the remote user, only the remote user can initiate a VPN connection request.

The remote user side needs a VPN client, such as FortiClient. You must configure FortiClient to match the VPN server settings. FortiClient takes care of establishing the tunnel, as well as routing the traffic destined to the remote site through the tunnel.

In addition, you can use one remote access VPN configuration on your FortiGate device for many remote users. FortiGate establishes a separate tunnel for each of them.

DO NOT REPRINT
© FORTINET

VPN Topologies—Site-to-Site



12

Site-to-site VPN is also known as LAN-to-LAN VPN. A simple site-to-site deployment involves two peers communicating directly to connect two networks located at different offices.

When you need to connect more than two locations, you can use a hub-and-spoke topology. In hub-and-spoke, all clients connect through a central hub. In the example shown on this slide, the clients—spokes—are branch office FortiGate devices. For any branch office to reach another branch office, its traffic must pass through the hub. One advantage of this topology is that the configuration needed is easy to manage. Another advantage is that only the FortiGate at HQ must be very powerful because it handles all tunnels simultaneously, while the branch office FortiGate devices require much fewer resources because they maintain only one tunnel. One disadvantage is that communication between branch offices through HQ is slower than in a direct connection, especially if your HQ is physically distant. Also, if the FortiGate device at HQ fails, VPN failure is company-wide.

In a mesh topology, you can connect FortiGate devices directly and therefore bypass HQ. Two variations of mesh topology exist: full mesh and partial mesh. Full mesh connects every location to every other location. The higher the number of FortiGate devices, the higher the number of tunnels to configure on each FortiGate device. For example, in a topology with five FortiGate devices, you would need to configure four tunnels on each device, for a total of 20 tunnels. This topology causes less latency and requires much less HQ bandwidth than hub-and-spoke, but requires each FortiGate device to be more powerful. Partial mesh attempts to compromise, minimizing required resources but also latency. Partial mesh can be appropriate if communication is not required between every location. However, the configuration of each FortiGate device is more complex than in hub-and-spoke. Routing, especially, may require extensive planning.

Generally, the more locations you have, hub-and-spoke will be cheaper, but slower, than a mesh topology. Mesh places less strain on the central location. It's more fault-tolerant, but also more expensive.

DO NOT REPRINT**© FORTINET**

VPN Topologies—Comparison

Hub-and-Spoke	Partial Mesh	Full Mesh
Easy configuration	Moderate configuration	Complex configuration
Few tunnels	Medium number of tunnels	Many tunnels
High central bandwidth	Medium bandwidth in hub sites	Low bandwidth
Not fault tolerant	Some fault tolerance	Fault tolerant
Low system requirements on average, but high for center	Medium system requirements	High system requirements
Scalable	Somewhat scalable	Difficult to scale
No direct communication between spokes	Direct communication between some sites	Direct communication between all sites

To review, this slide shows a high-level comparison of VPN topologies. You should choose the topology that is most appropriate to your situation.