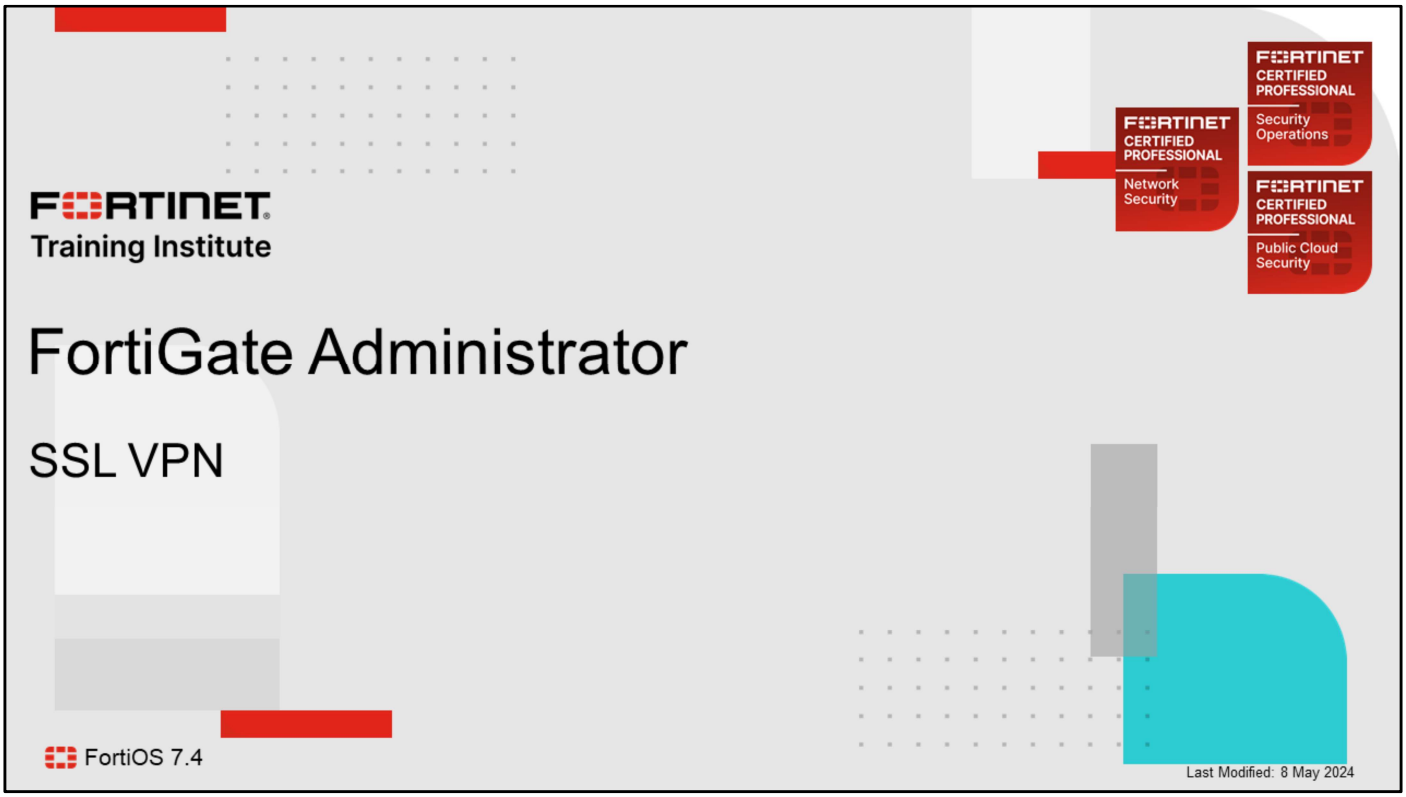


In this lesson, you will learn how to configure and use SSL VPNs. SSL VPNs are an easy way to give remote users access to your private network.

Objectives

- Configure SSL VPN portals
- Configure tunnel mode SSL VPN
- Monitor SSL VPN-connected users
- Troubleshoot common SSL VPN issues

FORTINET Training Institute

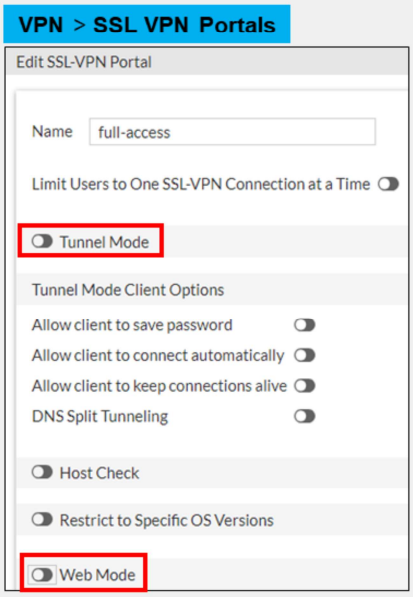
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the different ways FortiGate allows SSL VPN connections, you will be able to better design the configuration and architecture of your SSL VPN. You will also be able to avoid, identify, and solve common issues and misconfigurations.

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
```



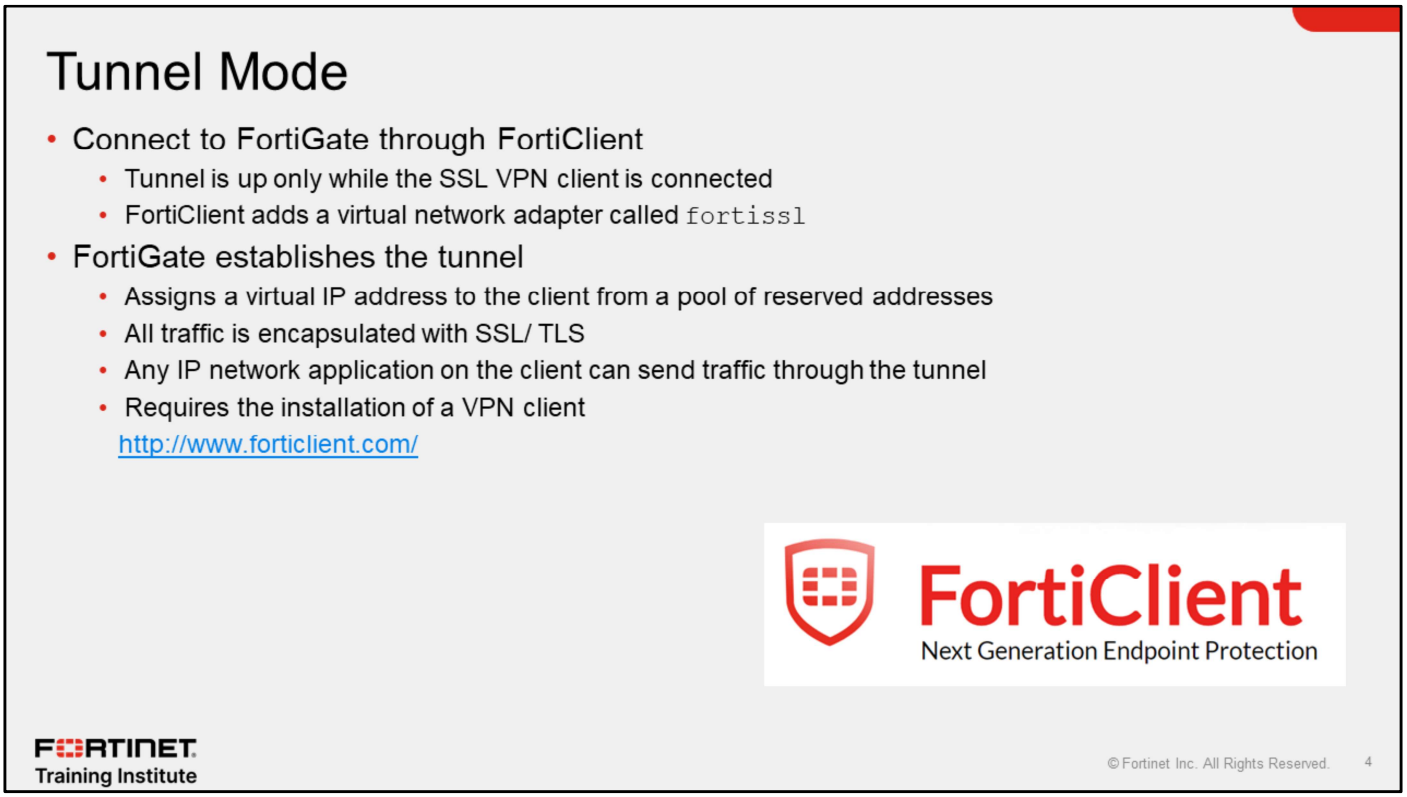
FORTINET Training Institute

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. You will only learn SSL VPN tunnel mode in this lesson.



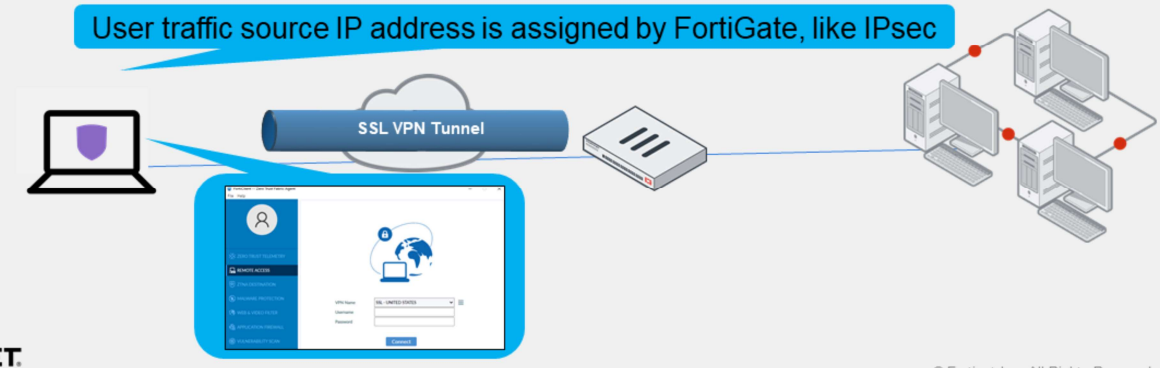
Tunnel mode is the second option FortiGate provides to access resources within an SSL VPN.

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

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)



FORTINET Training Institute

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.

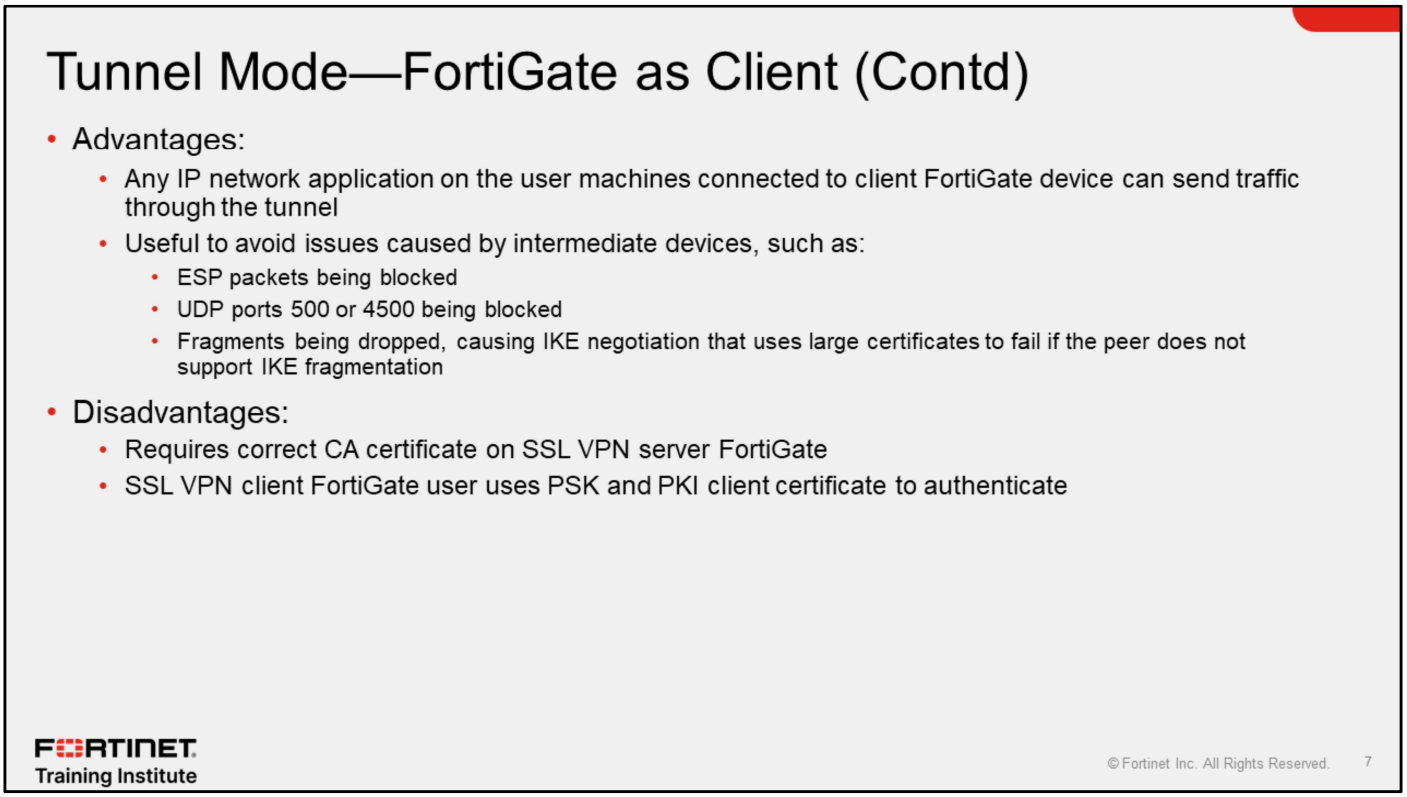
FortiClient encrypts all traffic from the remote computer and sends it over the SSL VPN tunnel. FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

Tunnel Mode—FortiGate as Client

- Connect to server FortiGate device as SSL VPN client
  - Use *SSL VPN Tunnel* interface type
  - Devices connected to client FortiGate 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 from a pool of reserved addresses

FORTINET Training Institute

You can configure FortiGate 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 the SSL VPN server returns. You can define policies to allow users who 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 you to configure hub-and-spoke topologies with FortiGate devices as both the SSL VPN hub and spokes. This can be useful to avoid issues caused by intermediate devices, such as:

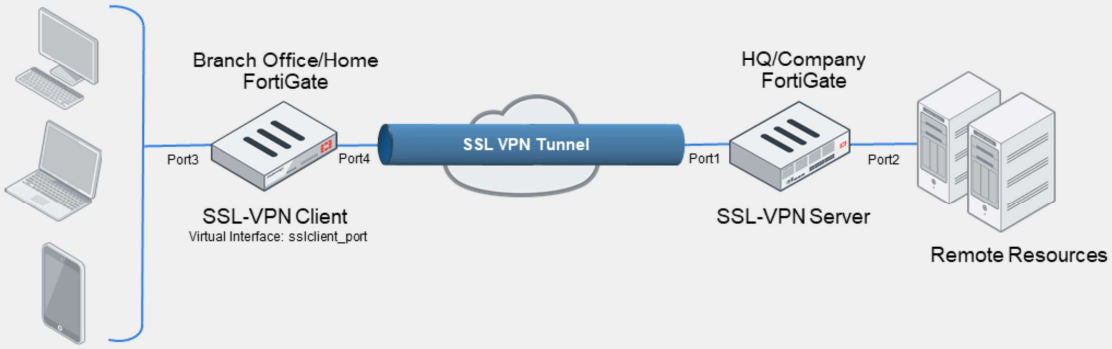
- ESP packets being blocked
- UDP ports 500 or 4500 being blocked
- Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation

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 the route distance or priority according to your requirements. To prevent a default route being learned on the SSL VPN client, define a specific destination on the SSL VPN server. Split tunneling is used so that only the destination addresses defined in the server firewall policies are routed to the server, and all other traffic is connected directly to the internet.

This configuration requires you to install the correct CA certificate because the SSL VPN client FortiGate/user uses PSK and a PKI client certificate to authenticate. You must install the correct CA certificate on the FortiGate devices to verify the certificate chain to the root CA that signed the certificate.

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)

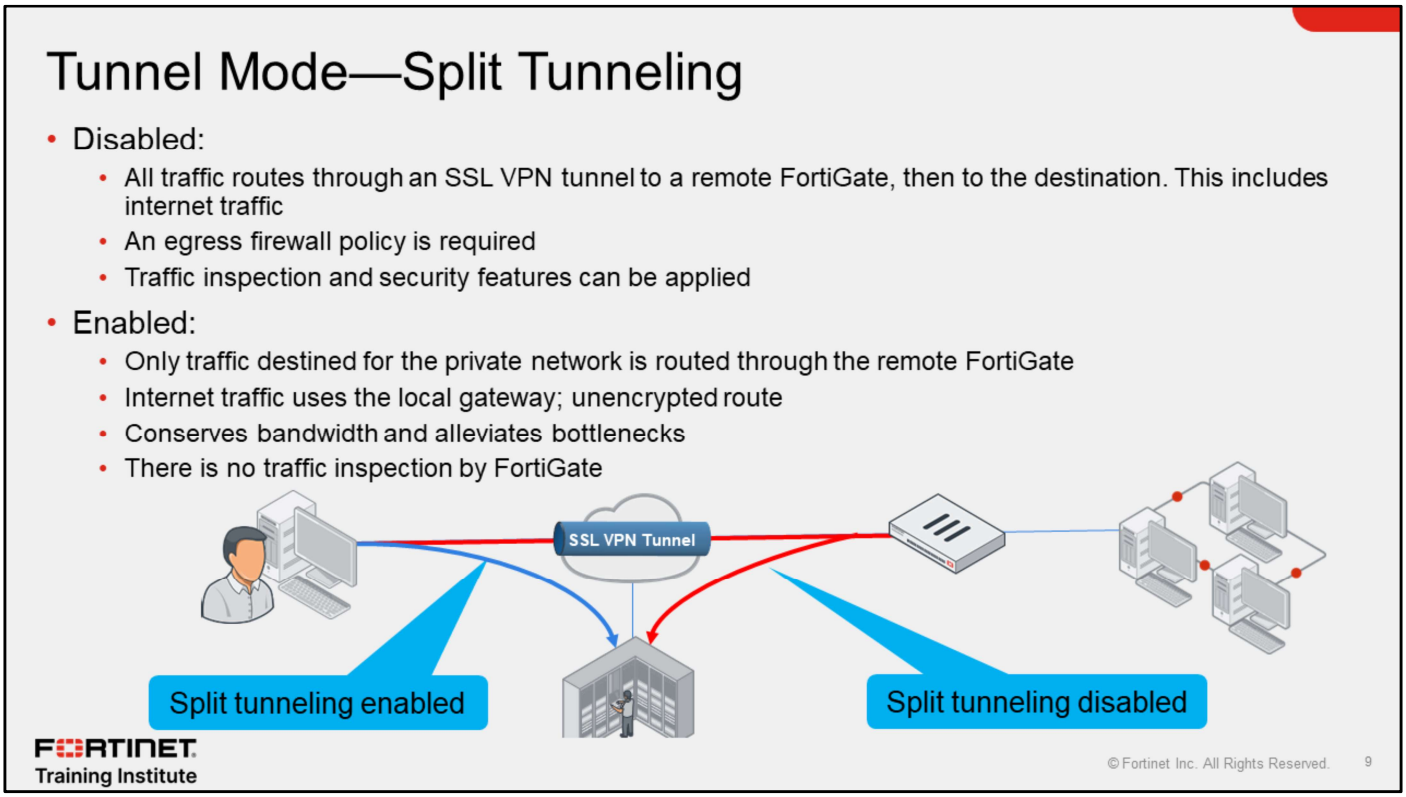


FORTINET Training Institute

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.



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:

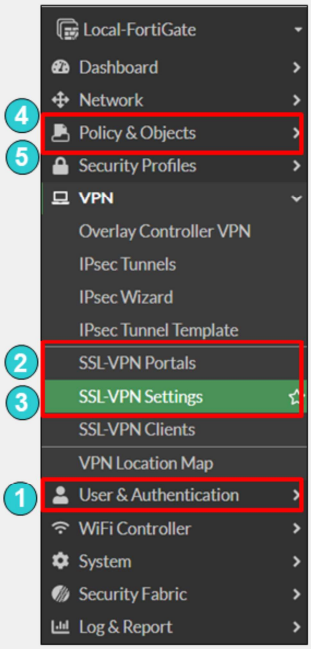
- To make all traffic default to the SSL VPN server and still have a route to the server's listening interface, on the SSL VPN client, set a lower distance for the default route that is learned from the server.
- To include both default routes in the routing table, with the route learned from the SSL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

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
     - You can use FortiGate to apply security profiles

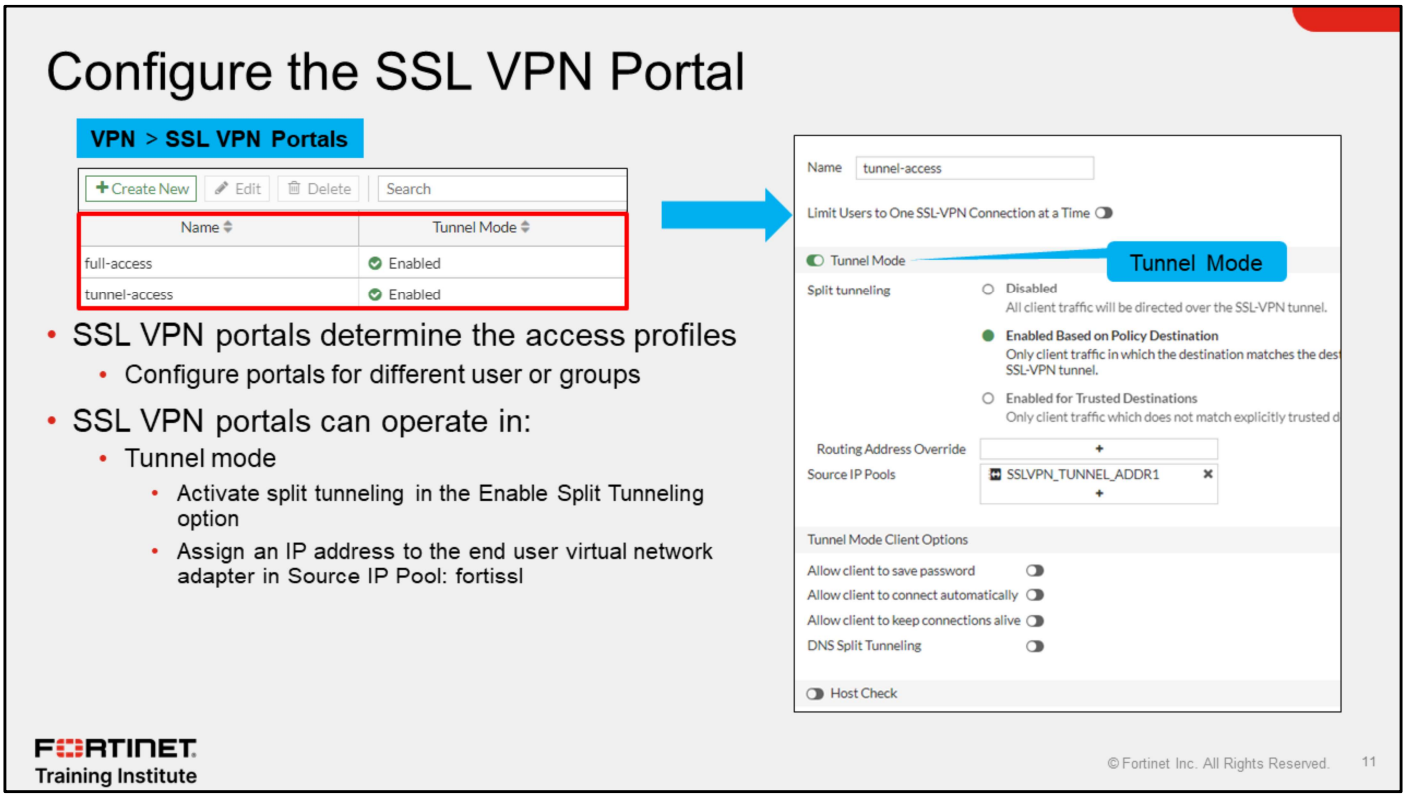


FORTINET Training Institute

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

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

This slide shows the steps an administrator must take to configure SSL VPN. You can configure some steps in a different order than what is shown on this slide.

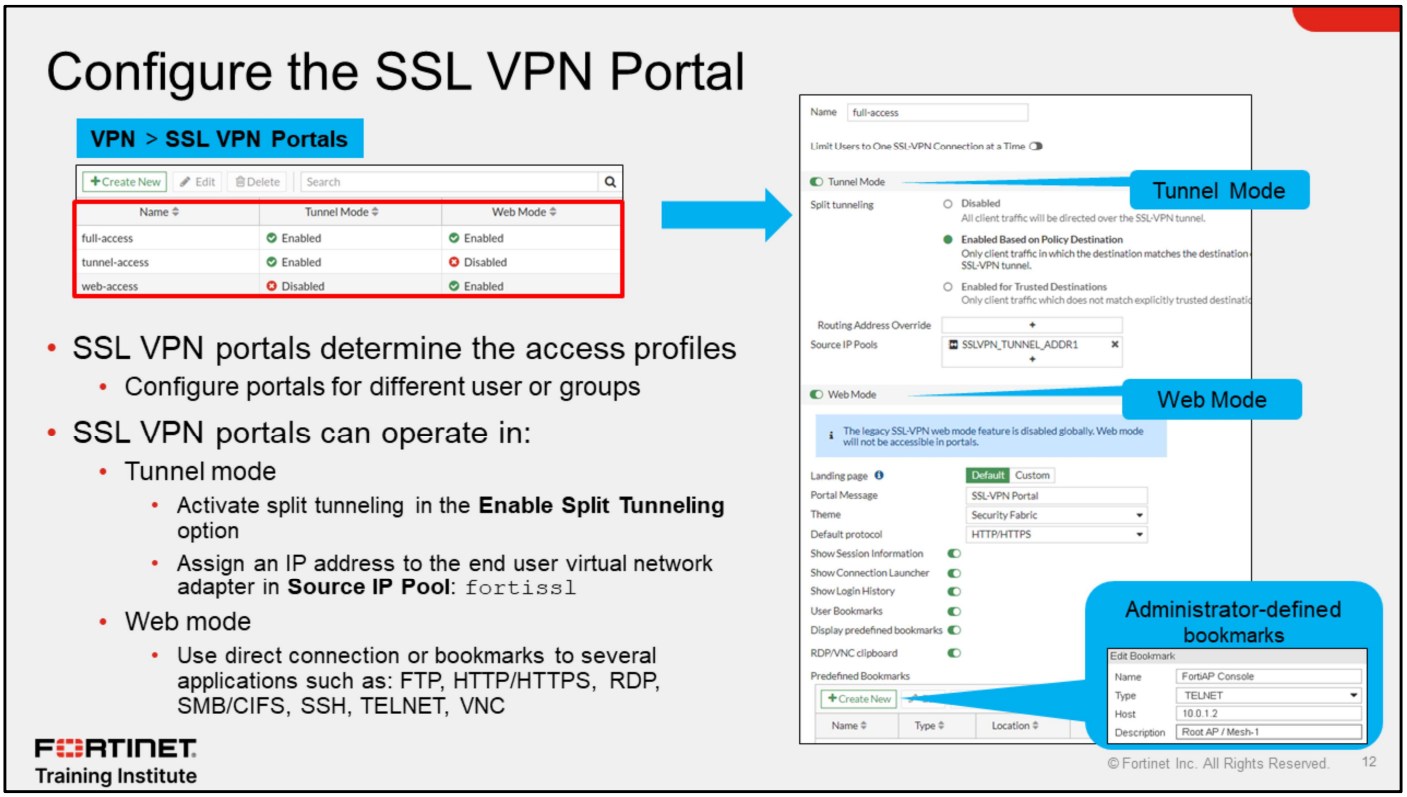


The next step is to configure the SSL VPN portal(s). An SSL VPN portal contains tools and resource links for the users to access.

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.

Routing Address Override allows you to define the destination network (usually the corporate network) that routes through the tunnel. If you don't select the **Routing Address Override**, the destination address in the respective firewall policies defines the destination network.

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.



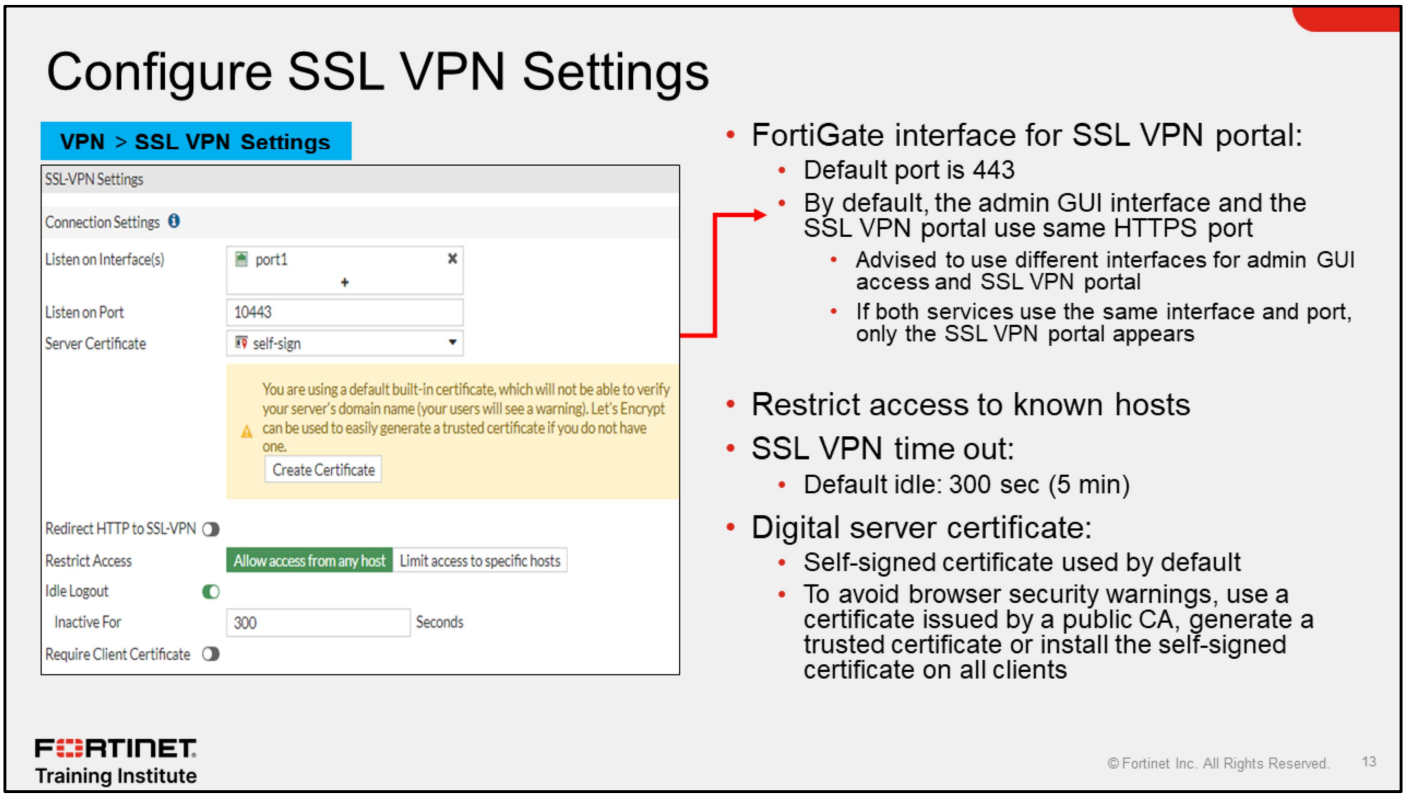
The next step is to configure the SSL VPN portal(s). An SSL VPN portal contains tools and resource links for the users to access.

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.

Routing Address Override allows you to define the destination network (usually the corporate network) that routes through the tunnel. If you don't select the **Routing Address Override**, the destination address in the respective firewall policies defines the destination network.

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.



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.

Configure SSL VPN Settings (Contd)

- Define the IP range for the SSL VPN
  - IPs are assigned to clients' virtual adapters while joined to VPN
- 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
    - You cannot delete this portal

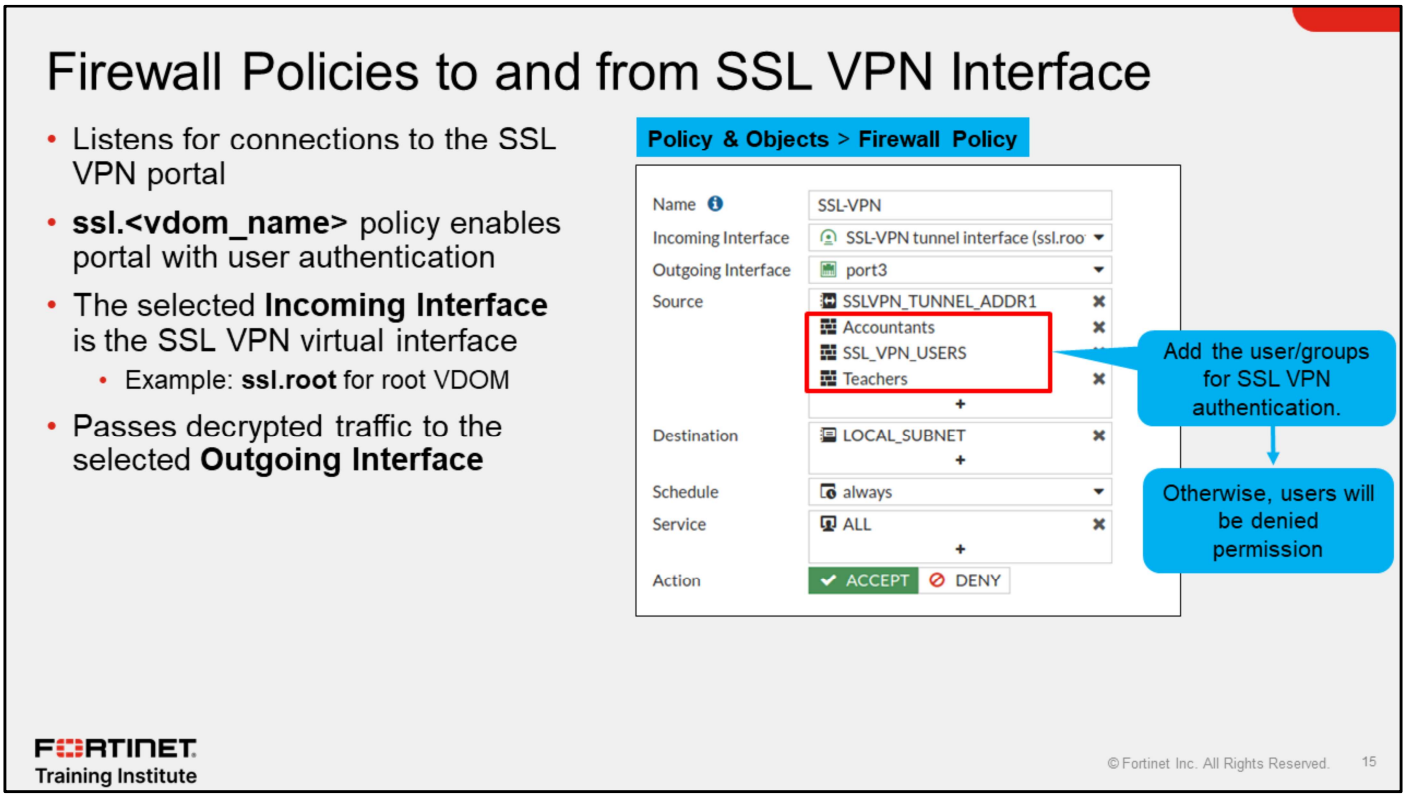
FORTINET Training Institute

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.

DNS server resolution is effective only when the DNS traffic is sent over the VPN tunnel. Usually, this is the case only when split tunnel mode is disabled and all traffic is 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 **Teacher_Portal**. Accountants can connect to **tunnel-access** portal.



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

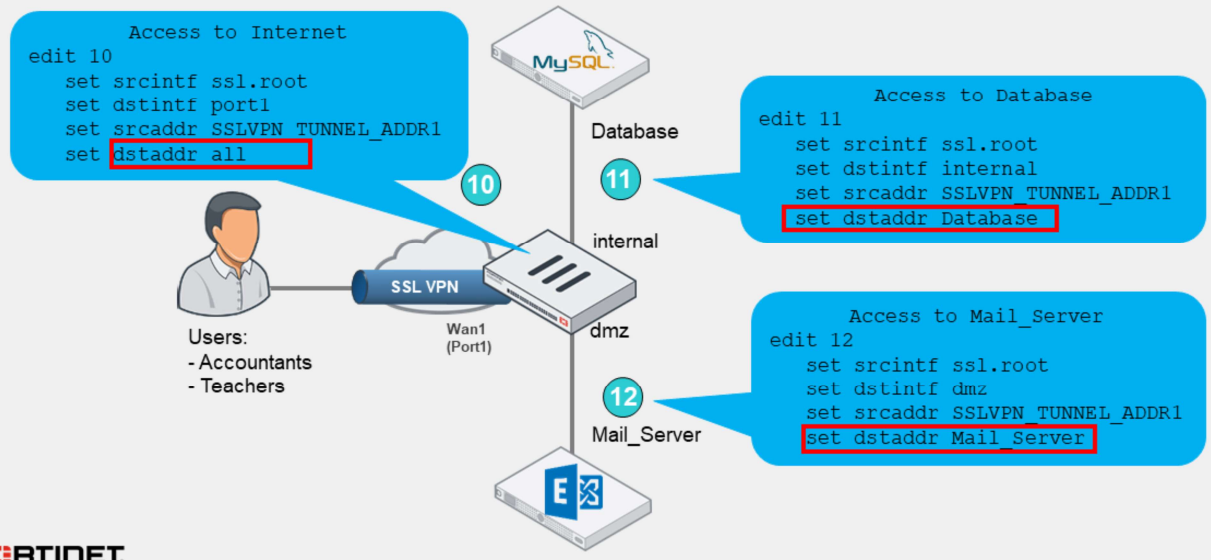
SSL VPN traffic on FortiGate uses a virtual interface called `ssl.<vdom_name>`. Each virtual domain (VDOM) contains a different virtual interface based on its name. By default, if VDOMs are not enabled, then the device operates with a single VDOM called *root*.

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.

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

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.

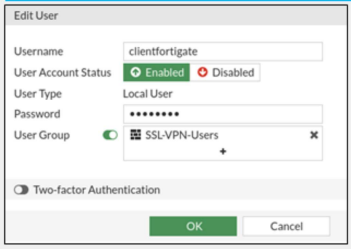
Optionally, if split tunneling is disabled, you need to create an additional firewall policy from `ssl.root` to the egress interface to allow clients access to the internet.

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

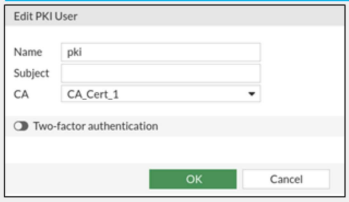
Configuring SSL VPN—FortiGate as Server

- SSL VPN Server FortiGate
  1. 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
  2. Configure SSL VPN portals
  3. Configure SSL VPN settings
     - Authentication rules include both accounts using CLI
  4. Create a firewall policy to and from the SSL VPN interface
  5. Create a firewall policy to allow SSL VPN traffic to the internet (optional)

User & Authentication > User Definition



User & Authentication > PKI



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

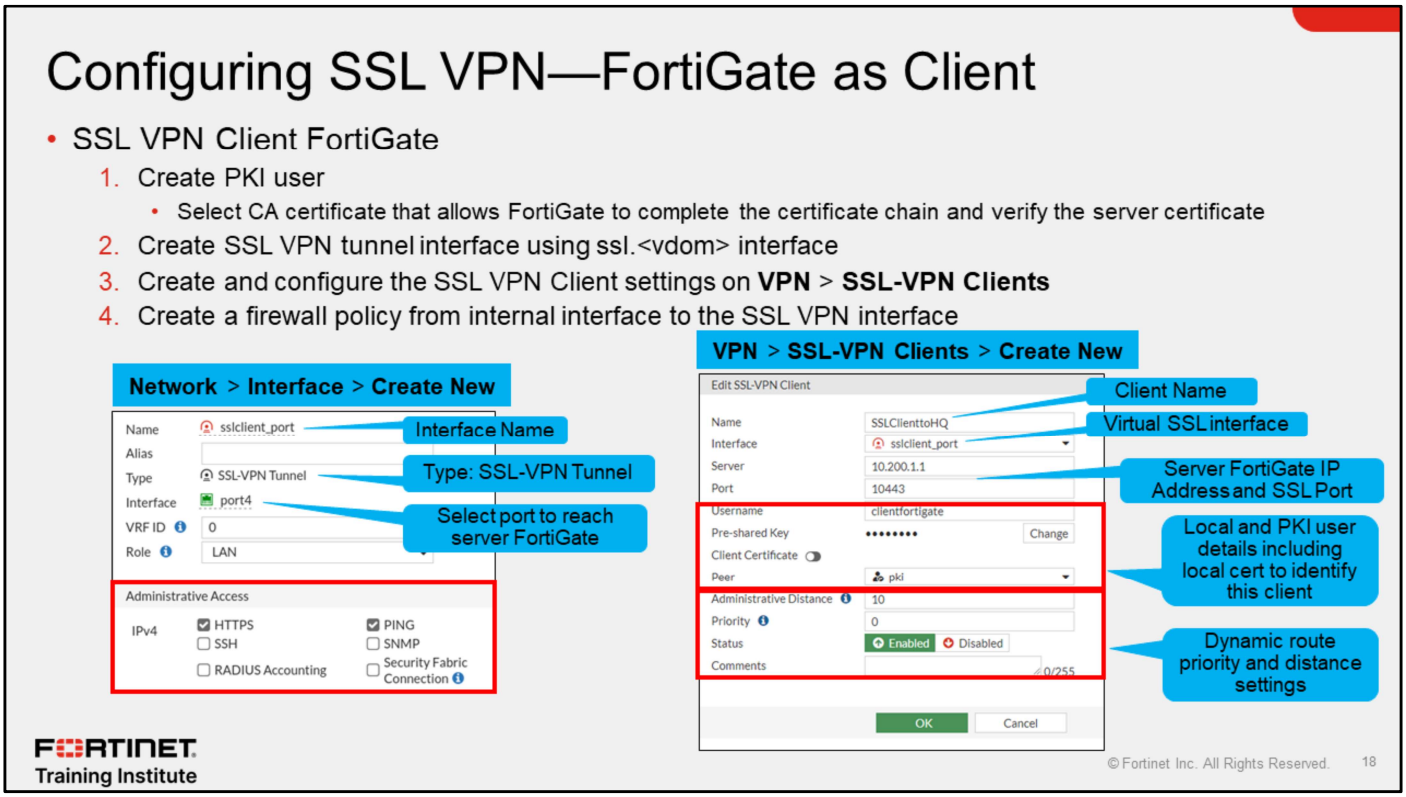
```
config user peer
   edit pki
       set ca "CA_Cert_1
       set cn "FGVM01TM905"
   end
```

FORTINET Training Institute

To configure FortiGate as an SSL VPN server, you must take the steps shown on this slide.

This includes local or remote user accounts or groups and PKI users. The PKI menu is available on the GUI only after you have created a PKI user using the CLI. You can configure a CN only on the CLI. If you do not specify a CN, then any certificate that is signed by the CA is considered valid and matched. Client authentication requires both the client certificate and username and password.

The other steps are identical to SSL VPN setup for remote users. You can configure some steps in a different order than what is shown on this slide.



This slides shows the steps you must take to configure FortiGate as an SSL VPN client.

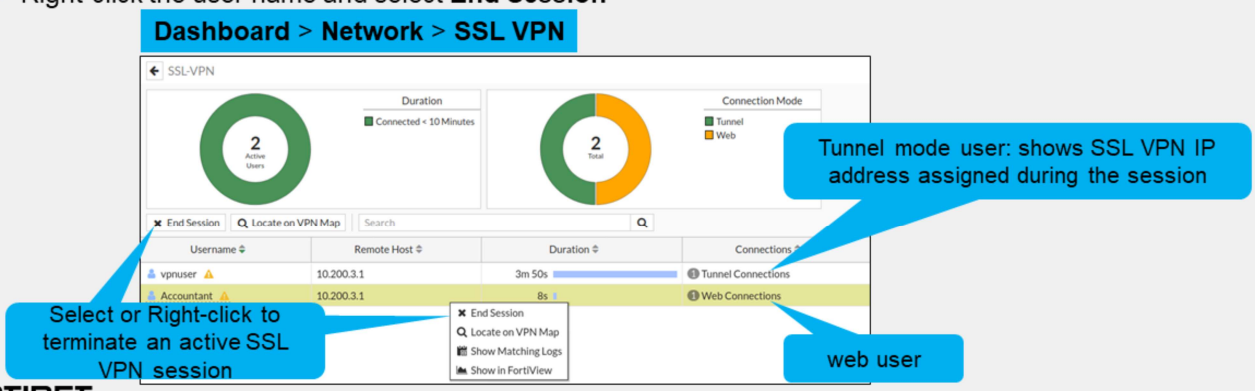
The PKI user must have the same CN if a CN is configured on the SSL VPN server FortiGate certificate. You must also select a CA certificate that allows FortiGate to complete the certificate chain and verify the server certificate. Next, create the SSL VPN tunnel interface using the ssl.<vdom> interface.

The **SSL-VPN Clients** settings include name, virtual SSL VPN interface, SSL VPN server FortiGate IP address and SSL port number, and local username, password and PKI(Peer) user. The **Client Certificate** as shown on this slide is the local certificate that is used to identify this client, and is assumed to already be installed on FortiGate. The SSL VPN server requires it for authentication.

Lastly, you must create a firewall policy to allow traffic from the internal interface to the SSL VPN interface.

Monitoring SSL VPN Sessions

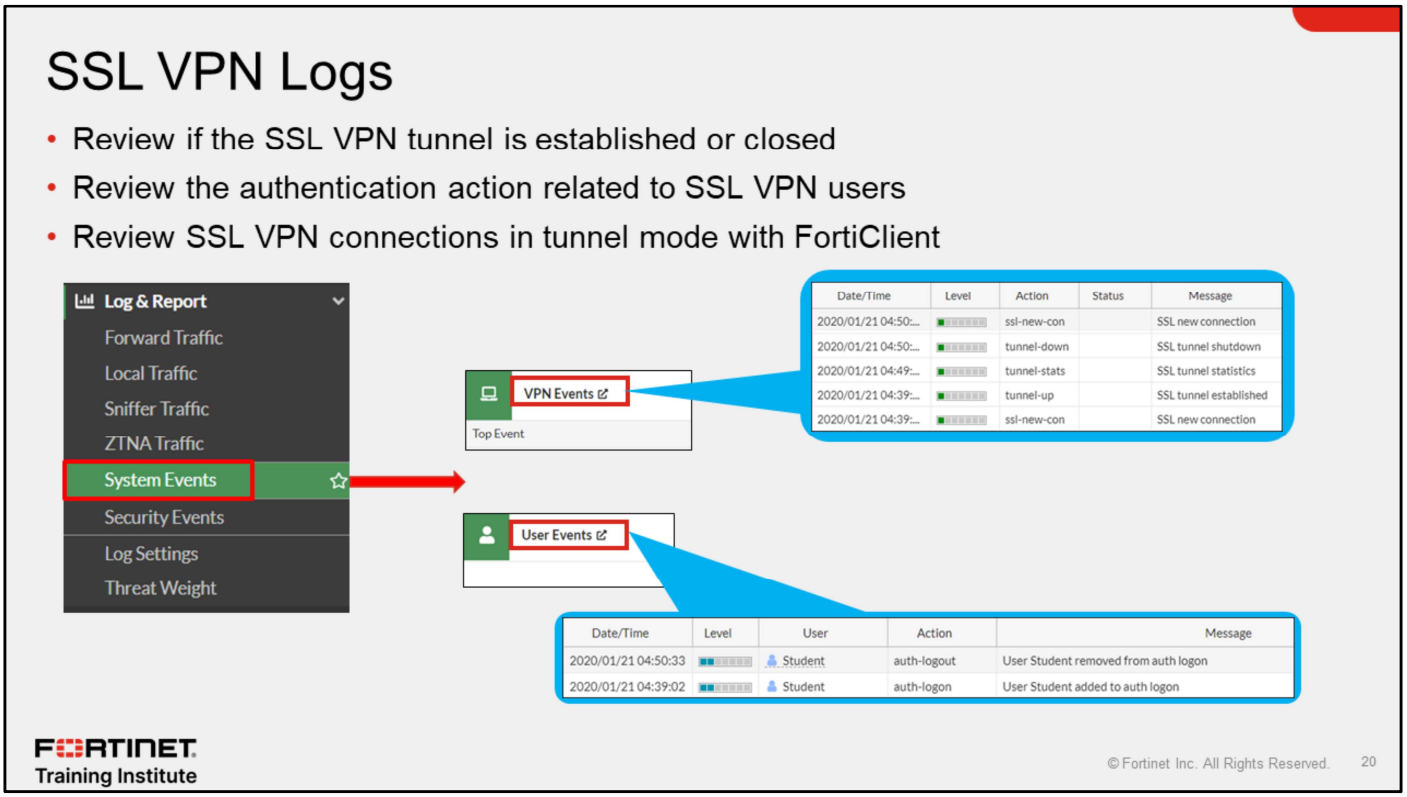
- Monitor which SSL VPN users are connected
  - GUI: **Dashboard** > **Network** > **SSL VPN**
- Shows SSL VPN user names, connection times, and IP addresses
  - For tunnel mode, **Active Connections** displays IP address assigned to `fortissl` virtual adapter
- Force end user disconnection
  - Right-click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



FORTINET Training Institute

You can monitor which SSL VPN users are connected on the **SSL VPN** widget. This shows the names of all SSL VPN users who 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.

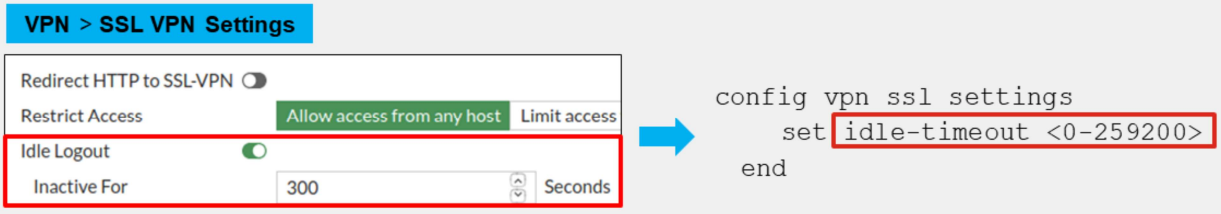


You can also review SSL VPN logs. On **Log & Report** > **System Events**:

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

SSL VPN Idle Timeout vs. Authentication Session

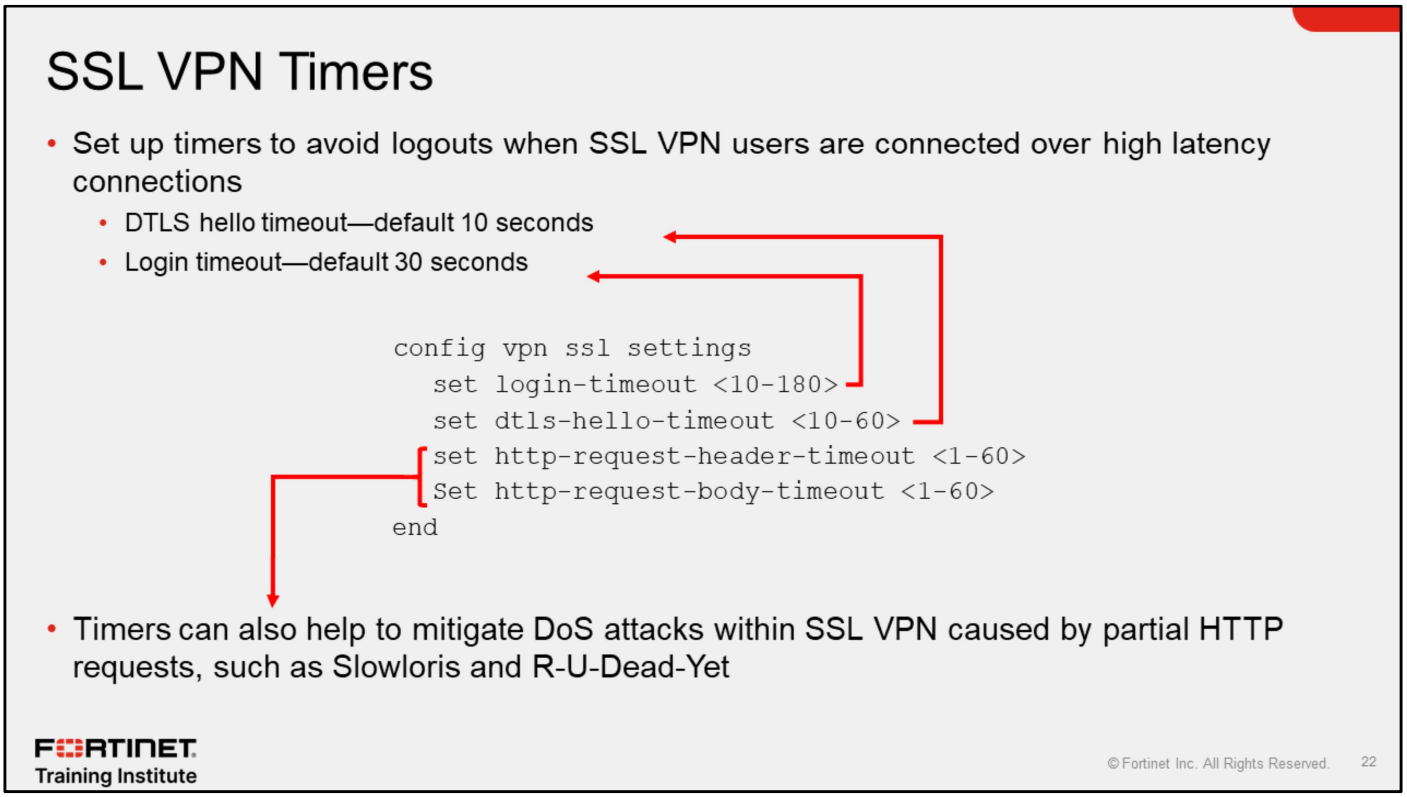
- Firewall policy authentication session is associated with SSL VPN tunnel session
  - Firewall policy authentication session is forced to end when SSL VPN tunnel session ends
  - Prevents reuse of authenticated SSL VPN firewall sessions (not yet expired) by a different user, after the initial user terminates 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



FORTINET Training Institute

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.



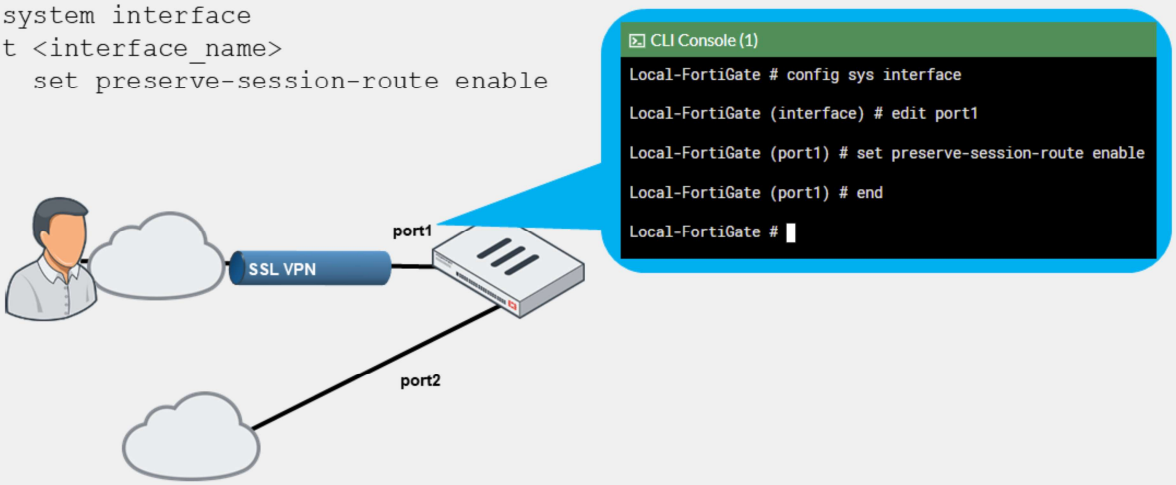
When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under `config vpn ssl settings` have been added to address this. The first command allows 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.

SSL VPN—Session Preservation

- Set session preservation on interface to avoid SSL VPN disconnections
  - Multi-WAN setup

```
config system interface
    edit <interface_name>
        set preserve-session-route enable
end
```

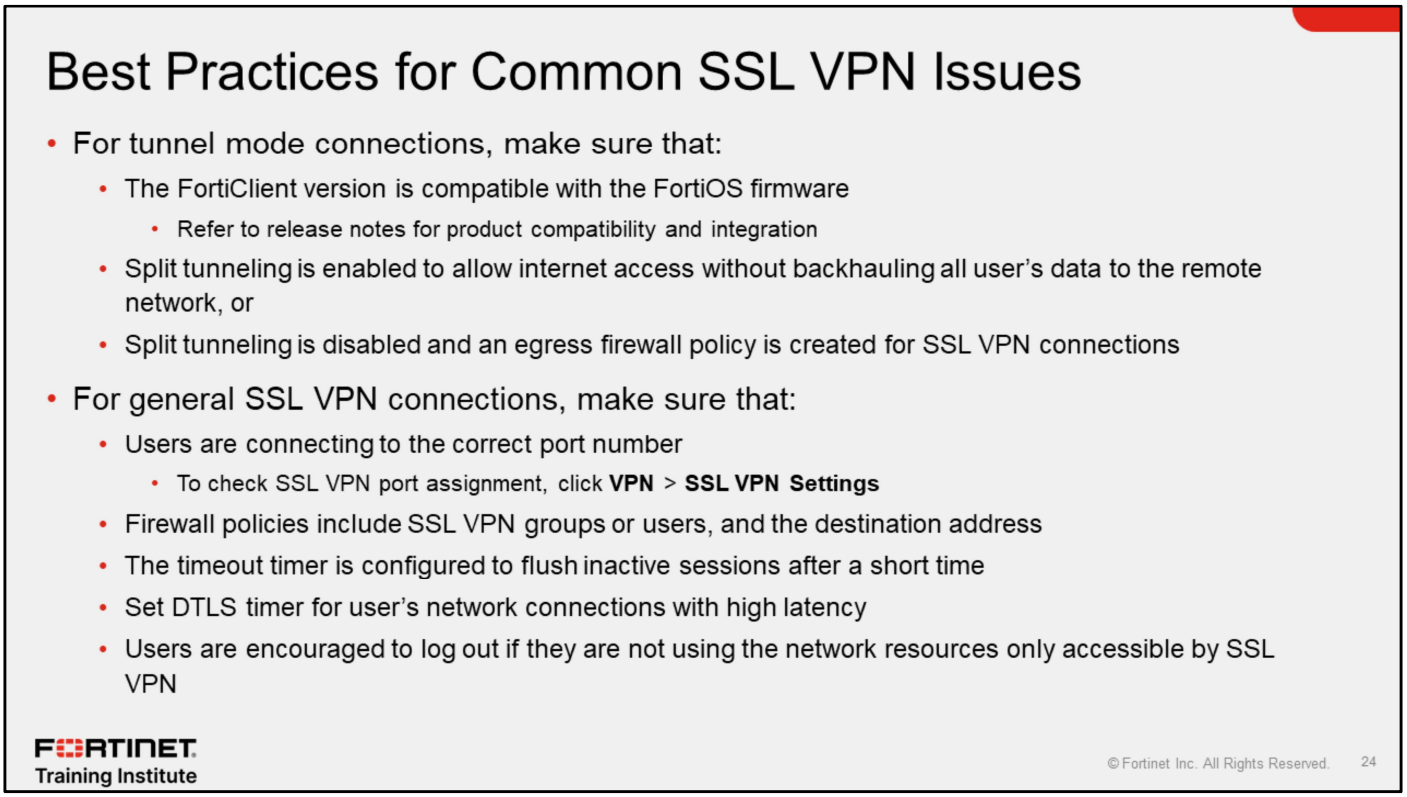


FORTINET Training Institute

In the typical enterprise network, there can be multiple WAN links. In the FortiGate, by default, any session with source NAT disabled go through the route lookup when routing table changes. The sessions are marked dirty after changes to routing table and reevaluated. Because of these route changes in multi-WAN setup, there is possibility that request comes from one interface and response goes out through other causing disconnections.

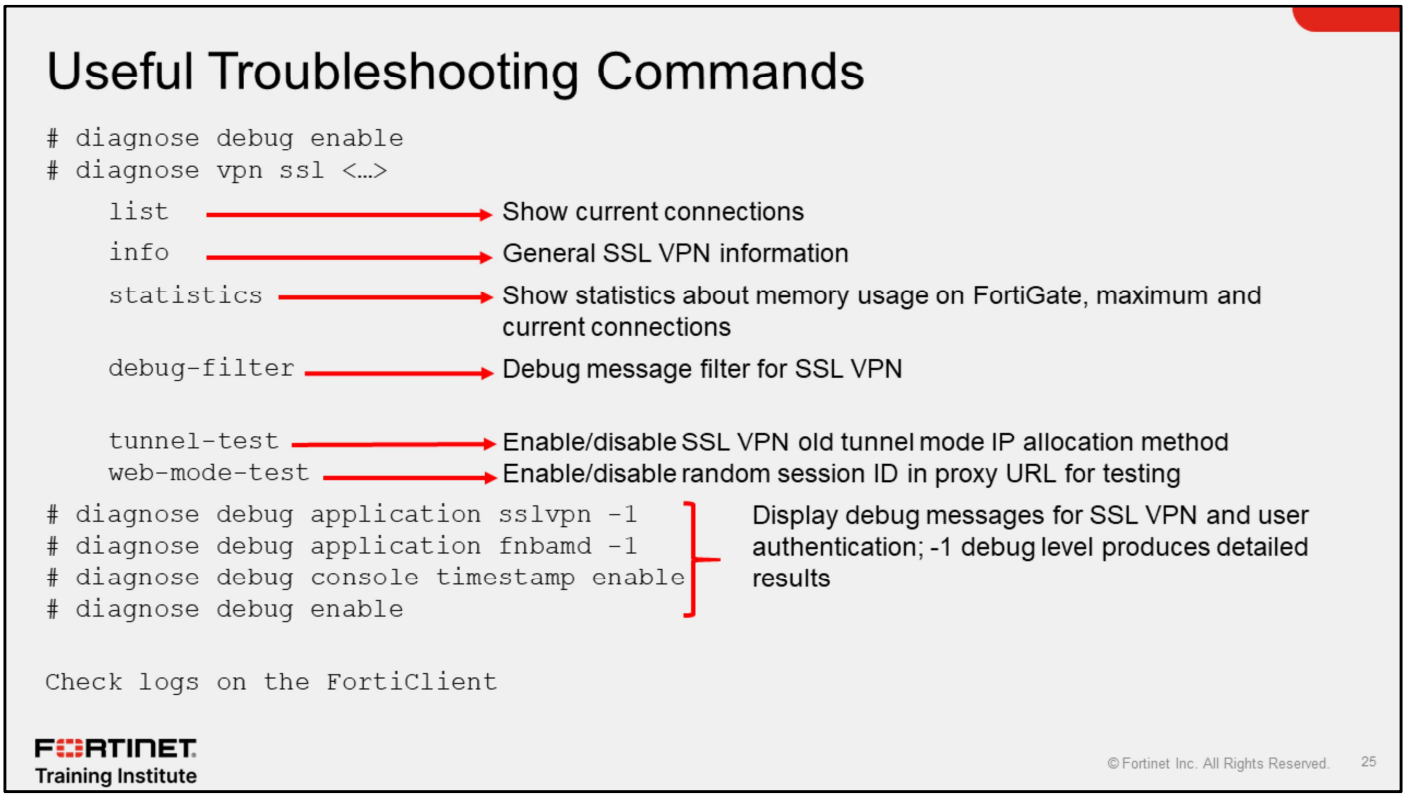
The `set preserve-session-route` command keeps the session on same interface even if session is eligible for routing changes. By default, route preservation is disabled on the interface.

The example on this slide shows `port1` is reserved for SSL VPN connections and `port2` is used for other services. Even if `port2` becomes primary connection because of route changes, FortiGate will keep the existing SSL VPN sessions on `port1` interface.



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:

- 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
- Set DTLS timeout for high latency network connections
- Flush inactive sessions by timeout



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
- `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

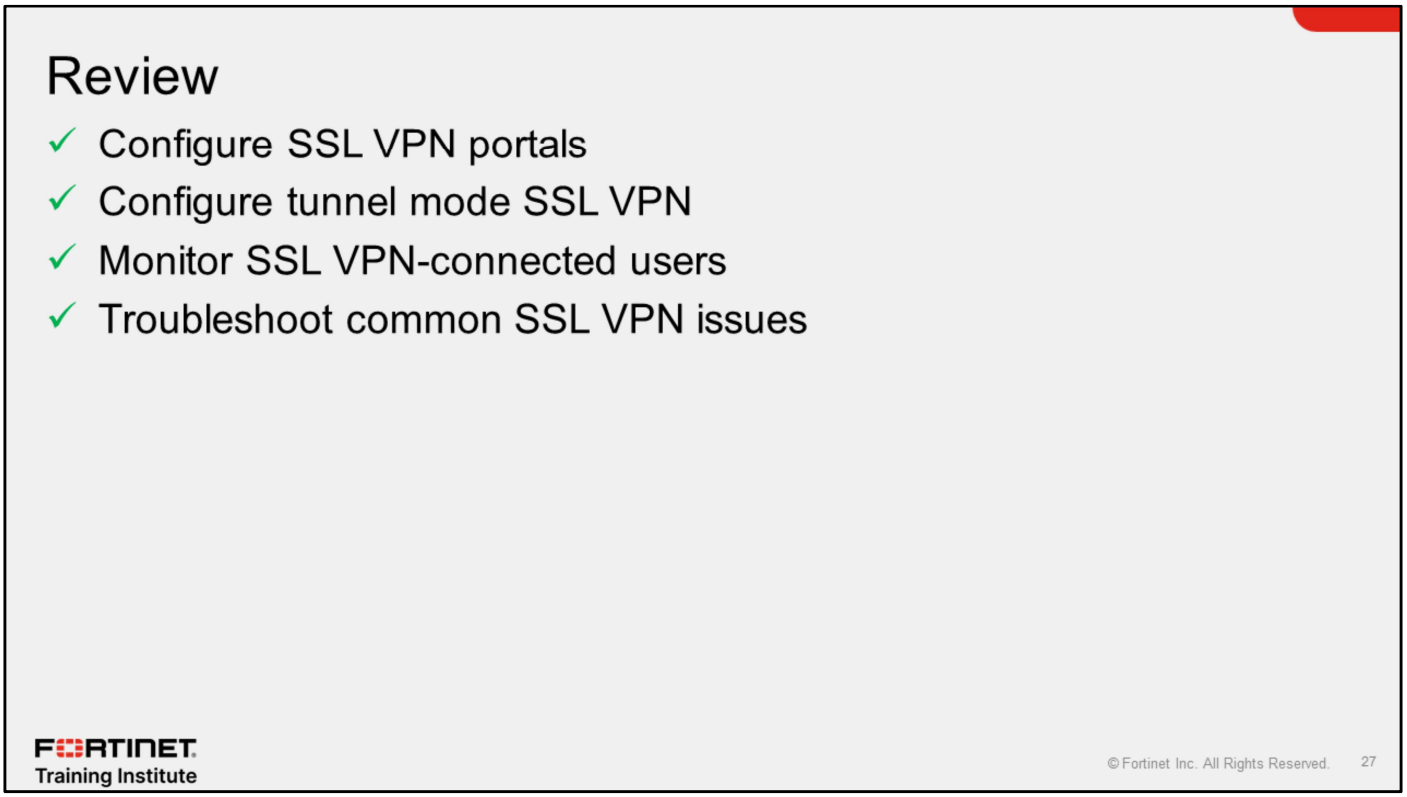
The command `diagnose debug application sslvpn` shows the entire list of debug messages for SSL VPN connections.

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

Knowledge Check

1. 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

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



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.