Deep Dive into

SSL VPN

in FortiGate

Table of Contents

SSL VPN At a Glance

What is SSL VPN?

An **SSL VPN** (Secure Sockets Layer Virtual Private Network) is a type of VPN that allows users to securely access a private network remotely over a standard web browser. Unlike traditional VPNs that typically use IPsec (Internet Protocol Security), SSL VPNs utilize the **SSL/TLS protocol** to encrypt traffic between the user's device and the network. This offers several advantages:

Key Features of SSL VPN:

1. **Remote Access:** SSL VPN is ideal for remote users (e.g., employees, contractors) who need secure access to company resources from anywhere using their web browser or a lightweight VPN client.
2. **Browser-Based Access**: Users can connect via a web browser without needing to install specialized VPN software. This makes it more accessible, especially for remote users.
3. **Encryption and Security**: SSL VPNs use SSL/TLS to create a secure, encrypted tunnel for data transmission. This ensures that sensitive data, like login credentials or personal information, is protected from potential threats during transit.
4. **Clientless** (in many cases): In most cases, SSL VPNs are "clientless," meaning they do not require a dedicated VPN client to be installed on the user's device. Users only need a browser that supports SSL/TLS, which is standard in most modern browsers.
5. **Secure Access to Specific Applications**: SSL VPNs often grant access to specific internal applications or resources, like webmail, file sharing, or an internal intranet, or internal websites, based on user roles and permissions rather than providing full network access like IPsec VPNs.
6. **User Authentication**: SSL VPNs often integrate with authentication mechanisms, such as username/password, tokens, or certificates, and can support multi-factor authentication (MFA) for enhanced security.

Use Cases:

- **Remote Work**: Employees accessing corporate resources securely from home or while traveling.
- **Mobile Users**: Users who need to connect securely using mobile devices without installing VPN clients.
- **Specific Resource Access**: Allowing access to particular services or applications instead of a full network connection.
- **BYOD (Bring Your Own Device)**: Users can securely connect to a private network using personal devices without the need to install complex software.

SSL VPNs have become popular due to their ease of use, enhanced security, and compatibility with modern web browsers.

Benefits of SSL VPN:

- **Ease of Use**: SSL VPNs are easy to set up and use, as they don't typically require complicated configurations or installations on the client side.
- **Security**: Since the traffic is encrypted with SSL/TLS, SSL VPN provides robust security, protecting against eavesdropping or data tampering.
- **Flexibility**: It works across multiple platforms and devices, including desktops, laptops, and mobile devices, making it convenient for remote workers.

Can we use SSL VPN for Site-To-Site connectivity?

No, **SSL VPN** is not typically used for **site-to-site connectivity**. Instead, SSL VPNs are mainly used for **remote access VPNs**, where individual users securely connect to a private network over the internet using a web browser or lightweight client.

For **site-to-site VPN** connectivity, which connects two or more entire networks (such as a branch office network to a headquarters network), organizations commonly use **IPsec VPNs (Internet Protocol Security VPNs)**. IPsec is designed to provide a secure tunnel between two networks, ensuring confidentiality, integrity, and authenticity of data transferred between them.

Differences:

- **SSL VPN** is mainly used for **remote access** by individual users connecting from various devices.
- **IPsec VPN** is preferred for **site-to-site** connections between two networks or offices because it is optimized for establishing and maintaining secure tunnels between routers or gateways at both locations.

Why IPsec for Site-to-Site VPN?

- **Encryption and Security**: IPsec provides strong encryption and security, making it well-suited for persistent connections between two sites.
- **Gateway-to-Gateway Connectivity**: Site-to-site VPNs require connectivity between routers or gateways, which IPsec is designed to handle.
- **Network-to-Network Traffic**: IPsec VPNs can efficiently manage the high volumes of traffic exchanged between two corporate networks.

In summary, SSL VPN is typically used for **remote user access**, while **IPsec VPN** is the standard choice for **site-to-site connectivity** between multiple networks.

Learning Objectives

After completing this section, you should be able to achieve the following objectives. 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.

- **Describe what SSL VPN is and its benefits.**
- **Describe how FortiGate SSL VPN works.**
- **Configure FortiGate SSL VPN Portals.**
- **Configure Tunnel mode SSL VPN.**
- **Monitor SSL VPN-connected users.**
- **Apply general best practices when using SSL VPN.**
- **Troubleshoot common SSL VPN issues.**

What is SSL/TLS?

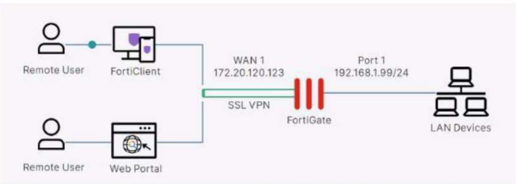
Secure Sockets Layer (SSL) is a protocol **for encrypting HTTP traffic**, such as connections between user devices and web servers. Websites that use SSL encryption have https:// in their URLs instead of http://.

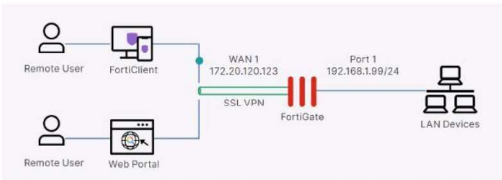
SSL was replaced several years ago by Transport Layer Security (TLS), but the term "SSL" is still in common use for referring to the protocol.

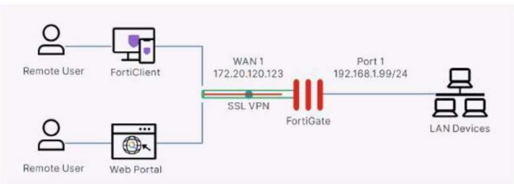
In addition to encrypting client-server communications in web browsing, SSL can also be used in VPNs.

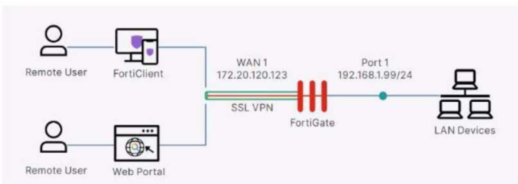
Secure Sockets Layer Virtual Private Network (SSL VPN) is a type of VPN that uses **SSL encryption** to:

- create a secure and encrypted connection **between a client device and a device acting as a VPN server**.
- Although SSL VPN is most commonly used to **grant remote workers access to their corporate networks**,
- it is also possible to configure it **between two FortiGate firewalls**.









Why use SSL VPN?

Many organizations opt to use SSL VPN for remote access over (instead of) the IPsec VPN. However, each technology has its pros and cons, so you should examine your scenario carefully to make the best choice.

These are some benefits of using SSL VPNs with FortiGate. It is important to note that some of these benefits apply only to specific configurations.

• **Use of common protocol**: SSL is used to encrypt HTTP traffic and, by default, uses port 443. This means that typically this traffic is not blocked by intermediate firewalls.

• **Flexibility**: Depending on the needs of the clients, they may only require a web browser to access a customized web portal. This is especially useful when dealing with mobile devices. However, the option of installing client VPN software is also available.

• **Granular access**: Administrators can easily restrict which resources the clients are allowed to access.

• **Integrity checks for Windows clients**: This security feature ensures that remote devices connecting to the VPN are compliant with the security policies of the organization. For example, it can check if the client has antivirus software installed and deny access if it doesn't.

• **Cost effective**: Unlike other vendors, no additional license is required to use SSL VPN. **The FortiClient VPN can also be made available for download at no cost from the SSL portal**. Additionally, the number of remote users supported is determined only by the FortiGate model.

How does SSL VPN work?
(SSL VPN Deployment Modes)

SSL VPNs are available in two modes:

Web Mode and **Tunnel Mode**.

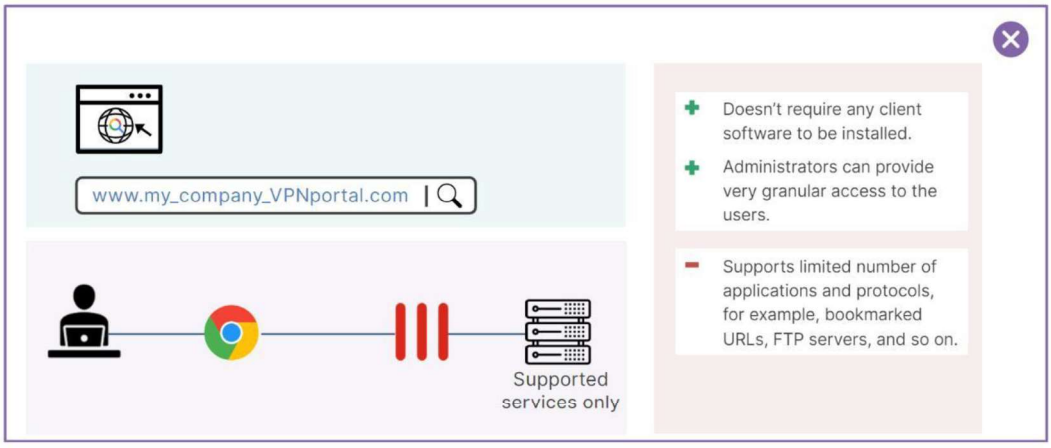
Based on your requirements, you can deploy an SSL VPN using one mode or both. Both can build an SSL VPN connection, but they don't support the same features.

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.

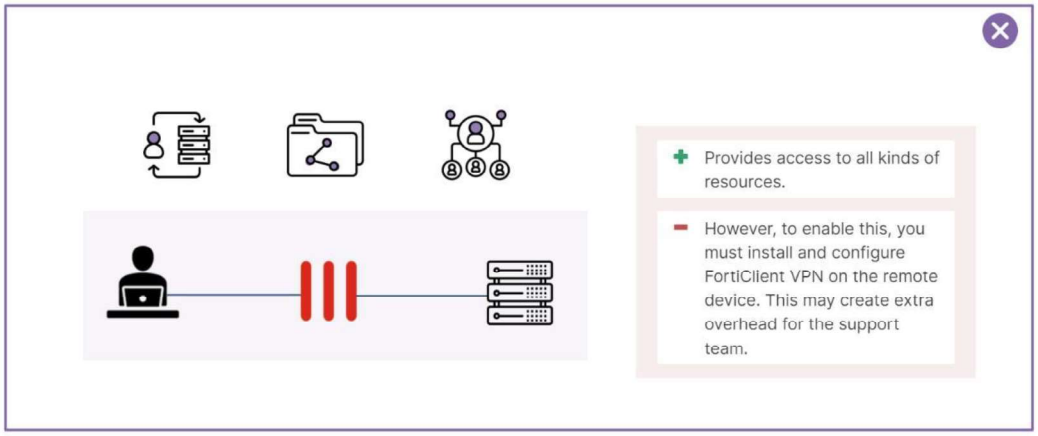
• **Web mode (Portal Mode)** provides **access to web-based applications** through a web browser. The user only needs to open the URL or IP address provided and log in to the web portal. It is important to mention that FortiGate functions as a reverse web proxy to allow access to applications that are not natively designed to be accessed through the web. This mode is best suited for users who need to access a limited set of resources, such as web-based applications, intranet sites, and email, among others. The main advantages of this mode are that it doesn't require any client software to be installed and administrators can provide very granular access to the users. On the downside, since all the access is through a web page, there is a limited number of applications and protocols supported. Typical access includes bookmarked URLs, FTP servers, Windows shares, and remote sessions to other systems using Telnet, SSH, VNC, or RDP.

- Requires only a web browser
- Supports a limited number of protocols: FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, Telnet, VNC, and Ping



• **Tunnel mode** provides **full network access to remote users** as if they were physically present on the corporate network. This mode is best suited for remote workers who need to access a wide range of services, including **client-server applications**, **file shares**, and **other typical network resources**. The ability to access all kinds of resources is the big advantage of this mode. However, to enable this, you must install and configure the **FortiClient VPN** on the remote device. This may create extra overhead for the support team when dealing with users who are not technically savvy and are trying to use their own devices.

- Accessed through a FortiClient
- Requires a virtual adapter on the client host



So, what are the differences between Web Mode and Tunnel Mode?

SSL VPN (Secure Sockets Layer Virtual Private Network) provides two primary modes of operation: **Web Mode** and **Tunnel Mode**. Here's a breakdown of the key differences between them:

1. SSL VPN Web Mode:

- **Functionality**: In Web Mode, the user accesses internal network resources through a web browser without requiring additional VPN client software. This mode is typically used to access web-based applications (e.g., internal websites, email portals, or file sharing) via an SSL-enabled connection.
- **Client Setup**: No need for dedicated VPN client software; a compatible web browser is sufficient.
- **Access**: Limited to web-based or browser-accessible services (HTTP, HTTPS, etc.).
- **Use Cases**: Ideal for quick, lightweight access to internal resources when only a browser is available (e.g., on public computers or in situations where the user cannot install VPN client software).
- **Network Integration**: The traffic is typically proxied through the VPN gateway, so the user does not have full access to the internal network.
- **Performance**: Usually faster for web applications since it doesn't need to encrypt and tunnel all traffic.

2. SSL VPN Tunnel Mode:

- **Functionality**: In Tunnel Mode, a dedicated VPN client is used to create a secure, encrypted tunnel between the user and the internal network. This allows access to all network resources (e.g., file servers, databases, remote desktops) as if the user were directly connected to the corporate network.
- **Client Setup**: Requires a VPN client installed on the user's device (usually provided by the VPN provider). This client handles encrypting the connection and routing all traffic through the tunnel.
- **Access**: Provides access to a wider range of services and applications (not just web-based).
- **Use Cases**: Suitable for users who require comprehensive access to the corporate network, such as remote workers needing to use various internal systems and applications.
- **Network Integration**: The user appears as if they are part of the internal network, with access to all the permitted internal services.
- **Performance**: Encrypting and tunneling all traffic may result in higher latency compared to Web Mode, especially for bandwidth-heavy applications.

Summary of Differences:

Feature	SSL VPN Web Mode	SSL VPN Tunnel Mode
Client Requirements	Web browser only	Dedicated VPN client software required
Access to Resources	Web-based resources only	Full access to all network resources
Use Cases	Quick, lightweight access to web apps	Comprehensive remote access to all apps
Network Integration	Limited, proxy-based access	Full network access as if on LAN
Performance	Typically faster for web apps	May be slower due to tunneling overhead

Each mode serves different use cases, with Web Mode offering easier, browser-based access, and Tunnel Mode providing more robust, full network access for remote users.

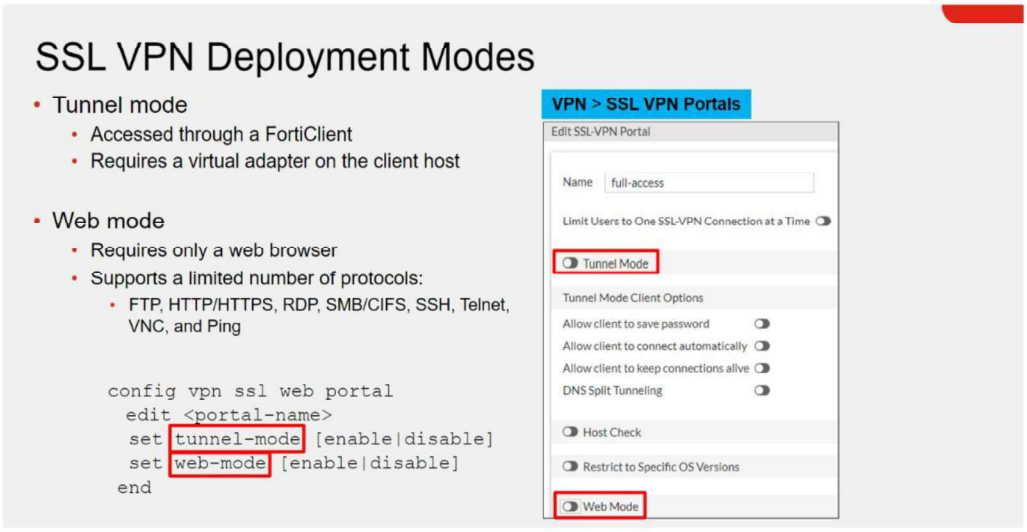
SSL VPN Web Mode can support **RDP (Remote Desktop Protocol)**, but it depends on the capabilities of the VPN gateway or firewall providing the SSL VPN service. In Web Mode, you typically access resources through a web browser. Some SSL VPN solutions provide **RDP access through a web portal**, allowing you to launch an RDP session from the browser without needing to install a full VPN client.

Here's how it works:

1. **RDP via Web Portal**: In Web Mode, many SSL VPN appliances or firewalls offer a web portal where users can access internal resources. From this portal, users can launch an RDP session directly within the browser or through a Java/HTML5-based RDP client. This is convenient as it does not require an RDP client installed on the local machine.
2. **Limitations**:
    - **Performance**: RDP over Web Mode may not perform as well as in Tunnel Mode because it depends on the quality of the web interface and the resources of the VPN appliance.
    - **Features**: The functionality of the RDP session might be limited compared to using a native RDP client. For example, certain advanced features like printer redirection or clipboard sharing might not work as well.
    - **Browser Compatibility**: Accessing RDP through Web Mode often relies on browser compatibility, and in some cases, users might need plugins or specific browsers for it to work properly.

Summary:

Yes, SSL VPN Web Mode can support RDP, but it usually depends on the specific VPN appliance or software. It is typically provided through a web-based interface, offering convenient access to remote desktops via a browser. For more seamless and robust RDP performance, however, **Tunnel Mode** with a dedicated VPN client is often preferred.



An Important Question

Can we use SSL VPN in Tunnel Mode for a Site-to-Site VPN?

Technically, it is possible to use **SSL VPN in Tunnel Mode** for a form of **Site-to-Site VPN**, but it is **not the standard or optimal approach**. Typically, Site-to-Site VPNs rely on **IPsec** because it is specifically designed for network-to-network connections. However, some VPN solutions might offer advanced configurations that allow the use of SSL VPN for Site-to-Site connections. Here's an explanation of why SSL VPN Tunnel Mode might be considered and the challenges involved:

1. How SSL VPN Tunnel Mode Could Work for Site-to-Site VPN:

- **Tunnel Mode** creates an encrypted tunnel between two endpoints, which can theoretically be used to connect two networks.
- If you set up an SSL VPN Tunnel Mode on both sides (between two gateways or routers), it could route traffic between the two sites, allowing devices on either network to communicate with each other.
- This could be configured using special VPN appliances that support such configurations.

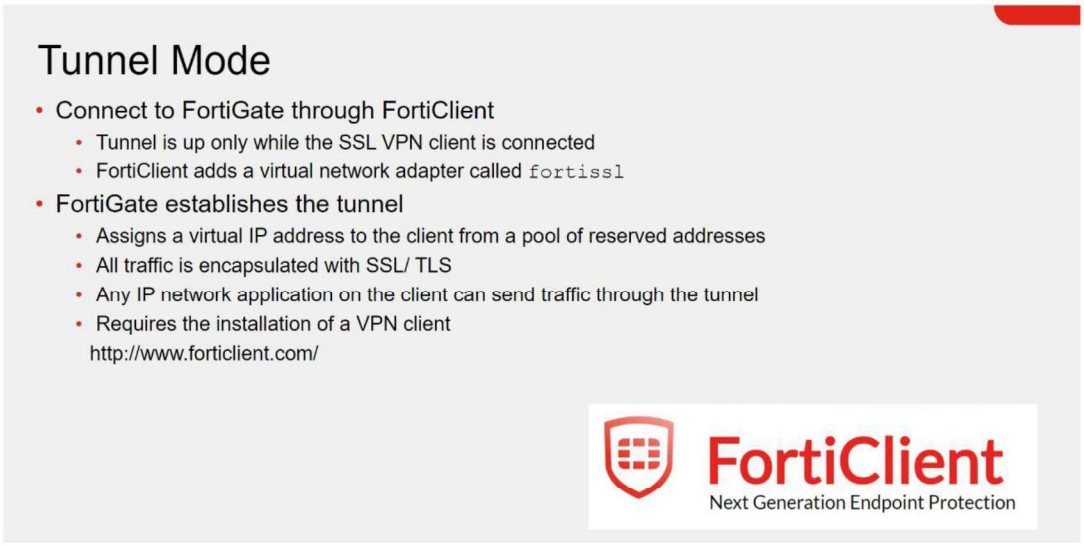
2. Challenges and Limitations:

- **Performance**: SSL VPN Tunnel Mode is not optimized for continuous, high-volume traffic typical in Site-to-Site VPN connections. SSL/TLS encryption tends to have more overhead than IPsec, which could lead to performance bottlenecks, especially for bandwidth-heavy applications.
- **Scalability**: SSL VPN is designed for individual user access. Scaling this to handle multiple devices on both sides of the site-to-site connection could be inefficient compared to IPsec, which is designed to manage such scenarios.
- **Complexity**: Configuring SSL VPN for Site-to-Site VPN can be more complex because it's not a typical use case for SSL VPNs. IPsec offers easier, standardized configuration options for Site-to-Site setups across most routers and firewalls.

3. When It Might Be Used:

- **Firewall Limitations**: In some cases, firewalls might block IPsec VPN traffic (protocols like ESP or AH). SSL VPN, using SSL/TLS over TCP or UDP, can bypass such restrictions.
- **NAT Traversal**: SSL VPN is often better at handling NAT (Network Address Translation) issues than IPsec because SSL/TLS is commonly used on ports like TCP 443, which are generally open in most networks.
- **Specific VPN Solutions**: Certain proprietary VPN solutions may allow SSL VPN Tunnel Mode to be used for Site-to-Site configurations. These are typically vendor-specific implementations.

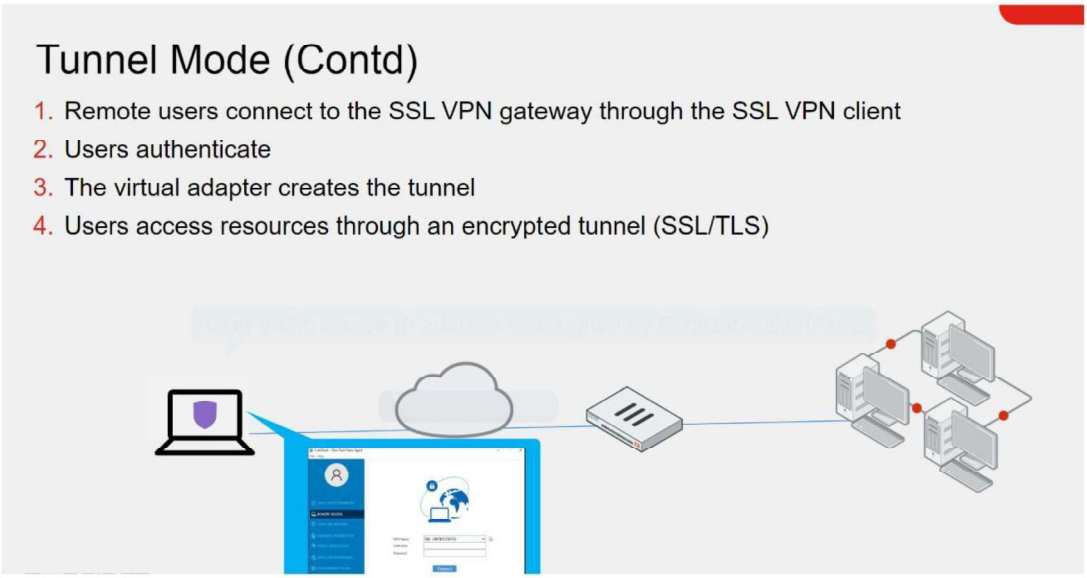
Tunnel Mode



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.

How does tunnel mode work?



1. Users connect to FortiGate through FortiClient.

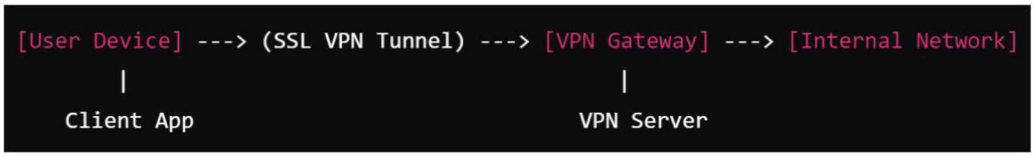
2. Users provide credentials to successfully authenticate.

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, deencapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

Here's a breakdown of how SSL VPN tunnel mode works:



1. Establishing the Connection

The SSL VPN tunnel mode connection is initiated by the remote user (client) connecting to the VPN server (gateway) via a web browser or dedicated VPN client software. The process typically proceeds as follows:

- **Client Authentication:** The client authenticates with the VPN server using a username, password, and possibly additional methods like multi-factor authentication (MFA) or certificates.
- **SSL/TLS Handshake:** Once authenticated, the SSL/TLS handshake begins. During this handshake:
  - The client and server agree on encryption methods (cipher suites).
  - The server sends its digital certificate for authentication.
  - Encryption keys are negotiated using a secure key exchange process (e.g., Diffie-Hellman).

This handshake ensures that a secure, encrypted communication channel is established between the client and server using SSL/TLS.

2. Creating the Tunnel

After a secure connection is established, an SSL VPN tunnel is created. The key points of tunnel mode include:

- **Full Traffic Encryption:** All data sent from the client to the VPN server is encrypted using the agreed-upon cipher suite. This includes not only the application data but also protocol information (such as IP packets) being transmitted.
- **Encapsulation of Traffic:** In tunnel mode, the entire IP packet (including headers and payloads) is encapsulated within the SSL VPN tunnel. This means that multiple types of traffic (e.g., HTTP, SSH, RDP, email) can be routed through the tunnel securely.
  - The client acts as if it's on the same network as the internal network, and any data it sends is encapsulated in SSL/TLS packets.
- **IP Address Allocation:** The client typically gets an IP address from the VPN server, making it appear as if it is part of the internal network. This allows the client to access resources within the private network (such as file servers, printers, internal web servers, etc.).

3. Traffic Flow in SSL VPN Tunnel Mode

Once the SSL VPN tunnel is established, all data flows through this encrypted tunnel, ensuring secure communication between the client and the VPN gateway. The following steps occur as traffic flows:

- **Client Sends Traffic:** The user's device generates traffic (e.g., a request to access an internal web server or send an email). The VPN client software encapsulates the traffic in SSL/TLS-encrypted packets.
- **Encryption and Transmission:** The encapsulated, encrypted traffic is sent over the Internet to the VPN gateway.
- **Decryption at Gateway:** The VPN gateway decrypts the traffic and forwards it to the internal network. To internal systems, this traffic appears to come from a device on the internal network (with the assigned internal IP address).
- **Return Traffic:** Responses from internal network resources (e.g., web server responses) are sent back through the VPN gateway. The VPN gateway encrypts these responses using SSL/TLS and forwards them to the client.
- **Decryption at Client:** The VPN client receives the encrypted data, decrypts it, and forwards the response to the appropriate application on the user's device.

Security Features of SSL VPN Tunnel Mode

SSL VPN tunnel mode is highly secure and includes several key security features:

- **Strong Encryption:** The data exchanged between the client and server is encrypted using SSL/TLS protocols, protecting against eavesdropping, man-in-the-middle attacks, and other threats.
- **Authentication:** SSL VPNs often require multi-factor authentication (MFA) to ensure that only authorized users can access the internal network.
- **Data Integrity:** SSL VPN ensures data integrity using hashing techniques like HMAC (Hash-based Message Authentication Code) to verify that data is not altered in transit.
- **Endpoint Security:** Some SSL VPN implementations include endpoint security checks (e.g., verifying antivirus or firewall status) to ensure that the client device meets security requirements before connecting.

Tunnel Mode Types

When discussing SSL VPN connections, **FortiGate as a client** and **User as a client** refer to different roles and configurations in the VPN setup. Here's a breakdown of the key differences between these two:

1. FortiGate as a Client (Gateway-to-Gateway SSL VPN):

- **Purpose**: This refers to a scenario where the **FortiGate device itself** acts as an SSL VPN client, connecting to another VPN server or gateway. It is typically used in **site-to-site VPN** setups, where one FortiGate (at a branch office) connects to another VPN server (at the headquarters).
- **Use Case**: Mainly for **Site-to-Site** VPNs, connecting entire networks securely over the internet.
- **Traffic**: When FortiGate is the client, it routes traffic from the entire local network (behind the FortiGate) through the VPN tunnel to the remote network. Devices behind the FortiGate don't need to individually establish the VPN connection.
- **Connection Scope**: The entire **network behind the FortiGate** can access the remote network through the VPN.
- **Configuration**: Requires configuring the FortiGate as an SSL VPN client, specifying the remote server details, and setting routing and policies to ensure traffic is properly forwarded.
- **VPN Type**: Mostly used in gateway-to-gateway (site-to-site) VPN configurations.

2. User as a Client (Remote Access SSL VPN):

- **Purpose**: This refers to individual **users** connecting to the FortiGate (acting as the VPN server) using SSL VPN to securely access internal network resources. Each user establishes their own SSL VPN connection.
- **Use Case**: Mainly for **Remote Access** VPN, where users (employees, contractors, etc.) connect to the corporate network from external locations (e.g., from home or while traveling).
- **Traffic**: The traffic is specific to the user's device, not the entire network. Only the user's device that initiates the SSL VPN connection can access the internal network.
- **Connection Scope**: The **individual user's device** gets access to the network, allowing them to use resources such as internal web applications, file servers, or remote desktops (RDP).
- **Configuration**: The user installs a VPN client (like FortiClient) or uses a web browser to initiate the SSL VPN connection to the FortiGate device, and the connection is authenticated via user credentials.
- **VPN Type**: Used in user-to-network (remote access) VPN setups.

Key Differences:

Aspect	FortiGate as a Client	User as a Client
Purpose	Site-to-site VPN, connecting two networks	Remote access VPN, providing secure access to individual users
Role	FortiGate device itself acts as the client	Individual users act as the clients
Traffic Scope	Routes traffic for the entire network behind the FortiGate	Routes traffic only for the user's device
Connection Scope	Entire network gains access to remote network	Only the user's device gains access to the internal network
Use Case	Site-to-site (branch office to HQ) VPN	Remote access for users (e.g., work-from-home scenarios)
Configuration	Configured on the FortiGate to connect to a VPN server	Configured on the user's device using VPN client or web browser
VPN Type	Gateway-to-Gateway SSL VPN	User-to-Network SSL VPN

Summary:

- **FortiGate as a Client** is used to connect entire networks (site-to-site) where the FortiGate device itself handles the VPN connection.
- **User as a Client** is used to connect individual users to the network for remote access (remote workers accessing internal resources).

Both configurations serve different purposes, with **FortiGate as a client** focusing on network-to-network connections, and **User as a client** enabling secure access for individual users.

Tunnel Mode – FortiGate as Client

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

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.

Tunnel Mode—FortiGate as Client (Contd)

- Advantages:
  - Any IP network application on the user machines connected 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
- Disadvantages:
  - Requires correct CA certificate on SSL VPN server FortiGate
  - SSL VPN client FortiGate user uses PSK and PKI client certificate to authenticate

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** (Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely).
- **UDP ports 500 or 4500 being blocked** (Traffic on UDP port 500 is used for the start of all IKE negotiations between VPN peers. This is true of all IPSec platforms. In some cases, UDP port 4500 is also used).
- **Fragments being dropped**, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.

Let me simplify and explain each part of the statement:

1. IP-level Connectivity in Tunnel Mode

- **Tunnel Mode**: In SSL VPN tunnel mode, the entire IP traffic (including the IP headers and payload) is encrypted and sent through the VPN tunnel. This means that the client behaves as if it is part of the remote network.
- **IP-level Connectivity**: The devices at both ends of the SSL VPN can communicate with each other at the IP level, meaning they can exchange data packets just like computers on the same local network, even though they are in different physical locations.

2. Hub-and-Spoke Topology with FortiGate

- **Hub-and-Spoke**: This refers to a network design where a central device (the **hub**) connects to multiple remote devices (the **spokes**). The spokes don't connect directly to each other but communicate through the hub. In this case, the **FortiGate device** can serve as both the hub (central location) and the spokes (remote locations).
  - **FortiGate as Hub**: The central device that connects all the remote spokes.
  - **FortiGate as Spokes**: The remote devices that connect back to the hub.

  This design can be useful for creating secure communication between branch offices (spokes) through a central office (hub).

3. Benefits of SSL VPN in Tunnel Mode vs IPsec VPN

The next section explains why SSL VPN (in tunnel mode) can be a better choice than IPsec VPN (which relies on certain protocols and ports) in some cases. Here are the issues that SSL VPN helps avoid:

A. ESP Packets Being Blocked

- **ESP (Encapsulating Security Payload)** is a protocol used by IPsec VPNs to provide encryption and authentication of data packets.
- **Issue**: Some intermediate devices (like firewalls or ISPs) may block ESP packets. This would prevent an IPsec VPN from working because it relies on ESP for security.
- **SSL VPN Advantage**: SSL VPN does not rely on ESP. Instead, it uses standard SSL/TLS encryption (just like HTTPS websites), which is less likely to be blocked by intermediate devices.

B. UDP Ports 500 and 4500 Being Blocked

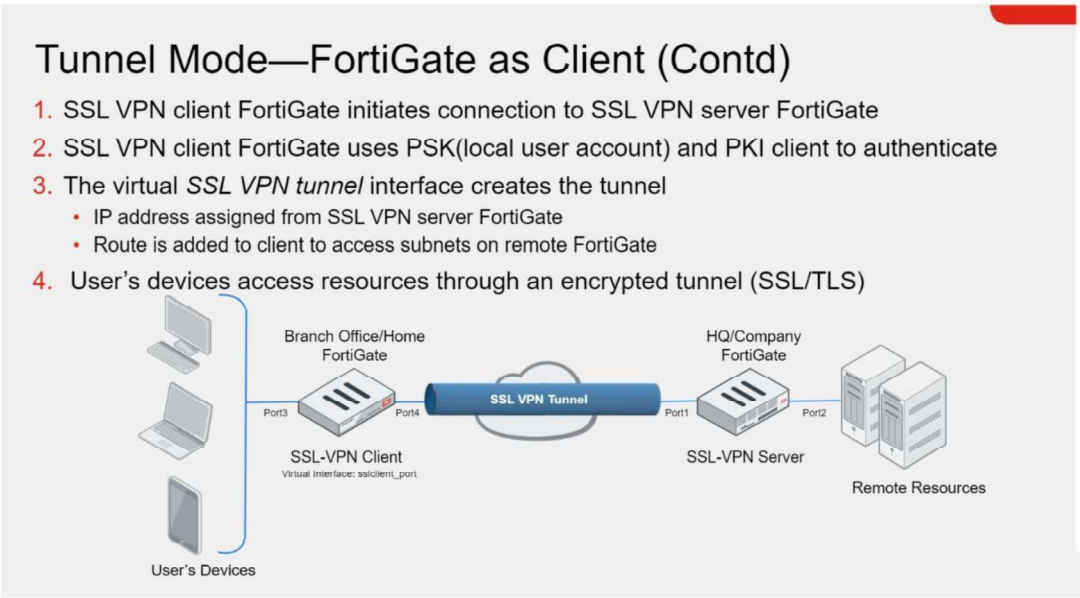
- **UDP Port 500**: Used by IPsec VPNs for the Internet Key Exchange (IKE) protocol, which is necessary to establish a secure VPN tunnel.
- **UDP Port 4500**: Sometimes used when the network uses Network Address Translation (NAT). It is also part of the IKE protocol for IPsec VPNs.
- **Issue**: If these UDP ports (500 and 4500) are blocked by intermediate devices like firewalls, the IPsec VPN connection cannot be established.
- **SSL VPN Advantage**: SSL VPN uses TCP port 443 (the same port used for HTTPS traffic). Port 443 is rarely blocked because it is needed for regular web browsing. This makes SSL VPN more reliable in environments where specific ports are blocked.

C. Fragmentation and Dropped Packets

- **Fragmentation**: When large data packets are broken into smaller fragments to be transmitted across the network.
- **Issue**: If large packets (like those containing large certificates during IKE negotiation) are fragmented, some network devices may drop the fragments. This can cause the VPN connection to fail, especially if the peer device does not support IKE fragmentation.
- **SSL VPN Advantage**: Since SSL VPN operates over **TCP** (rather than UDP like IPsec), it handles packet fragmentation more reliably. TCP ensures that packets are reassembled correctly, so there is less chance of fragmentation issues disrupting the VPN.

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.



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

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 (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 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, deencapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

SSL VPN packet format

In **SSL VPN tunnel mode**, the original packet (which could be a TCP, UDP, or other protocol data packet) is encapsulated and encrypted within SSL/TLS to secure the traffic over the VPN. Here's a detailed breakdown of all the fields added to the original packet as it traverses through the SSL VPN tunnel.

Overview of SSL VPN Encapsulation

1. The original packet (which can be IP, TCP/UDP, etc.) is encapsulated inside an SSL/TLS packet.
2. The SSL/TLS layer encrypts the data, and the encrypted packet is then sent over a transport protocol like TCP.
3. Additional headers are added at each stage to enable the secure transmission of the packet.

Detailed Structure: SSL VPN Tunnel Packet Format

Here is a step-by-step breakdown of the **fields added** to the original packet in SSL VPN:

---

1. Original IP Packet

This is the original packet that is generated by the client application or operating system before any encryption or encapsulation. It typically consists of:

- **Original IP Header (20 bytes)**: Contains source and destination IP addresses, protocol type (e.g., TCP, UDP), etc.
- **Transport Layer Header (e.g., TCP/UDP) (20 bytes for TCP)**: Contains information like source and destination ports, sequence numbers, etc.
- **Application Layer Data (variable size)**: The actual data (payload) being transmitted, such as HTTP, email, or other application data.

---

2. SSL/TLS Record Layer

Once the SSL VPN tunnel is established, the original packet is encapsulated inside an **SSL/TLS record**. The SSL/TLS layer encrypts the original packet and adds headers to ensure secure transmission. The main components added at this stage are:

- **Content Type (1 byte)**: Indicates the type of SSL/TLS record (e.g., handshake, application data).
  - Typical values:
    - 20: ChangeCipherSpec
    - 21: Alert
    - 22: Handshake
    - 23: Application data (most common for VPN data traffic).
- **Version (2 bytes)**: Indicates the SSL/TLS protocol version (e.g., TLS 1.2 is 0x0303).
- **Length (2 bytes)**: Specifies the length of the encrypted payload inside the SSL/TLS record.

- **Encrypted Payload (variable size)**: The original IP packet is encrypted at this stage using symmetric encryption (e.g., AES or ChaCha20). The length depends on the size of the original packet.
- **MAC (Message Authentication Code) (variable size)**: A cryptographic checksum added to ensure the integrity of the data. If the data is tampered with, the MAC will not match, and the packet will be rejected.

---

3. Transport Layer (Typically TCP)

Since SSL VPN relies on **SSL/TLS**, the encapsulated data is transmitted over **TCP**. **This is one of the main differences between SSL VPN and IPsec VPN, where SSL VPN uses TCP (typically port 443) for transmission, while IPsec often uses UDP.**

- **TCP Header (20 bytes for IPv4)**: The original packet, now encrypted and encapsulated in the SSL/TLS layer, is transmitted over TCP.
  - Important fields in the TCP header include:
    - **Source and Destination Port**: Typically port 443 for SSL VPN.
    - **Sequence and Acknowledgment Numbers**: For ensuring reliable transmission.

⇨ **Detail:**

- For the encrypted traffic to travel across the internet securely, an **outer TCP header** is added to carry the encrypted SSL/TLS data.
- This **new TCP header** is part of the TCP session between the SSL VPN client and the VPN server.
  - It is used to manage the **encrypted traffic** between the client and the VPN server.
  - Typically, this session uses **TCP port 443** on the VPN server for SSL/TLS traffic.

---

4. IP Header

The encrypted data (including the original packet and SSL/TLS encapsulation) is then wrapped in an **outer IP header** for routing over the internet.

- **Outer IP Header (20 bytes for IPv4)**: The outer IP header contains the source IP address (the client) and the destination IP address (the VPN server). The inner original IP header is already encrypted inside the SSL/TLS payload.

Summary of Fields Added to the Original Packet

When an original packet is encapsulated and sent through an SSL VPN tunnel, the following fields are added:

1. **SSL/TLS Record Layer**:
   - **Content Type (1 byte)**
   - **Version (2 bytes)**
   - **Length (2 bytes)**
   - **Encrypted Payload (variable size)**: Contains the original IP packet.
   - **MAC (Message Authentication Code) (variable size)**
2. **Outer TCP Header (20 bytes)**: The encrypted SSL/TLS packet is transmitted over TCP.
   - **Source and Destination Ports**
   - **Sequence and Acknowledgment Numbers**
3. **Outer IP Header (20 bytes)**: Wraps the entire packet for routing over the internet.
   - **Source and Destination IP addresses**

Example:

Let's say the original packet is HTTP traffic between a client and a web server on the internal network (e.g., 192.168.1.100 is the internal web server).

- **Original Packet**: This contains:
  - **Original IP header**: Source IP: 10.0.0.2 (client), Destination IP: 192.168.1.100 (internal web server).
  - **Original TCP header**: Source port: 50000, Destination port: 80 (HTTP).
  - **Original payload**: The HTTP data.
- **SSL VPN Encapsulation**:
  - The **original packet** (including its headers and payload) is **encrypted** and encapsulated in an SSL/TLS record.
  - A **new TCP header** is added, which is part of the **SSL VPN connection** between the client and the VPN server. This header contains:
    - **Source port**: Random port on the client.
    - **Destination port**: Typically, 443 on the VPN server (since SSL VPN traffic usually travels over HTTPS).
- **Outer IP header**: The packet is routed over the internet, with the client's public IP and the VPN server's IP as the source and destination, respectively.

Final Packet (on the wire):

```
[Outer IP Header (client IP, VPN server IP)]
    -> [New TCP Header (source port, port 443)]
        -> [SSL/TLS Record Layer]
            -> [Encrypted Original IP Packet (with original TCP header and payload)]
```

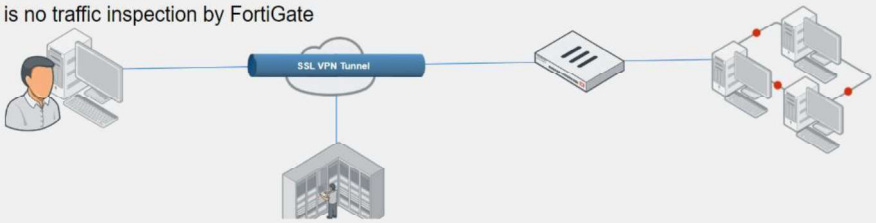
Summary:

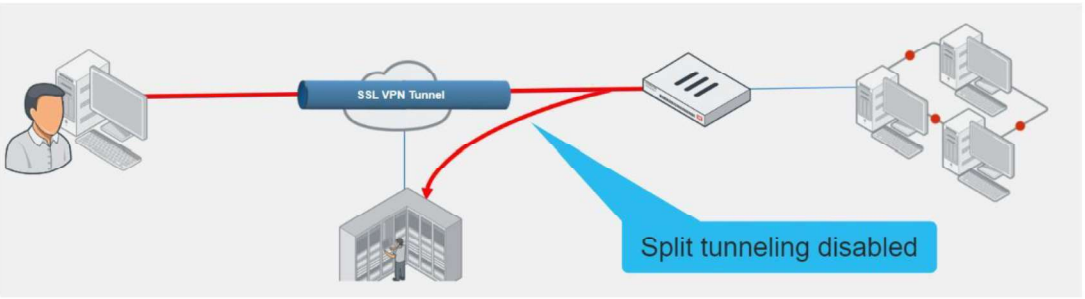
- The **TCP header you see** in the SSL VPN packet is the **new TCP header** used for the VPN transport, not the one from the original packet.
- The **original TCP header** is **inside** the encrypted SSL/TLS payload, along with the original packet.

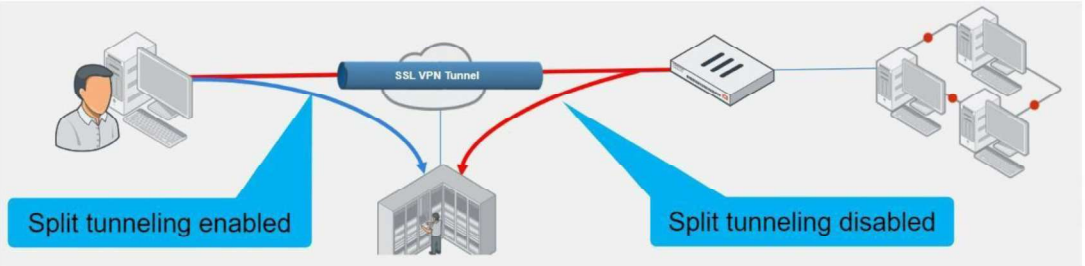
Tunnel Mode—Split Tunneling

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







Tunnel mode also supports split tunneling.

There are two implementaions:

1- **Disabled Split Tunneling**
2- **Enabled Split Tunneling**

Without (Disabled) 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.

Advantage:

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.

Disdvantage:

- 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.**

Let me break down the concepts step by step to help you better understand the topic regarding **SSL VPN without split tunneling** in a **FortiGate (client) to FortiGate (server) setup**.

1. Default Route Creation in SSL VPN (Without Split Tunneling)

When an SSL VPN connection is established **without split tunneling**, all traffic from the **FortiGate client** is routed through the SSL VPN tunnel to the **FortiGate server**. This means that even internet traffic, which would normally go directly to the internet from the client's local network, is now routed through the VPN tunnel.

- **Default Route**: A default route is a catch-all route used when no specific route to a destination is available in the routing table. In networking, a default route is often configured as "0.0.0.0/0" which matches all destinations.
- **ECMP (Equal-Cost Multi-Path)**: If multiple default routes exist (e.g., a regular internet route and a route through the VPN tunnel), **ECMP** allows traffic to be distributed across multiple routes with equal "cost" (i.e., the same metric or distance).

In the **FortiGate SSL VPN client** setup, when the VPN connection is established:

- A **new default route** is dynamically created to route all traffic through the VPN tunnel.
- This new default route is **added** to the client's existing routing table, possibly alongside the original default route (which may route traffic directly to the internet).

If both default routes (VPN and non-VPN) have equal distances (costs), ECMP will kick in, distributing traffic between the two routes. However, to control how traffic is routed, you can adjust the **distance** and **priority** of these routes.

2. Options for Routing Configuration

Now, let's focus on the **two options** available for configuring how traffic is routed when multiple default routes are present:

Option 1: Make all traffic default to the SSL VPN server (Preferred Route)

- **Goal**: You want **all traffic** (including internet traffic) to go through the SSL VPN tunnel, meaning the VPN route should be preferred over any other routes on the SSL VPN client (FortiGate).
- **Solution**: To ensure this, you need to **set a lower distance** (a smaller numerical value) for the default route that is learned from the SSL VPN server. So, only the route with the lowest AD remains in RIB.
- **How it works**:
  - Routing decisions are made based on the **distance** (or metric) of each route. The route with the **lower distance** is preferred.
  - By setting a lower distance for the route learned from the SSL VPN server, you make sure that the **VPN route** is used for all traffic, and traffic doesn't accidentally go through the regular internet route.
- **Route to the VPN server**: However, to still be able to reach the VPN server's **listening interface** (the interface that handles the VPN traffic), the FortiGate client needs a separate route specifically for the VPN server's IP address (outside the tunnel), so it knows how to reach it.

Option 2: Include Both Routes but Prioritize the VPN Route

- **Goal**: You want to include **both default routes** in the routing table, but make sure the **route learned from the SSL VPN server** takes priority.
- **Solution**:
  - Similar to Option 1, you can **set a lower distance** for the route learned from the SSL VPN server. If the distance is already as low as possible (e.g., zero), then you should **increase the priority** of the original default route (the non-VPN route).
- **How it works**:
  - The **distance** determines the preferred route when multiple routes exist. The route with the lowest distance is preferred.
  - If both routes have the same distance (e.g., zero), the **priority** comes into play. Increasing the priority on the non-VPN default route makes sure the VPN route is prioritized.
  - By adjusting the **distance** and **priority**, you can control which route is preferred without completely removing the other default route from the routing table. The SSL VPN route is prioritized for most traffic, but the client still has a fallback route available if needed.

Simplified Breakdown of the Key Concepts:

1. **Default Route**: This is the route that handles all traffic when no other specific route exists.
2. **ECMP**: If multiple routes exist (e.g., a regular route to the internet and a VPN route), traffic is distributed equally unless you control it by setting **distance** or **priority**.
3. **Option 1** (Route all traffic through the VPN):
   - Set a **lower distance** for the VPN route (learned from the server) so all traffic goes through the VPN tunnel by default.
   - Ensure there's still a specific route to reach the VPN server itself.
4. **Option 2** (Include both routes but prefer the VPN):
   - Set a **lower distance** for the VPN route, so it's preferred over the local route.
   - If the VPN route distance is already low, increase the **priority** of the regular route (non-VPN), allowing the VPN route to take precedence.

Example:

- **Current Situation**: You have a FortiGate client with two routes:
  - Route 1 (regular internet route): Distance = 10, Priority = 5
  - Route 2 (SSL VPN route): Distance = 10, Priority = 5
- **Action for Option 1**:
  - Set the **SSL VPN route's distance to 5**, making it the preferred route. This way, all traffic defaults to the VPN.
- **Action for Option 2**:
  - If the **SSL VPN route's distance** is already **5**, increase the **priority of the regular internet route** (e.g., Priority = 6), making sure the SSL VPN route takes priority.

Summary:

- When using **SSL VPN without split tunneling**, the VPN client adds a default route through the VPN tunnel.
- You can control how traffic is routed by adjusting the **distance** (metric) and **priority** of the routes:
  - **Lower distance** = more preferred.
  - **Higher priority** = less preferred if distances are equal.
- You have two main options:
  - **Make the VPN route the preferred route** (and route all traffic through the VPN).
  - **Include both routes** but ensure the **VPN route is preferred** by adjusting distance or priority.

Example Scenario Without Split Tunneling:

1. **Client Device** (user's laptop) connects to the FortiGate SSL VPN.
    - Internal traffic (e.g., accessing a file server at 10.0.0.1) goes through the VPN.
    - General internet traffic (e.g., browsing www.google.com) also goes through the VPN.
2. **FortiGate VPN Server** routes:
    - Internal traffic directly to the internal network.
    - Internet traffic from the client to the internet, enforcing corporate security policies along the way (e.g., web filtering, traffic logging, etc.).

Example Configuration for Disabling Split Tunneling on FortiGate:

To **disable split tunneling**, the FortiGate SSL VPN configuration should be set to ensure **all traffic** passes through the VPN tunnel. Here's how you can configure it in the FortiGate CLI:

```
config vpn ssl web portal
    edit "full-tunnel-portal"
        set tunnel-mode enable            # Enables tunnel mode (SSL VPN)
        set split-tunneling disable       # Disables split tunneling
    next
end
```

In this configuration:

- **`set split-tunneling disable`**ensures that **all traffic** is routed through the VPN tunnel, making it a full-tunnel VPN.

Full Tunneling Process (No Split Tunneling):

1. **Client connects to the VPN** using a FortiGate SSL VPN client.
2. **All traffic** (both to internal networks and the public internet) is routed through the encrypted VPN tunnel.
3. The **FortiGate server** handles all traffic:
    - Internal traffic is sent to the appropriate internal resources (e.g., file servers, databases).
    - Internet traffic is routed back out to the internet through the FortiGate's external interface.

With (Enabled) Split Tunneling

SSL VPN with split tunneling is a feature that allows VPN clients to **route some traffic through the VPN tunnel** while sending other traffic directly to the internet (or local network) without going through the VPN tunnel. This setup optimizes bandwidth usage and improves performance, as only specific traffic (such as internal corporate resources) is sent through the secure VPN connection, while the rest (like general internet browsing) uses the local internet connection.

How Split Tunneling Works in SSL VPN:

When a user connects to an SSL VPN, there are typically two main types of traffic:

1. **Internal traffic**: Traffic that needs to access resources inside the corporate network (e.g., file servers, databases, internal applications).
2. **Public internet traffic**: Traffic that does not need to go through the corporate network (e.g., browsing websites, watching videos).

Without Split Tunneling, all traffic—both internal and public—is sent through the VPN tunnel, including internet browsing traffic. This is called **full tunneling**. In **split tunneling**, the VPN client decides which traffic goes through the VPN tunnel (typically traffic for the corporate network) and which traffic bypasses the VPN (general internet traffic).

Key Features of SSL VPN with Split Tunneling:

1. **Selective Routing**:
   - Only traffic destined for specific IP ranges (such as internal corporate subnets) is routed through the VPN tunnel.
   - All other traffic (e.g., general internet browsing) is routed directly to the internet via the user's local internet connection.
2. **Local Internet Access**:
   - By allowing non-corporate traffic to bypass the VPN, users maintain full-speed access to local internet resources without the overhead of routing through the corporate network.
3. **Improved Performance**:
   - Reducing the amount of traffic going through the VPN tunnel can improve performance, especially for bandwidth-heavy applications like video streaming or large file downloads that don't need to go through the corporate network.
4. **Reduced Bandwidth Usage**:
   - For organizations, split tunneling reduces the bandwidth load on the VPN gateway and the internal network because only essential traffic passes through the VPN.

How Split Tunneling is Implemented in SSL VPN:

- **VPN Server Configuration**: The administrator of the VPN server (e.g., FortiGate, Cisco ASA) configures which **subnets** or **IP addresses** should be routed through the VPN tunnel. These are usually internal IP ranges (e.g., 10.0.0.0/24, 192.168.1.0/24).
- **VPN Client Configuration**: On the client side, the VPN software (such as FortiClient or Cisco AnyConnect) receives the configuration from the server and only routes traffic to the specified subnets through the VPN tunnel.

Example Scenario of SSL VPN with Split Tunneling:

1. **Corporate Network**:
   - IP Range: 10.0.0.0/24 (internal servers, databases, etc.)
2. **Client's Local Network**:
   - The user has a local internet connection (e.g., home Wi-Fi) and connects to a FortiGate SSL VPN server.
3. **With Split Tunneling**:
   - Traffic to IP addresses in the 10.0.0.0/24 subnet (corporate network) is sent through the VPN tunnel.
   - Traffic to public websites (e.g., www.google.com) or other general internet traffic bypasses the VPN and goes directly through the local internet connection.

Advantages of SSL VPN with Split Tunneling:

1. **Improved User Experience**:
   - Users can access the internet and local resources (such as printers) without routing that traffic through the VPN, which can slow things down.
2. **Optimized Bandwidth Usage**:
   - Reduces the load on the corporate VPN gateway, freeing up bandwidth for critical traffic and reducing latency for internal applications.
3. **Flexibility**:
   - Users can still access local network devices (like printers, local file servers) while connected to the VPN.
4. **Lower Latency for Non-Corporate Traffic**:
   - Since general internet traffic is sent directly to the internet, users experience faster browsing and internet speeds.

Disadvantages of SSL VPN with Split Tunneling:

1. **Potential Security Risk**:
   - Since non-corporate traffic bypasses the VPN, it is not encrypted or monitored by corporate security controls. This can increase the risk of malware or data breaches if the user accesses insecure websites while connected to the VPN.
2. **Reduced Centralized Control**:
   - IT departments may have less control over the client's internet traffic, making it harder to enforce security policies or monitor all internet traffic for threats.
3. **Compromised Devices**:
   - If the user's device is compromised (e.g., by malware on the internet), the infected traffic can reach both the local internet and corporate network through the split-tunnel configuration.

Use Cases for SSL VPN with Split Tunneling:

1. **Remote Workers**:
   - Employees working from home need access to corporate resources, but they also want to browse the internet without slowing down their connection by routing everything through the VPN.
2. **Mobile Users**:
   - Mobile workers or employees on the go may want to access internal corporate applications while still using local resources like public Wi-Fi or mobile data for regular internet use.
3. **Bandwidth-Intensive Applications**:
   - For users running bandwidth-heavy applications (e.g., video conferencing, streaming), split tunneling can help ensure that only essential corporate traffic is routed through the VPN, while the rest uses the local internet connection to prevent VPN overload.

Example Configuration on a FortiGate:

On a **FortiGate SSL VPN** server, split tunneling can be enabled in the following way:

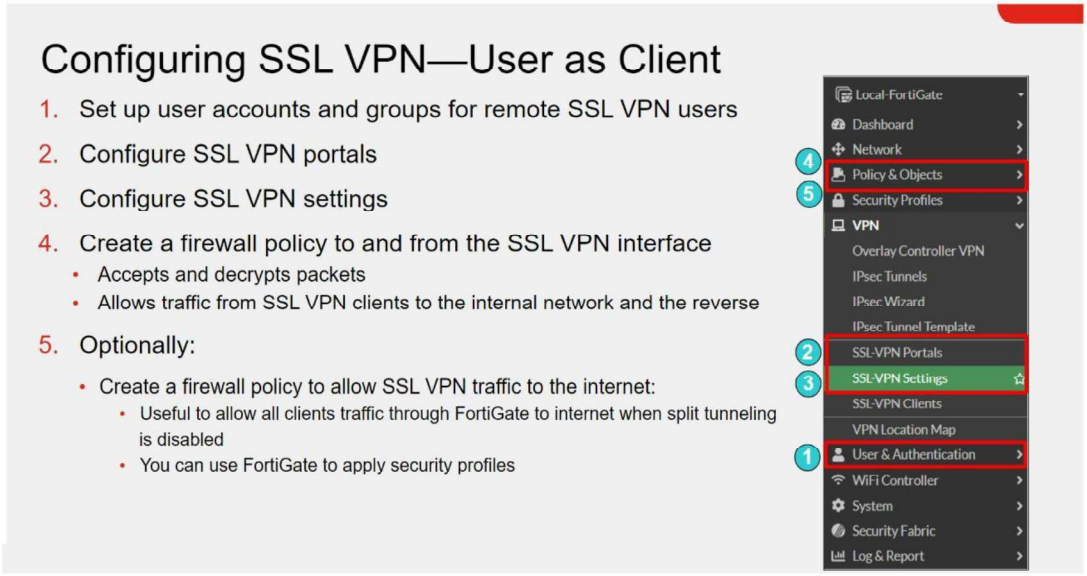
1. **Define the Internal Subnets**: Specify the internal subnets that should be routed through the VPN (e.g., 10.0.0.0/24).
2. **Enable Split Tunneling**: Configure the SSL VPN portal to enable split tunneling and push the defined internal routes to the client.

FortiGate CLI example:

```
config vpn ssl web portal
    edit "split-tunnel-portal"
        set split-tunneling enable
        set tunnel-mode enable
        set ipv4-split-include "10.0.0.0/24"  # Internal subnet
    next
end
```

Configuring SSL VPN – User as Client

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.



1 Set up user accounts and groups for remote SSL VPN users

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).

Create a User Account

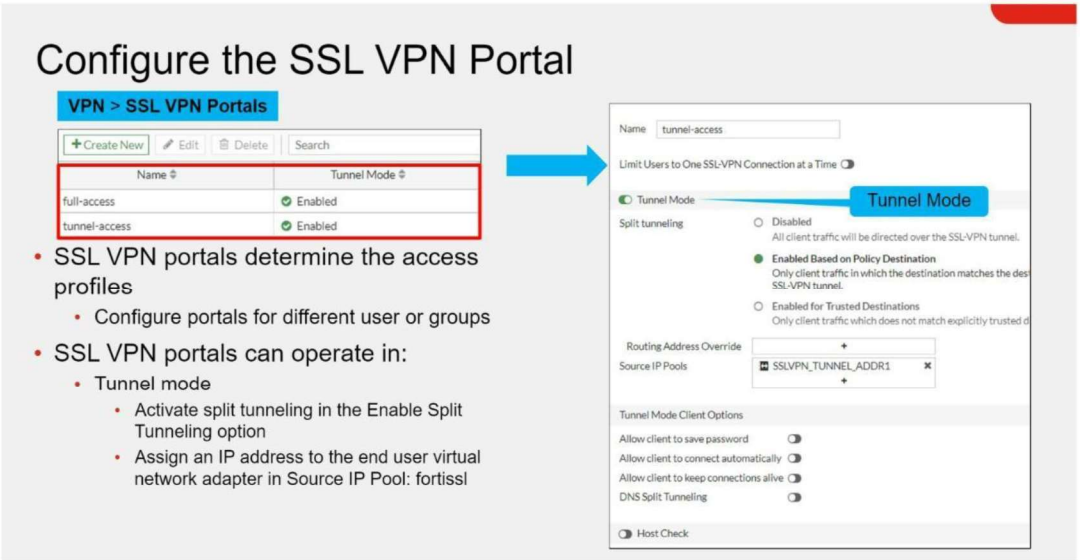
- Go to **User & Authentication > User Definition**.
- Click **Create New > User**.
- Provide a username and password that the user will use to authenticate to the VPN.
- (Optional) Set the user to expire after a specific time if needed for temporary access.

Create a User Group

- Go to **User & Authentication > User Groups**.
- Click **Create New**.
- Name the group (e.g., `SSLVPN_Users`).
- Add the user you just created to this group. This group will be assigned to SSL VPN later.

2 Configure SSL VPN portals

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. (**VPN > SSL VPN Portal**)

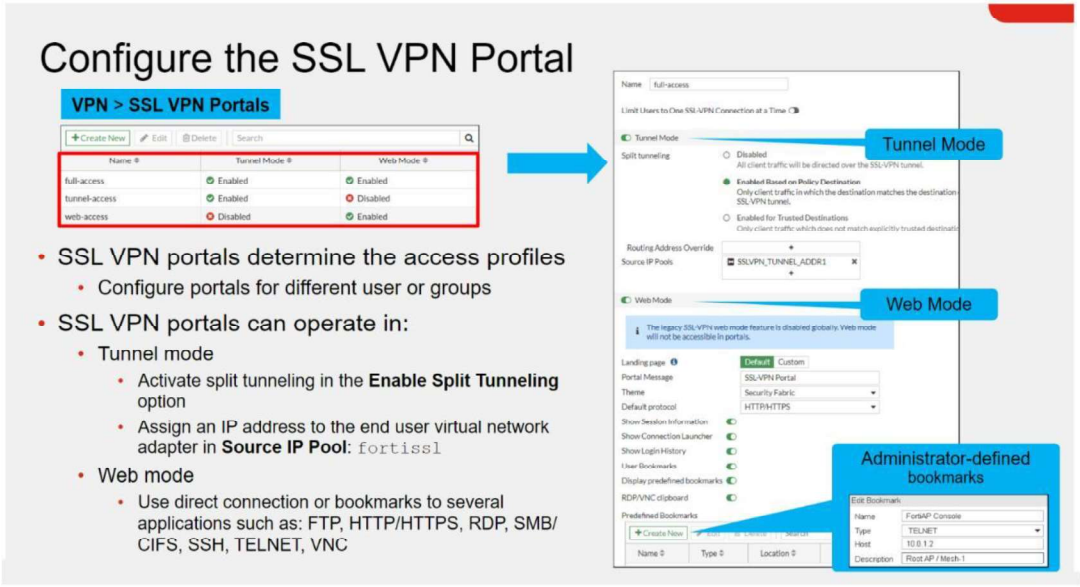


Understanding Portal Types: SSL VPN portals determine the access profiles

You can either edit the existing portals (e.g., full-access, tunnel-access, or web-access) or create a new portal if you need custom behavior.

- **Full Access**: Provides the client with complete access to the network resources. Useful for employees who need to connect to internal services remotely.
- **Tunnel Mode**: Provides access to internal resources via the VPN but can restrict access to specific subnets or services.
- **Web Access**: Limits access to web-based applications. Ideal for environments where users only

Tunnel Mode Configuration



Split Tunneling:

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** Only client traffic in which the destination matches the destination of the configured firewall polices will be directed over the SSL-VPN tunnel. Any other traffic (e.g., general web browsing) will bypass the VPN and go directly to the internet.
- **Enabled for Trusted Destination** Only client traffic which does not match explicitly trusted destination will be directed over the SSL-VPN tunnel.
  - This allows traffic that doesn't match your SSL VPN firewall policies but is destined for **trusted** networks to be routed through the VPN.
  - Trusted destinations could be defined as specific internal subnets or servers. Anything outside these destinations bypasses the VPN.

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. (Leave Routing Address Override undefined to use the destination in the respective firewall policies)

Source IP Pools:

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.

Web Mode Configuration

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.

Portal Message	Enter a message that appears at the top of the web portal screen (default = *SSL-VPN Portal*).
Theme	Select a color theme from the dropdown.
Show Session Information	Enable to display session information in the top banner of the web portal (username, amount of time logged in, and traffic statistics).
Show Connection Launcher	Enable to display the *Quick Connection* button.
Show Login History	Enable to display the user's login history (*History*).
User Bookmarks	Enable to allow users to add their own bookmarks (*New Bookmark*).
Rewrite Content IP/UI/	Enable contents rewrite for URIs containing `IP-address/ui/`.
RDP/VNC clipboard	Enable to support RDP/VPC clipboard functionality.
Predefined Bookmarks	Use the table to create and edit predefined bookmarks.

SSL VPN bookmarks

SSL VPN bookmarks are shortcuts or predefined links configured on an SSL VPN portal that provide users with easy access to internal resources (such as web applications, file servers, or remote desktops) through the SSL VPN. When users connect to the SSL VPN, they can access these bookmarks from the web portal, simplifying the process of reaching specific resources securely over the internet.

Key Features of SSL VPN Bookmarks

1. **Access to Internal Resources:**
   - Bookmarks allow users to access internal applications and services without needing direct access to the internal network. This is especially useful for accessing web-based applications, file shares, and remote desktops from outside the corporate network.

2. **Types of SSL VPN Bookmarks:**
   - **Web Bookmark:** Allows access to web-based applications (HTTP/HTTPS). It functions like a web link, where clicking the bookmark opens the application in a new browser tab.
   - **RDP Bookmark:** Provides access to remote desktops using the Remote Desktop Protocol (RDP). This is useful for connecting to Windows servers or workstations remotely.
   - **SSH/Telnet Bookmark:** Allows users to establish secure shell (SSH) or Telnet connections to remote devices such as routers, switches, or Linux servers.
   - **FTP/SFTP Bookmark:** Enables access to file transfer services over FTP or SFTP, allowing users to transfer files securely.

3. **Ease of Use:**
   - By using bookmarks, users don't need to remember the internal IP addresses or URLs of resources. They can simply click on the bookmark from the SSL VPN portal, and the connection will be established.

4. **Centralized Configuration and Management:**
   - Administrators can centrally configure and manage bookmarks for different user groups or individual users. They can control who has access to specific resources and update bookmarks as needed.

Benefits of Using SSL VPN Bookmarks

- **User-Friendly:** Provides an easy-to-use interface for accessing internal resources without needing a full VPN client.
- **Granular Access Control:** Administrators can control which bookmarks are available to which users or groups.
- **Increased Security:** Limits access to only the specified resources rather than providing full network access.
- **Centralized Management:** Easy to update or change bookmarks for all users from a single location.

Use Cases for SSL VPN Bookmarks

- **Remote Access to Internal Web Applications:** Employees can access intranet sites or web-based applications securely while working remotely.
- **Secure File Transfer:** Users can download or upload files from internal file servers using FTP/SFTP bookmarks.
- **Remote Server Administration:** IT staff can use RDP or SSH bookmarks to manage servers without needing a separate client.

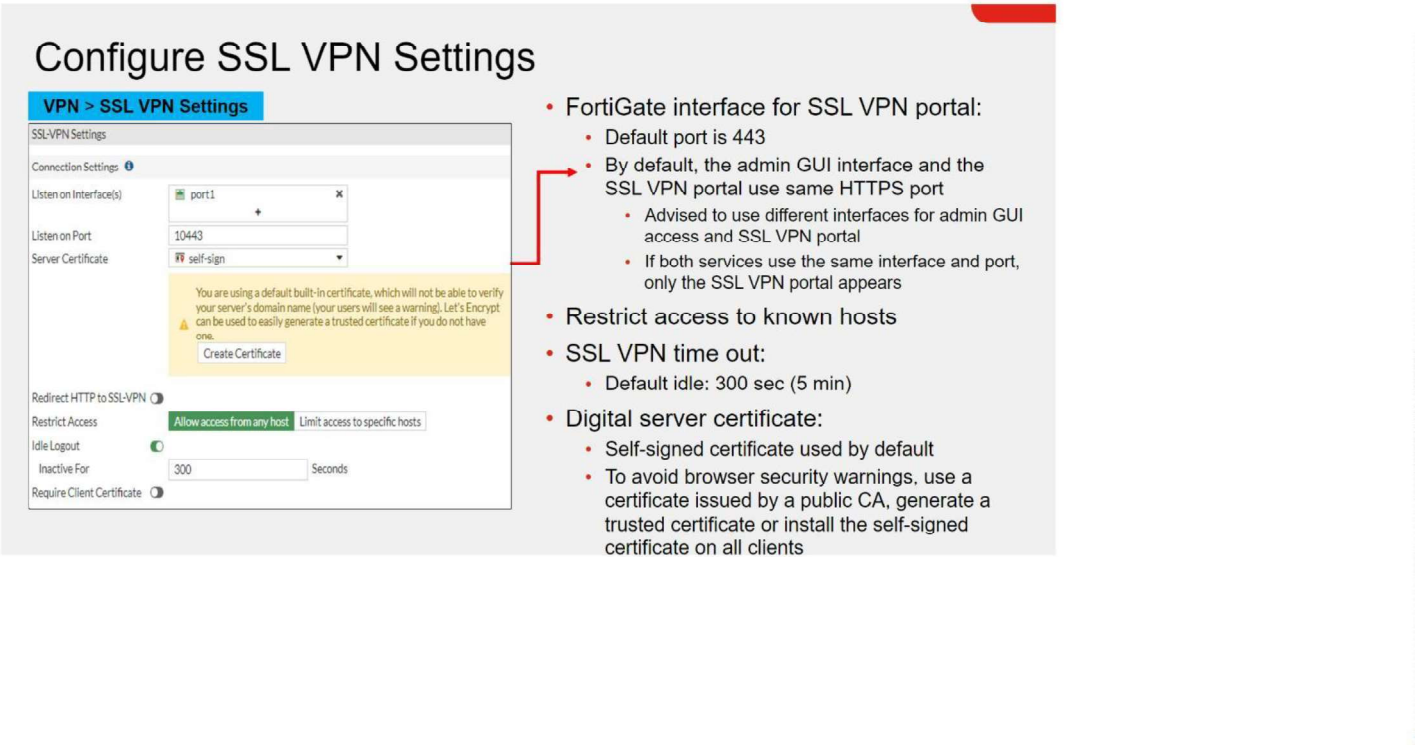
SSL VPN bookmarks enhance user experience and security by providing a convenient and controlled way to access internal resources through an SSL VPN portal.

FortiClient Download

FortiClient Download	Enable this option to display the *Download FortiClient* button.
Download Method	Select either *Direct* or *SSL-VPN Proxy* as the method to download FortiClient.
Customize Download Location	Enable to configure a custom download location for *Windows* or *Mac*.

3 Configure SSL VPN Settings

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



There are 4 parts in the SSL VPN Settings window:

1- **Connection Settings**
2- **Tunnel Mode Client Settings**
3- **Web Mode Settings**
4- **Authentication/Portal Mapping**

Listen on Interface(s):

Here, you need to map a FortiGate interface to the SSL VPN portal.

This option defines which network interfaces on the FortiGate device will listen for incoming SSL VPN connections.

- **WAN1, WAN2, etc.**: These are typically the interfaces connected to the internet. Select the interface(s) where users will connect from external networks.
- **Multiple interfaces** can be selected if you want the SSL VPN to be accessible from multiple public IP addresses.

Listen on Port: / Redirect HTTP to SSL VPN:

The port number that SSL VPN listens on for incoming connections. The default is port **443**, which is commonly used for HTTPS traffic.

- **443:** The standard HTTPS port, typically used for SSL VPN. If you are running a web service on this port, you can choose a different port (e.g., 8443).
- Changing the port may be necessary if port 443 is already used by another service on your FortiGate or if you want to use a custom port.

If you enable **Redirect HTTP to SSL VPN**, users who connect using HTTP (TCP port 80) will be redirected to HTTPS.

Note that:

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 port 443 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.

Server Certificate

This is the SSL certificate used to secure the VPN connection. It encrypts the traffic between the user and the FortiGate device.

- **Default Certificate**: FortiGate includes a self-signed certificate by default. This is fine for internal or testing purposes, but it will generate browser warnings since it's not from a trusted Certificate Authority (CA).
- **Custom Certificate**: For production environments, it's best to use a valid SSL certificate issued by a trusted CA. You can upload your own certificate to use for the SSL VPN.

Restrict Access:

This setting controls which users or user groups can access the SSL VPN.

- **Allow access from any host:** All users can access the SSL VPN as long as they have valid credentials.
- **Limit access to specific host:** You can limit access to only specific user groups. For example, you can select the **`SSLVPN_Users`**group so that only members of this group can log in.

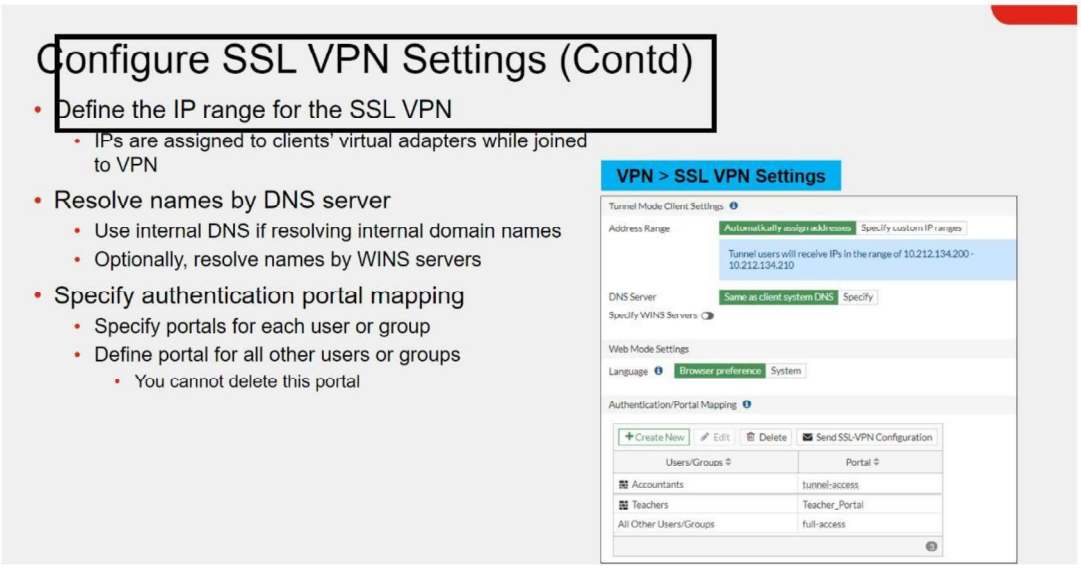
Idle Logout:

This setting determines how long a VPN connection can remain idle before the user is disconnected.

- **Default is 300 seconds (5 minutes)**: This means if there is no activity from the user's VPN connection for 5 minutes, the session will be disconnected.
- You can increase or decrease this value depending on your security policies.

Require Client Certificate:

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 selfsigned digital certificate into the browser as a trusted authority.



Tunnel mode allows the user to establish a full VPN connection to the network.

Address Range:

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.

Specify a range of IP addresses (e.g., 10.10.10.1 - 10.10.10.50) that VPN clients will use. These should not overlap with your internal network addresses.

DNS Server:

- You can configure the DNS server that VPN clients will use. This is especially useful if you want them to resolve internal domain names (e.g., intranet.company.local).
- **Custom DNS Server**: You can define custom DNS servers, such as a corporate DNS or a public DNS server like Google's DNS (8.8.8.8).

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.

Language:

- Browser Preference
- System

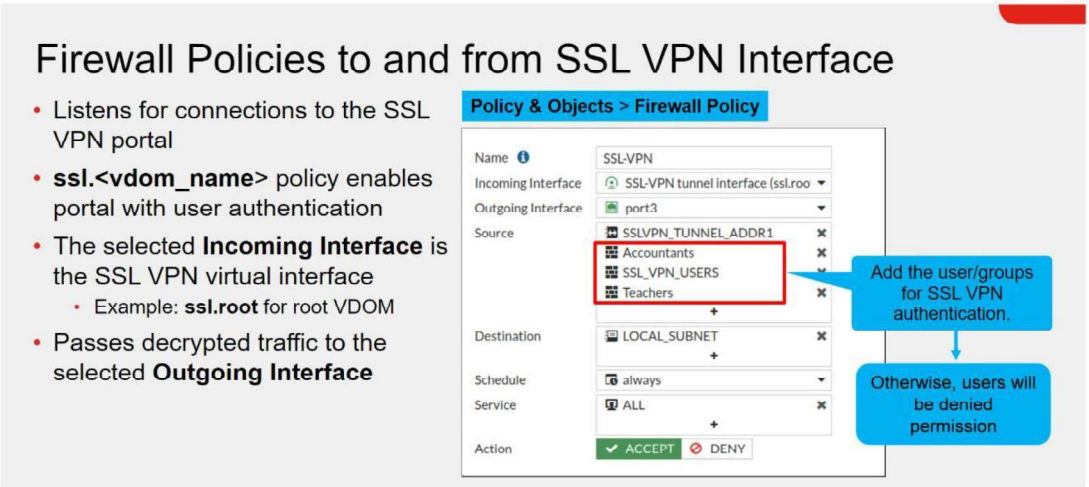
This controls which users or user groups have access to which SSL VPN portals. Portals define the level of access a user gets once connected to the VPN.

- **Source**: Select the user or user group. For example, you might select the SSLVPN_Users group that you created earlier.
- **Portal**: Choose the SSL VPN portal for these users. The portal defines what type of access the users have (e.g., full access, limited access, or web-only access).

4 Firewall Policies to and from SSL VPN Interface

In this step, you configure firewall policies to allow SSL VPN users to access the internal network resources securely. Firewall policies control which traffic is allowed or blocked between different network interfaces on the FortiGate device. For SSL VPN, you must create a policy that allows traffic from the SSL VPN tunnel interface to your internal network.

To allow VPN users to access internal resources, you need to configure a firewall policy.



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.

Step 1. Go to IPv4 Policy

- Log in to the FortiGate web interface.
- Navigate to **Policy & Objects > IPv4 Policy**. This is where you create and manage firewall policies.

Stepn 2. Create a New Firewall Policy

- Click **Create New** to start configuring a new policy.
- A new window will appear where you can configure the details of the policy.

Step 3. Configure Policy Settings

1. **Name**:
   - Give the policy a meaningful name, such as SSLVPN_to_Internal_Network. This helps in identifying the policy easily.
2. **Incoming Interface**:
   - Set this to the **SSL VPN Tunnel interface** (typically named ssl.root).
   - This is the virtual interface created by FortiGate for SSL VPN traffic.
3. **Outgoing Interface**:
   - Set this to your internal network interface (e.g., LAN, internal, vlan1).
   - This defines where the VPN users will be able to send their traffic (i.e., which network segment or VLAN).
4. **Source**:
   - The source defines where the traffic is coming from. In this case, it's the SSL VPN users or the IP pool assigned to VPN clients.
   - Choose one of the following options:
     - **User Group**: Select the user group that you created earlier (e.g., SSLVPN_Users). This ensures that only authenticated users from this group can send traffic through the VPN.
     - **IP Pool**: If you prefer, you can select the IP range or address pool that was defined earlier for the SSL VPN clients.
5. **Destination**:
   - The destination defines which resources or networks the VPN users can access.
   - Set this to the specific subnet or network where the internal resources are located. For example:
     - **All**: This allows access to the entire internal network.
     - **Specific Subnet**: If you want to restrict access, select a specific subnet (e.g., 192.168.1.0/24).
     - **Individual Server**: If users should only access certain resources, you can specify a single IP or a server.
6. **Schedule**:
   - Set the schedule for when this policy is active.
   - **Always**: This is typically set to allow the policy to be active all the time, but you can choose specific times/dates if needed.
7. **Service**:
   - The services define which types of traffic are allowed through the VPN.
   - You can select specific protocols or services that the VPN users will use, such as:
     - **ALL**: Allow all types of traffic (not recommended for strict environments).
     - **Predefined Services**: Select services like HTTP, HTTPS, SSH, RDP, etc., depending on what you want users to access.
     - **Custom Services**: You can also create custom service definitions if needed.

8. **Action**:
    - Set the action to **Accept** to allow the traffic.
    - This tells FortiGate to allow the SSL VPN traffic that matches the policy criteria (source, destination, service).
9. **Enable NAT (Optional)**:
    - If required, enable **NAT** (Network Address Translation). This is typically used when translating the VPN client's IP address into the internal IP address when communicating with the network. If the VPN clients' IP pool is on a different subnet from the internal network, NAT is usually required.

Step 4. Security Profiles (Optional but Recommended)

- **Enable Security Profiles**: You can apply security profiles like **Antivirus**, **Web Filter**, **Application Control**, etc., to protect the network from malware, unauthorized applications, or inappropriate content.
- These profiles help to inspect the traffic passing through the VPN for security threats and inappropriate usage.

Step 5. Save the Policy

- Once you've configured all the fields, click **OK** to save the policy.

Connecting from FortiClient VPN client

For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS. This version does not include central management, technical support, or some advanced features.

Downloading and installing the standalone FortiCient VPN client

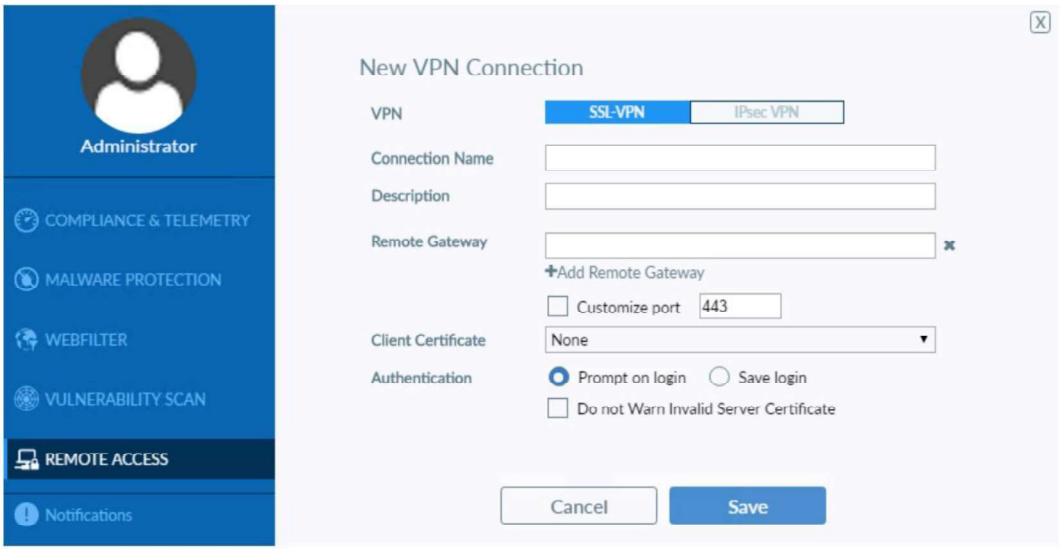
You can download the free VPN client from FNDN or FortiClient.com.

When the free VPN client is run for the first time, it displays a disclaimer. You cannot configure or create a VPN connection until you accept the disclaimer and click, *I accept*:

Configuring an SSL VPN connection

To configure an SSL VPN connection:

1. On the *Remote Access* tab, click on the settings icon and then *Add a New Connection*.



2. Select *SSL-VPN*, then configure the following settings:

Connection Name	SSLVPNtoHQ
Description	(Optional)
Remote Gateway	172.20.120.123
Customize port	10443
Client Certificate	Select *Prompt on connect* or the certificate from the dropdown list.
Authentication	Select *Prompt on login* for a prompt on the connection screen

3. Click *Save* to save the VPN connection.

Connecting to SSL VPN

To connect to SSL VPN:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.

   Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.
2. Enter your username and password.
3. Click the *Connect* button.
4. After connecting, you can now browse your remote network. Traffic to 192.168.1.0 goes through the tunnel, while other traffic goes through the local gateway. FortiClient displays the connection status, duration, and other relevant information.
5. Click the *Disconnect* button when you are ready to terminate the VPN session.

Checking the SSL VPN connection

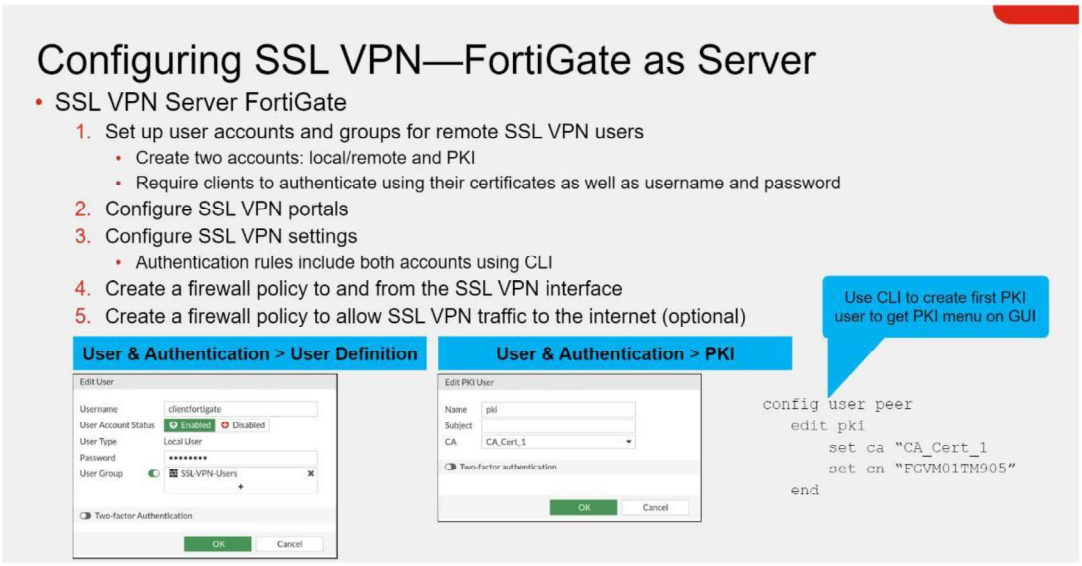
To check the SSL VPN connection using the GUI:

1. On the FortiGate, go to *VPN* > *Monitor* > *SSL-VPN Monitor* to verify the list of SSL users.
2. On the FortiGate, go to *Log & Report* > *Forward Traffic* to view the details of the SSL entry.

Configuring SSL VPN – FortiGate as Server

To configure an SSL VPN on FortiGate as the server, follow this step-by-step guide.

All steps are identical to SSL VPN setup for remote users. However, I'll cover the entire process from initial setup to user authentication and connection again.



Step 1: Access the FortiGate Web Interface

1. Open a web browser and navigate to the IP address of your FortiGate device.
2. Login with your administrator credentials.

Step 2: Create User Accounts or Integrate LDAP/Radius

SSL VPN users can either be local users on the FortiGate or authenticated via LDAP, Radius, or another external authentication method.

For local user creation:

1. Navigate to **User & Authentication** > **User Definition**.
2. Click **Create New** > **Local User**.
3. Enter a **Username** and **Password**.
4. Optionally, set up **Two-Factor Authentication** for added security.
5. Click **OK**.

For LDAP authentication:

1. Go to **User & Authentication** > **LDAP Servers**.
2. Click **Create New**.
3. Enter the necessary details like:
    - **Server Name**.
    - **Server IP/Name**.
    - **Common Name Identifier** (usually cn).
    - **Distinguished Name** (base DN of your LDAP, e.g., dc=example,dc=com).
    - **Bind Type** and credentials.
4. Click **OK** and test the connection.

For RADIUS authentication:

1. Navigate to **User & Authentication** > **RADIUS Servers**.
2. Click **Create New** and fill in the RADIUS server details (e.g., IP, shared secret).
3. Save and test the connection.

Create two accounts:

- local or remote user accounts or groups
- and PKI users.

- **Require clients to authenticate using their certificates as well as username and password.**

Note That:

The PKI menu is available on the GUI only after you have created a PKI user using the CLI. You can configure a CN (Common Name) 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.

What is PKI?

Step 3: Create a User Group for SSL VPN Access

1. Navigate to **User & Authentication** > **User Groups**.
2. Click **Create New** and name the group something identifiable, like "SSL-VPN-Users".
3. Add either the local users created or the LDAP/RADIUS group.

Step 4: Enable SSL VPN on the Interface

1. Navigate to **VPN** > **SSL-VPN Settings**.
2. In the **Listen on Interface(s)** section, select the interface through which users will connect to the VPN (typically the WAN interface).
3. Set the **Listen on Port** to 443 (default HTTPS port) unless you want to change it to another custom port.
4. Set the **Mode**:
    - **Tunnel Mode**: Allows access to internal network resources.
    - **Web Mode**: Users can access internal resources through a web browser.
5. Configure the **Server Certificate**. If you have an SSL certificate, select it. Otherwise, you can use the default FortiGate certificate, although it's recommended to use a valid one.
6. Under **Authentication/Portal Mapping**, assign the previously created user group to either the full-access, tunnel access, or a custom portal.

Step 5: Configure SSL VPN Portal

The portal determines what the users can access when they connect via SSL VPN.

1. Navigate to **VPN** > **SSL-VPN Portals**.
2. Edit the default **full-access** portal or create a new one:
    - In the **Tunnel Mode** section, enable **Allow Access to Local Network**.
    - Specify the **IP Pools** for users who will connect.
    - Customize the portal options based on your needs, like split tunneling or specific resources.

Step 6: Create IP Pools for SSL VPN Users

The IP Pool defines the IP address range for users when they connect through SSL VPN.

1. Navigate to **Network** > **Interfaces** > **IP Pools**.
2. Click **Create New** and define an IP range that does not conflict with your internal network.
3. Associate the pool with the SSL VPN settings under **VPN** > **SSL-VPN Settings**.

Step 7: Configure Firewall Policy for SSL VPN Traffic

1. Go to **Policy & Objects** > **IPv4 Policy**.
2. Click **Create New** and name the policy (e.g., "SSLVPN Access").
3. Set the **Incoming Interface** to ssl.root.
4. Set the **Outgoing Interface** to your internal LAN interface.
5. Under **Source**, select **SSLVPN_Users** and the IP Pool you configured earlier.
6. Under **Destination**, specify the resources or network the users can access (e.g., internal servers or subnets).
7. Set **Service** to ALL (or define a specific service like HTTP, RDP, etc.).
8. Enable **NAT** if necessary (usually not required if you're only accessing internal resources).
9. Click **OK** to save the policy.

Step 8: Configure DNS for SSL VPN Users (Optional)

To ensure VPN clients can resolve internal DNS names, configure DNS settings.

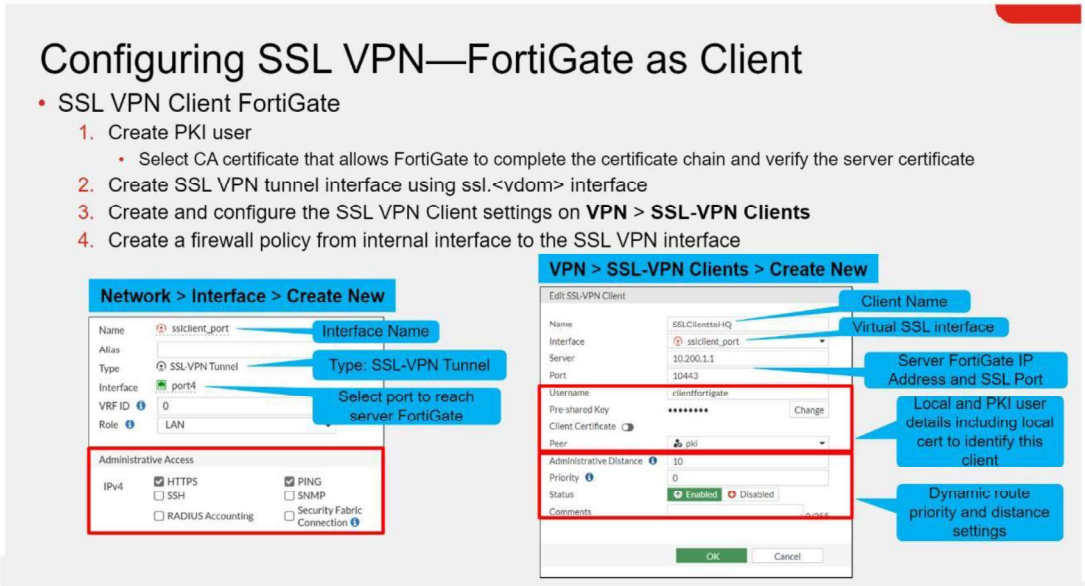
1. Go to **VPN** > **SSL-VPN Settings**.
2. Scroll down to **DNS Settings**.
3. Specify your internal DNS servers and domain.
4. Save the settings.

Step 9: Test the Configuration

1. Download the FortiClient from the Fortinet website and install it on a client machine.
2. Open FortiClient and configure the VPN settings:
    - Connection Type: **SSL VPN**.
    - Remote Gateway: Enter the public IP or domain name of the FortiGate's WAN interface.
    - Port: Enter the port you set (default is 443).
3. Enter the username and password of a user that has SSL VPN access.
4. Test the connection by attempting to connect to internal resources or pinging devices within the network.

Configuring SSL VPN – FortiGate as Client

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



Step 1: Set up user accounts and groups for remote SSL VPN users (Through CLI)

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. (Username and password are created on FortiGate Server)

To create a PKI user in the GUI:

1. Go to *User & Authentication* > *PKI* and click *Create New*.
2. Set the *Name* to *fgt_gui_automation*.
3. Set *CA* to the CA certificate. The CA certificate allows the FortiGate to complete the certificate chain and verify the server 's certificate, and is assumed to already be installed on the FortiGate.
4. Click *OK*.

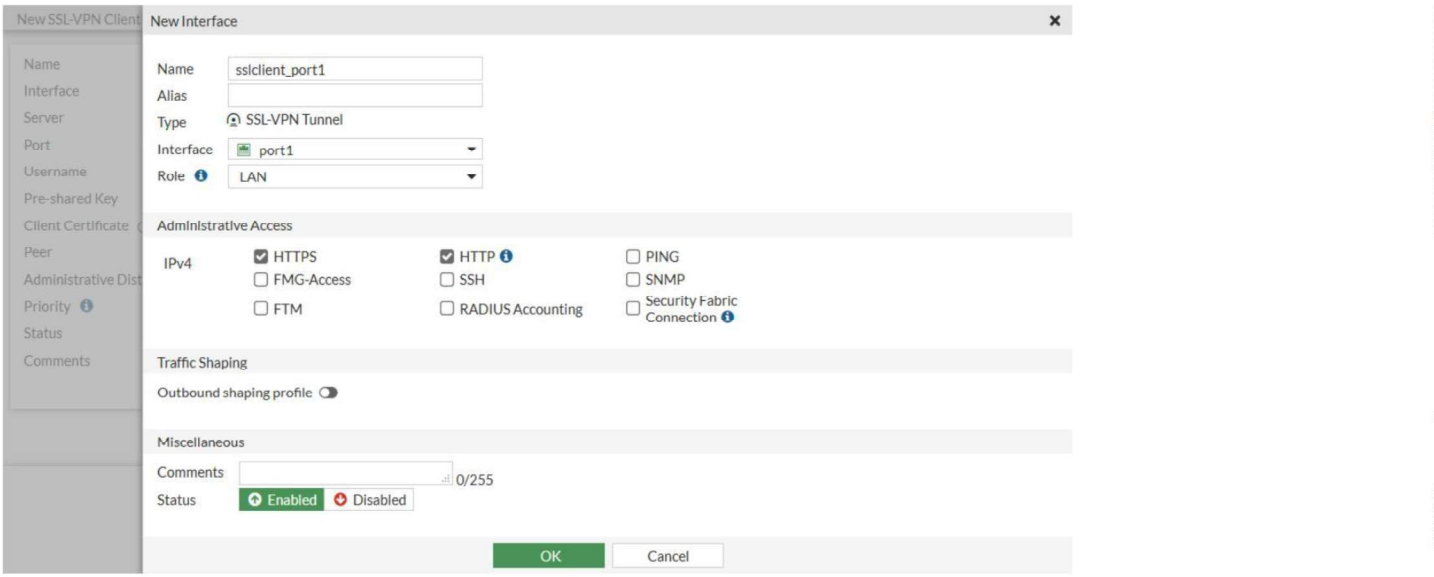
5. In the CLI, specify the CN of the certificate on the SSL VPN server:

```
config user peer
    edit "fgt gui automation"
        set cn "*.fos.automation.com"
    next
           end
```

Step 2: Create SSL VPN Tunnel Interface using `ssl.<vdom>`interface

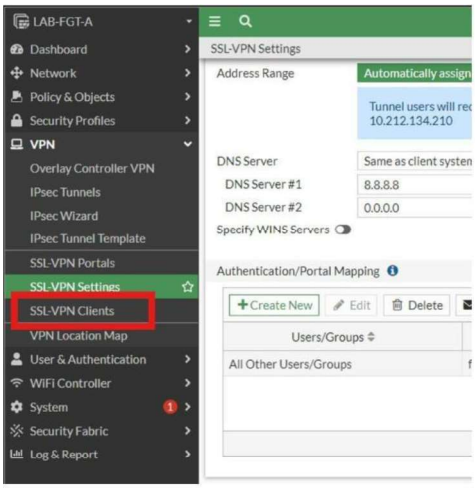
Network > Interface > Create New

Next, create the SSL VPN tunnel interface using the **`ssl.<vdom>`**interface.



Step 3: Create and configure the SSL VPN Client settings on:

VPN > SSL-VPN Client



The SSL-VPN Clients settings include:

- name,
- virtual SSL VPN interface,
- SSL VPN server FortiGate IP address,
- SSL port number,
- local username,
- password,
- and PKI (Peer) user,
- Client Certificate 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.

Step 4: Create a firewall policy from internal interface to the SSL VPN interface

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

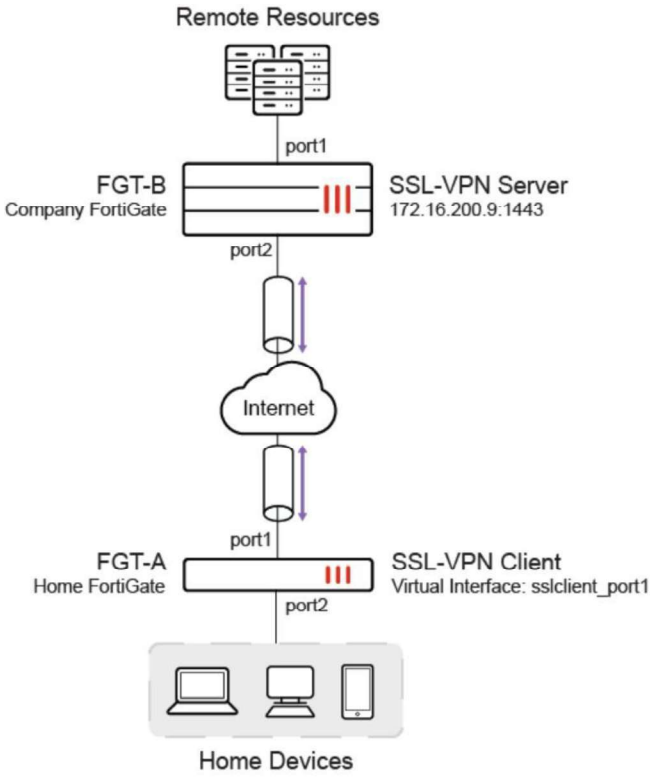
Examples and real-world scenarios

SCENARIO 1

In this example, the home FortiGate (FGT-A) is configured as an SSL VPN client, and the company FortiGate (FGT-B) is configured as an SSL VPN server. After FGT-A connects to FGT-B, the devices that are connected to FGT-A can access the resources behind FGT-B.

The SSL VPN server has a custom server certificate defined, and the SSL VPN client user uses PSK and a PKI client certificate to authenticate. The FortiGates must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.

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.



Configure the SSL VPN server

To create a local user in the GUI:

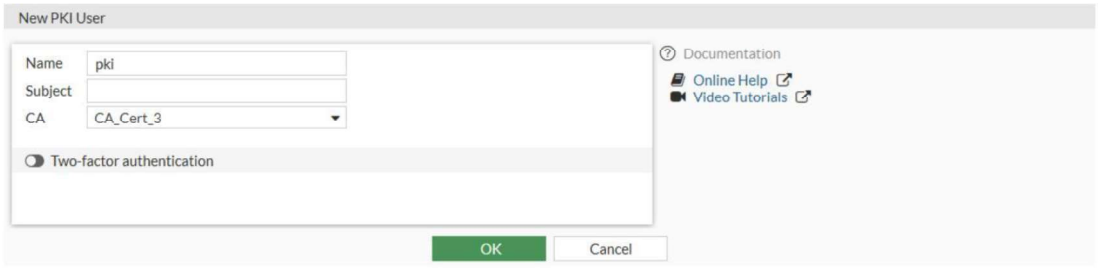
1. Go to *User & Authentication* > *User Definition* and click *Create New*.
2. Use the wizard to create a local user named *client2*.

To create a PKI user in the GUI:

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.

---

1. Go to *User & Authentication* > *PKI* and click *Create New*.
2. Set the *Name* to *pki*.
3. Set *CA* to the CA certificate that is used to verify the client certificate.



4. Click *OK*.
5. In the CLI, specify the CN that must be matched. If no CN is specified, then any certificate that is signed by the CA will be valid and matched.

```
config user peer
    edit "pki"
        set cn "*.fos.automation.com"
    next
            end
```

To create an SSL VPN portal in the GUI:

1. Go to *VPN* > *SSL-VPN Portals* and click *Create New*.
2. Set the *Name* to *testportal2*.
3. Set *Enable Split Tunneling* to *Enabled Based on Policy Destination*.
4. Set *Source IP Pools* to *SSLVPN_TUNNEL_ADDR1*.
5. Click *OK*.

To configure SSL VPN settings in the GUI:

1. Go to *VPN* > *SSL-VPN Settings* and enable *Enable SSL-VPN*.
2. Set *Listen on Interface(s)* to *port2*.
3. Set *Listen on Port* to *1443*.
4. Set *Server Certificate* to *fgt_gui_automation*.
5. In the *Authentication/Portal Mapping* table click *Create New*:
    1. Set *Users/Groups* to *client2*.
    2. Set *Portal* to *testportal2*.
    3. Click *OK*.
6. Click *OK*.
7. In the CLI, enable SSL VPN client certificate restrictive and set the user peer to *pki*:

```
config vpn ssl settings
    config authentication-rule
        edit 1
            set client-cert enable
            set user-peer "pki"
        next
    end
            end
```

To create a firewall address in the GUI:

1. Go to *Policy & Objects* > *Addresses* and select *Address*.
2. click *Create new*.
3. Set the *Name* to *bing.com*.
4. Set *Type* to *FQDN*.
5. Set *FQDN* to *www.bing.com*.
6. Click *OK*.

To create a firewall policy in the GUI:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Configure the policy:

Name	*sslvpn2*
Incoming Interface	*SSL-VPN tunnel interface (ssl.root)*
Outgoing Interface	*port1*
Source	*Address*: *all* *User*: *client2*
Destination	*bing.com*: This FQDN resolves to 13.107.21.200 and 204.79.197.200. Traffic to these addresses is directed to the SSL VPN, while other traffic is routed to the remote devices' default adapters or interfaces. *mantis*
Schedule	*always*
Service	*ALL*
Action	*Accept*

3. Click *OK*.

Configure the SSL VPN client

To create a PKI user in the GUI:

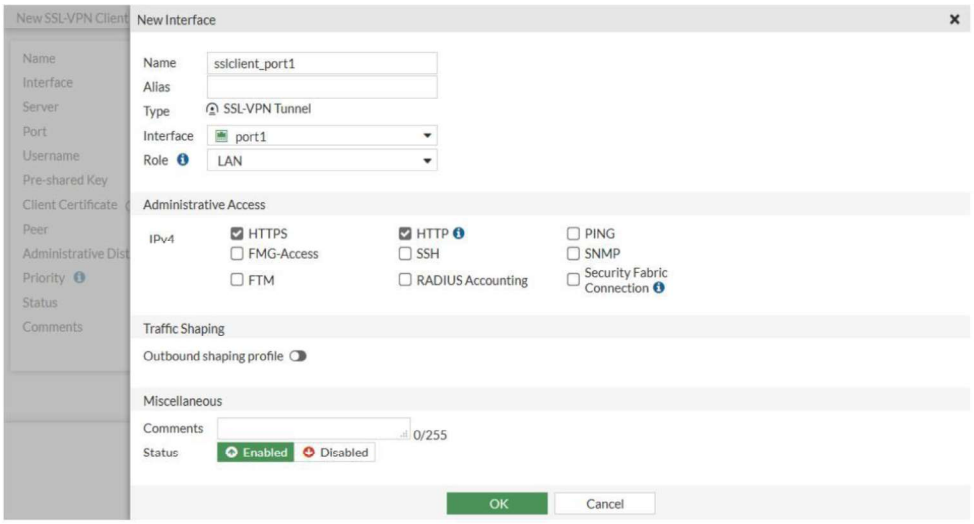
The PKI menu is only available in the GUI after a PKI user has been created using the CLI, and a CN can only be configured in the CLI.

1. Go to *User & Authentication* > *PKI* and click *Create New*.
2. Set the *Name* to *fgt_gui_automation*.
3. Set *CA* to the CA certificate. The CA certificate allows the FortiGate to complete the certificate chain and verify the server 's certificate, and is assumed to already be installed on the FortiGate.
4. Click *OK*.
5. In the CLI, specify the CN of the certificate on the SSL VPN server:

```
config user peer
    edit "fgt_gui_automation"
        set cn "*.fos.automation.com"
    next
          end
```

To create an SSL VPN client and virtual interface in the GUI:

1. Go to *VPN* > *SSL-VPN Clients* and click *Create New*.
2. Expand the *Interface* drop down and click *Create* to create a new virtual interface:
   A. Set the *Name* to *sslclient_port1*.
   B. Set *Interface* to *port1*.
   C. Under *Administrative Access*, select *HTTPS* and *PING*.



D. Click *OK*.

3. Configure the SSL VPN client:

Name	*sslclientTo9*
Interface	*sslclient_port1*
Server	*172.16.200.9*
Port	*1443*
Username	*client2*
Pre-shared Key	**********
Client Certificate	*fgtb_gui_automation* This 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.
Peer	*fgt_gui_automation*
Administrative Distance	Configure as needed.
Priority	Configure as needed.
Status	Enabled

4. Click *OK*.

To create a firewall policy in the GUI:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Configure the policy:

Name	*policy_to_sslvpn_tunnel*
Incoming Interface	*port2*
Outgoing Interface	*sslclient_port1*
Source	*all*
Destination	*all*
Schedule	*always*
Service	*ALL*
Action	*Accept*

3. Click *OK*.

Verification

After the tunnel is established, the route to 13.107.21.200 and 204.79.197.200 on FGT-A connects through the SSL VPN virtual interface *sslclient_port1*.

To check the routing table details:

```
(vdom1) # get router info routing-table details
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 172.16.200.254, port1
C       10.0.1.0/24 is directly connected, link_11
C       10.1.100.0/24 is directly connected, port2
                      is directly connected, port2
C       10.212.134.200/32 is directly connected, sslclient_port1
S       13.107.21.200/32 [10/0] is directly connected, sslclient_port1
C       172.16.200.0/24 is directly connected, port1
S       192.168.100.126/32 [10/0] is directly connected, sslclient_port1
S       204.79.197.200/32 [10/0] is directly connected, sslclient_port1
```

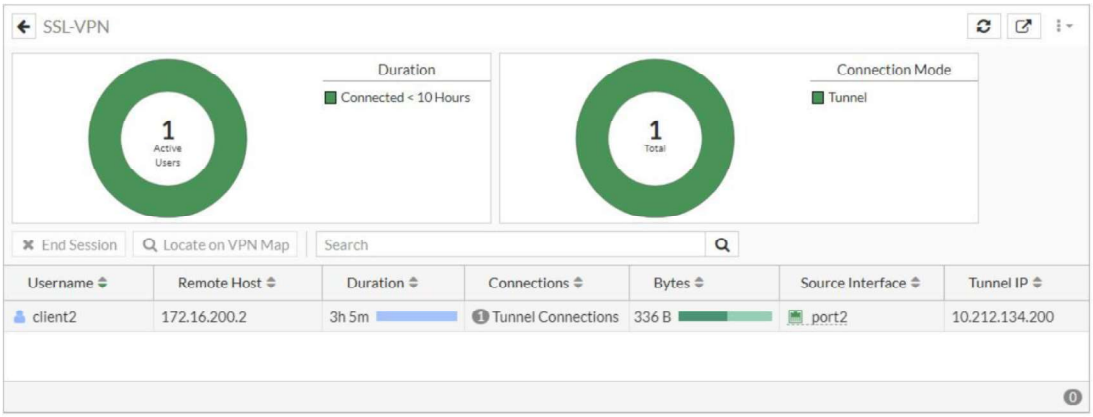
To check the added routing for an IPv6 tunnel:

```
(vdom1) # get router info6 routing-table database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, B - BGP
       > - selected route, * - FIB route, p - stale info
Timers: Uptime
```

```
S     *> ::/0 [10/0] via 2000:172:16:200::254, port1, 00:00:01, [1024/0]
      *>      [10/0] via ::, sslclient_port1, 00:00:01, [1024/0]
C     *> ::1/128 via ::, vdom1, 03:26:35
C     *> 2000:10:0:1::/64 via ::, link_11, 03:26:35
C     *> 2000:10:1:100::/64 via ::, port2, 03:26:35
C     *> 2000:172:16:200::/64 via ::, port1, 03:26:35
C     *> 2001:1::1:100/128 via ::, sslclient_port1, 00:00:01
C     *> fe80::/64 via ::, port2, 03:26:35
```

To check the connection in the GUI:

1. On the SSL VPN server FortiGate (FGT-B), go to *Dashboard* > *Network* and expand the *SSL-VPN* widget.



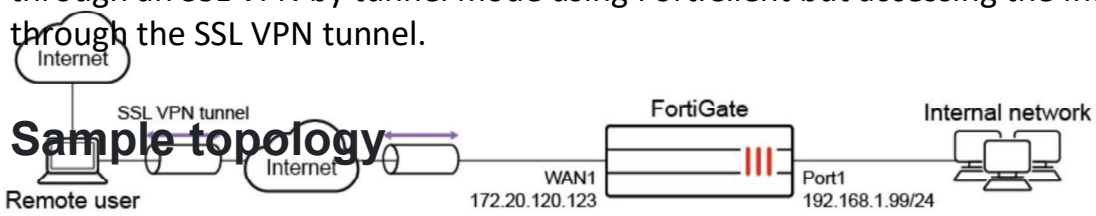
2. On the SSL VPN client FortiGate (FGT-A), go to *VPN* > *SSL-VPN Clients* to see the tunnel list.

SCENARIO 2

SSL VPN split tunnel for remote user

This is a sample configuration of remote users accessing the corporate network and internet through an SSL VPN by tunnel mode using FortiClient but accessing the Internet without going through the SSL VPN tunnel.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface. Ensure that SSL VPN feature visibility is enabled before starting the configuration.

The split tunneling routing address cannot explicitly use an FQDN or an address group that includes an FQDN. To use an FQDN, leave the routing address blank and apply the FQDN as the destination address of the firewall policy.

To configure SSL VPN using the GUI:

1. Enable SSL VPN feature visibility:

A. Go to *System > Feature Visibility*.

B. In the *Core Features* section, enable *SSL-VPN*.

C. Click *Apply*.

2. Configure the interface and firewall address. The port1 interface connects to the internal network.

A. Go to *Network > Interfaces* and edit the *wan1* interface.

B. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.

C. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.

D. Click *OK*.

E. Go to *Policy & Objects > Address* and create an address for internal subnet *192.168.1.0*.

3. Configure user and user group.

A. Go to *User & Authentication > User Definition* to create a local user *sslvpnuser1*.

B. Go to *User & Authentication > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.

4. Configure SSL VPN web portal.

A. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-split-tunnel-portal*.

B. Enable *Tunnel Mode* and select one of the *Split tunneling* settings.

C. Select *Routing Address Override* to define the destination network (usually the corporate network) that will be routed through the tunnel.

Leave *Routing Address Override* undefined to use the destination in the respective firewall policies.

D. Select *Source IP Pools* for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.

5. Configure SSL VPN settings.

A. Go to VPN > SSL-VPN Settings.

B. For Listen on Interface(s), select wan1.

C. Set Listen on Port to 10443.

D. Choose a certificate for Server Certificate. The default is Fortinet_Factory.

E. In Authentication/Portal Mapping All Other Users/Groups, set the Portal to tunnel-access.

F. Create new Authentication/Portal Mapping for group sslvpngroup mapping portal my-split-tunnel-portal.

6. Configure SSL VPN firewall policy.

A. Go to *Policy & Objects > Firewall Policy*.

B. Fill in the firewall policy name. In this example, *sslvpn split tunnel access*.

C. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.

D. Choose an *Outgoing Interface*. In this example, *port1*.

E. Set the *Source* to *all* and group to *sslvpngroup*.

F. In this example, the *Destination* is the internal protected subnet 192.168.1.0.

G. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.

H. Click *OK*.

SCENARIO 3

Set up FortiToken multi-factor authentication

This configuration adds multi-factor authentication (MFA) to the split tunnel configuration. It uses one of the two free mobile FortiTokens that is already installed on the FortiGate.

To configure MFA using the GUI:

1. Configure a user and user group:

A. Go to User & Authentication > User Definition and edit local user sslvpnuser1.

B. Enable Two-factor Authentication.

C. For Authentication Type, click FortiToken and select one mobile Token from the list.

D. Enter the user's Email Address.

E. Enable Send Activation Code and select Email.

F. Click Next and click Submit.

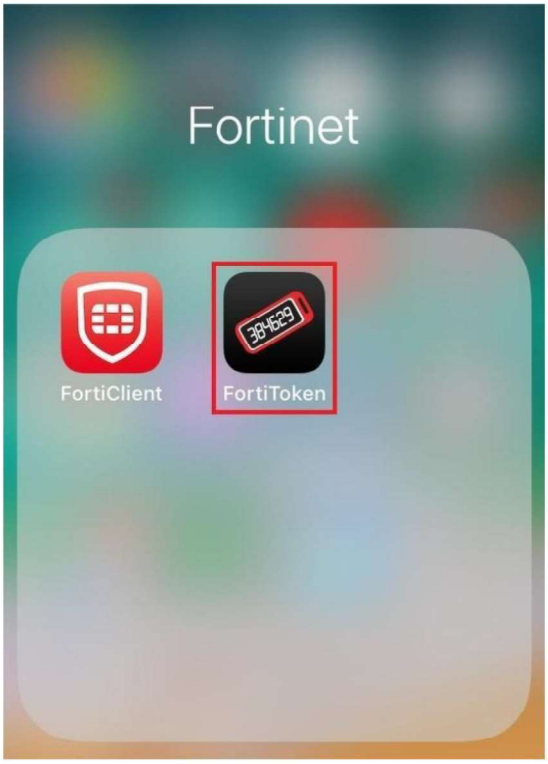
2. Activate the mobile token.

When a FortiToken is added to user sslvpnuser1, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

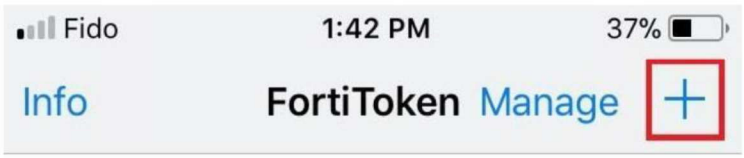
SCENARIO 4 Connecting from FortiClient with FortiToken

To activate your FortiToken:

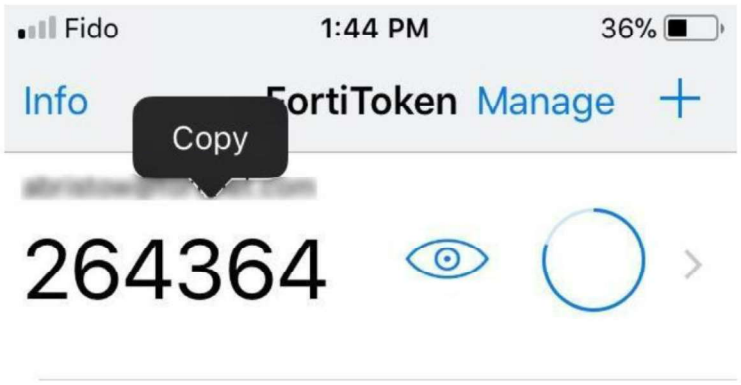
1. On your device, open FortiToken Mobile. If this is your first time opening the application, it may prompt you to create a PIN for secure access to the application and tokens.



2. You should have received your notification via email, select + and use the device camera to scan the token QR code in your email.



3. FortiToken Mobile provisions and activates your token and generates token codes immediately. To view the OTP's digits, select the eye icon. After you open the application, FortiToken Mobile generates a new six-digit OTP every 30 seconds.



To connect to SSL VPN:

A. On the *Remote Access* tab, select the VPN connection from the dropdown list.

   Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.

B. Enter your username and password.

C. Click the *Connect* button.

D. A Token field will appear, prompting you for the FortiToken code. Enter the FortiToken code from your Mobile device.

E. After connecting, you can now browse your remote network. Traffic to 192.168.1.0 goes through the tunnel, while other traffic goes through the local gateway. FortiClient displays the connection status, duration, and other relevant information.

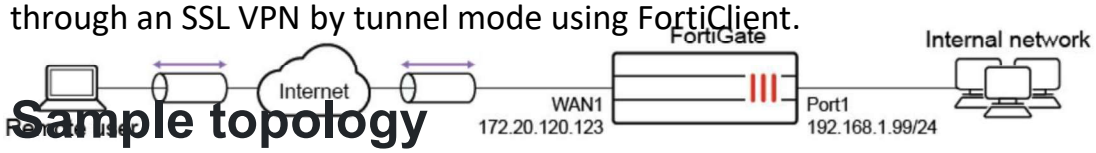
F. Click the *Disconnect* button when you are ready to terminate the VPN session.

SCENARIO 5

SSL VPN full tunnel for remote user

This is a sample configuration of remote users accessing the corporate network and internet through an SSL VPN by tunnel mode using FortiClient.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface. Ensure that SSL VPN feature visibility is enabled before starting the configuration.

To configure SSL VPN using the GUI:

1. Enable SSL VPN feature visibility:

A. Go to *System* > *Feature Visibility*.

B. In the *Core Features* section, enable *SSL-VPN*.

C. Click *Apply*.

2. Configure the interface and firewall address:

A. Go to *Network* > *Interfaces* and edit the *wan1* interface.

B. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.

C. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.

D. Click *OK*.

3. Configure user and user group:

A. Go to *User & Authentication > User Definition* to create a local user *sslvpnuser1*.

B. Go to *User & Authentication > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.

4. Configure SSL VPN web portal:

A. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-full-tunnel-portal*.

B. Disable *Split Tunneling*.

5. Configure SSL VPN settings:

A. Go to *VPN > SSL-VPN Settings*.

B. For *Listen on Interface(s)*, select *wan1*.

C. Set *Listen on Port* to *10443*.

D. Choose a certificate for *Server Certificate*. The default is *Fortinet_Factory*.

E. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *tunnel-access*.

F. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-full-tunnel-portal*.

6. Configure SSL VPN firewall policies to allow remote user to access the internal network:

A. Go to *Policy & Objects > Firewall Policy* and click *Create New*.

B. Set *Name* to *sslvpn tunnel mode access*.

C. Set *Incoming Interface* to *SSL-VPN tunnel interface(ssl.root)*.

D. Set *Outgoing Interface* to *port1*.

E. Set the *Source* Address to *all* and User to *sslvpngroup*.

F. Set *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.

G. Click *OK*.

H. Click *Create New*.

I. Set *Name* to *sslvpn tunnel mode outgoing*.

J. Configure the same settings as the previous policy, except set *Outgoing Interface* to *wan1*.

K. Click *OK*.

To see the results:

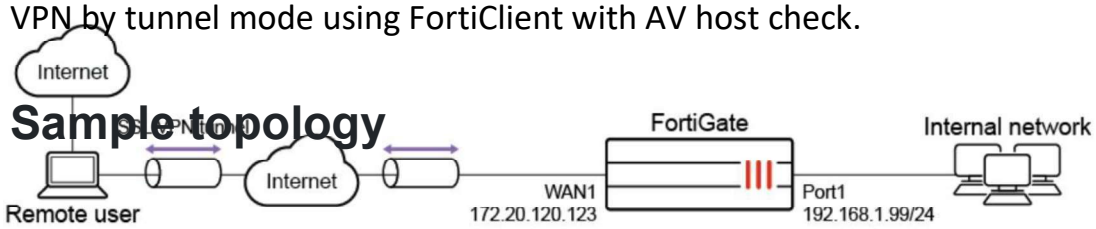
1. Download FortiClient from www.forticlient.com.
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection:
    - Set *VPN Type* to *SSL VPN*.
    - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Use the credentials you've set up to connect to the SSL VPN tunnel.
7. After connection, all traffic except the local subnet will go through the tunnel *FGT*.
8. Go to *VPN* > *Monitor* > *SSL-VPN Monitor* to verify the list of SSL users.
9. On the FortiGate, go to *Log & Report* > *Forward Traffic* and view the details for the SSL entry.

SCENARIO 6

SSL VPN tunnel mode host check

This is a sample configuration of remote users accessing the corporate network through an SSL VPN by tunnel mode using FortiClient with AV host check.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.

A. Go to *Network* > *Interfaces* and edit the *wan1* interface.

B. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.

C. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.

D. Click *OK*.

E. Go to *Policy & Objects* > *Address* and create an address for internet subnet *192.168.1.0*.

2. Configure user and user group.

A. Go to *User & Authentication* > *User Definition* to create a local user *sslvpnuser1*.

B. Go to *User & Authentication* > *User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.

3. Configure SSL VPN web portal.

A. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-split-tunnel-portal*.

B. Enable *Tunnel Mode* and select one of the *Split tunneling* settings.

C. Select *Routing Address Override*.

D. Select *Source IP Pools* for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.

4. Configure SSL VPN settings.

A. Go to *VPN > SSL-VPN Settings*.

B. For *Listen on Interface(s)*, select *wan1*.

C. Set *Listen on Port* to *10443*.

D. Choose a certificate for *Server Certificate*.

E. In *Authentication/Portal Mapping All Other Users/Groups*, set the ***Portal* to *tunnel-access*.**

F. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-split-tunnel-portal*.

5. Configure SSL VPN firewall policy.

A. Go to *Policy & Objects > Firewall Policy*.

B. Fill in the firewall policy name. In this example, *sslvpn tunnel access with av check*.

C. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.

D. Choose an *Outgoing Interface*. In this example, *port1*.

E. Set the *Source* to *all* and group to *sslvpngroup*.

F. In this example, the *Destination* is *all*.

G. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.

H. Click *OK*.

6. Use CLI to configure SSL VPN web portal to enable the host to check for compliant antivirus software on the user's computer.

```
config vpn ssl web portal
    edit my-split-tunnel-access
      set host-check av
    next
end
```

To see the results:

1. Download FortiClient from www.forticlient.com.
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection:
    - Set *VPN Type* to *SSL VPN*.
    - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Use the credentials you've set up to connect to the SSL VPN tunnel.

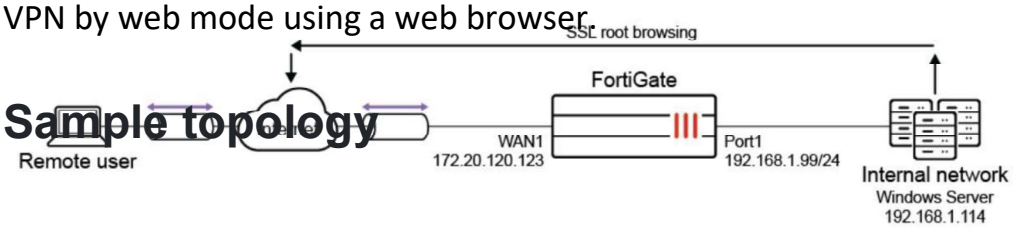
   If the user's computer has antivirus software, a connection is established; otherwise FortiClient shows a compliance warning.
7. After connection, traffic to *192.168.1.0* goes through the tunnel. Other traffic goes through local gateway.
8. On the FortiGate, go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
9. On the FortiGate, go to *Log & Report > Forward Traffic* and view the details for the SSL entry.

SCENARIO 7

SSL VPN web mode for remote user

This is a sample configuration of remote users accessing the corporate network through an SSL VPN by web mode using a web browser.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface. Ensure that SSL VPN web mode and SSL VPN feature visibility are enabled before starting the configuration.

To enable SSL VPN web mode and SSL VPN feature visibility in FortiOS:

1. Enable SSL VPN web mode:

```
config system global
   set sslvpn-web-mode enable
end
```

2. Enable SSL VPN feature visibility.

1. In the GUI:
   A. Go to *System* > *Feature Visibility*.
   B. In the *Core Features* section, enable *SSL-VPN*.
   C. Click *Apply*.
2. In the CLI:

```
config system settings
    set gui-sslvpn enable
end
```

To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.

A. Go to *Network* > *Interfaces* and edit the *wan1* interface.

B. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.

C. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.

D. Click *OK*.

E. Go to *Policy & Objects* > *Address* and create an address for internet subnet *192.168.1.0*.

2. Configure user and user group.

A. Go to *User & Authentication* > *User Definition* to create a local user *sslvpnuser1*.

B. Go to *User & Authentication* > *User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.

3. Configure SSL VPN web portal.

A. Go to *VPN* > *SSL-VPN Portals* to create a web mode only portal *my-web-portal*.

B. Set *Predefined Bookmarks for Windows server* to type *RDP*.

4. Configure SSL VPN settings.

A. Go to *VPN* > *SSL-VPN Settings*.

B. For *Listen on Interface(s)*, select *wan1*.

C. Set *Listen on Port* to *10443*.

D. Choose a certificate for *Server Certificate*.

E. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *web-access*.

F. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-Web-portal*.

5. Configure SSL VPN firewall policy.

A. Go to *Policy & Objects* > *Firewall Policy*.

B. Fill in the firewall policy name. In this example, *sslvpn web mode access*.

C. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.

D. Choose an *Outgoing Interface*. In this example, *port1*.

E. Set the *Source* to *all* and group to *sslvpngroup*.

F. In this example, the *Destination* is the internal protected subnet *192.168.1.0*.

G. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.

H. Click *OK*.

Do not set the virtual IP addresses as the destination address in a firewall policy when using SSL VPN web mode, as it will result in no destination address being accessible. Please note that the FortiOS SSL VPN web mode does not support mapping the virtual IP to the actual one.

To see the results:

1. In a web browser, log into the portal *https://172.20.120.123:10443* using the credentials you've set up.
2. In the portal with the predefined bookmark, select the bookmark to begin an RDP session. If there are no predefined bookmarks, the Quick Connection tool can be used;
3. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
4. Go to *Log & Report > Forward Traffic* to view the details for the SSL entry.

SCENARIO 8

SSL VPN bookmarks

The *Bookmarks* widget displays bookmarks configured by administrators and users. Administrator bookmarks cannot be edited, and they are configured in FortiOS. Users can add, edit, and delete their own bookmarks within the web portal.

The FortiGate forwards client requests to servers on the internet or internal network. To use the web portal applications, add the URL, IP address, or name of the server application to the *Bookmarks* list. Once a bookmark is created, click the bookmark icon to initiate a session.

To access a destination without adding a bookmark to the *Your Bookmarks* list, use the Quick Connection tool.

Configuring bookmarks

The following table summarizes which options can be configured based on the bookmark type in the SSL VPN web portal:

Setting	HTTP/ HTTPS	FTP	SMB	SFTP	RDP	VNC	SSH	Telnet
URL	✔							
Folder		✔	✔	✔				
Host					✔	✔	✔	✔
Domain			✔					
Port					✔	✔		
Description	✔	✔	✔	✔	✔	✔	✔	✔
Password						✔		
SSO Credentials	✔	✔	✔	✔				
SSL-VPN Login	✔	✔	✔	✔				
SSO Form Data	✔							
Form Key	✔							
Form Value	✔							
Alternative	✔	✔	✔	✔				
Username	✔	✔	✔	✔				
Password	✔	✔	✔	✔				
Use SSL-VPN Credentials					✔			
Username					✔			
Password					✔			
*Color Depth Per Pixel**					✔			
*Screen Width**					✔			
*Screen Height**					✔			

Setting	HTTP/ HTTPS	FTP	SMB	SFTP	RDP	VNC	SSH	Telnet
Keyboard Layout					✔			
Security					✔			
Preconnection ID					✔			
Preconnection Blob					✔			
Load Balancing Information					✔			
Restricted Admin Mode					✔			

* = This setting can only be configured by an administrator.

To create a user bookmark in the web portal:

1. In the *Personal Bookmarks* section, click *Create new bookmark*.
2. Enter a *Name*.
3. Select a bookmark type and configure the type-based settings.
4. Click *Save*.

To create a predefined administrator bookmark in FortiOS:

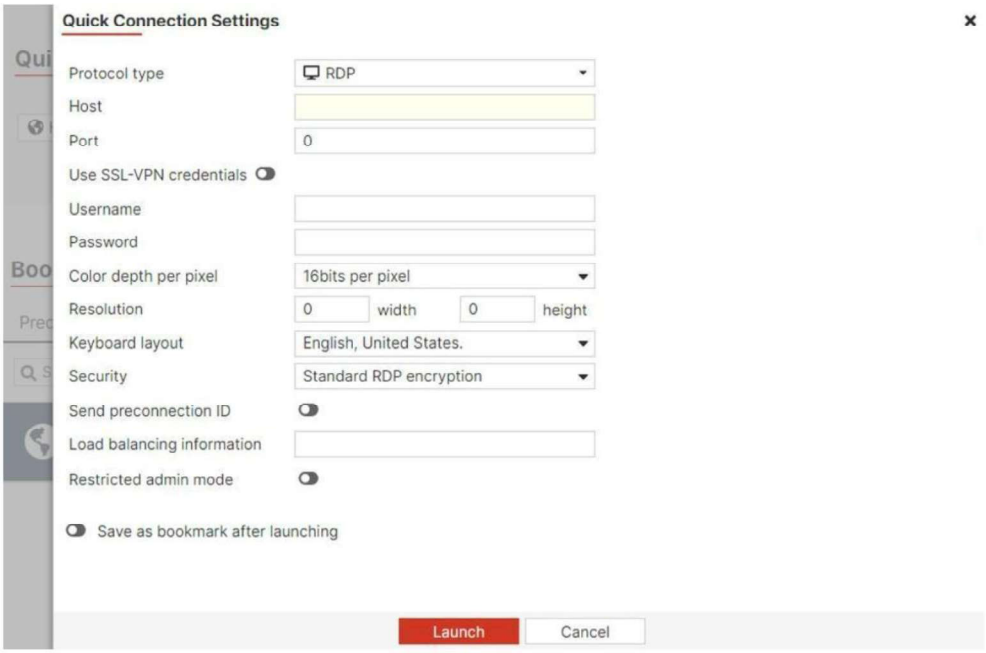
1. Go to *VPN* > *SSL-VPN Portals* and double-click a portal to edit it.
2. In the *Predefined Bookmarks* table, click *Create New*. The *New Bookmark* pane appears.
3. Enter a *Name*.
4. Select a bookmark type and configure the type-based settings.
5. Click *OK* to save the bookmark settings.
6. Click *OK* to save the portal settings.

SCENARIO 9 Quick Connection tool

The ***Quick Connection*** tool allows a user to connect to a resource when it is not a predefined bookmark. The tool allows the user to specify the type of server and the URL or IP address of the host.

To connect to a resource:

1. Select the connection type.
2. Enter the required information, such as the IP address or URL of the host.
3. Click *Configure & launch*.



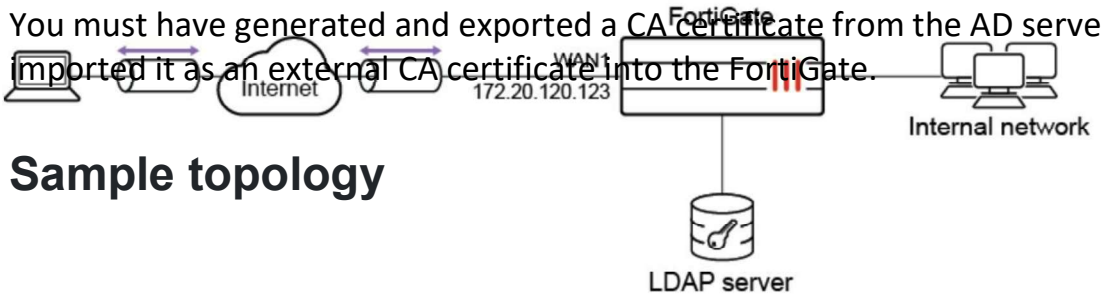
In a VNC session, to send Ctrl+Alt+Del, press *F8* then select *Send Ctrl-Alt-Delete*.

SCENARIO 10 SSL VPN with LDAP user authentication

This is a sample configuration of SSL VPN for LDAP users. In this example, the LDAP server is a Windows 2012 AD server. A user *ldu1* is configured on Windows 2012 AD server.

You must have generated and exported a CA certificate from the AD server and then have imported it as an external CA certificate into the FortiGate.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

To configure SSL VPN using the GUI:

1. **Configure the interface and firewall address. The port1 interface connects to the internal network:**
   A. Go to *Network* > *Interfaces* and edit the *wan1* interface.
   B. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
   C. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
   D. Click *OK*.
   E. Go to *Policy & Objects* > *Address* and create an address for internet subnet *192.168.1.0*.

2. Import CA certificate into FortiGate:

A. Go to *System* > *Features Visibility* and ensure *Certificates* is enabled.

B. Go to *System* > *Certificates* and select *Import* > *CA Certificate*.

C. Select *Local PC* and then select the certificate file.

The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA_Cert_1*.

D. If you want, you can use CLI commands to rename the system-generated *CA_Cert_1* to be more descriptive:

```
config vpn certificate ca
    rename CA_Cert_1 to LDAPS-CA
end
```

3. Configure the LDAP user:

A. Go to *User & Authentication* > *LDAP Servers* and click *Create New*.

B. Specify *Name* and *Server IP/Name*.

C. Specify *Common Name Identifier* and *Distinguished Name*.

D. Set *Bind Type* to *Regular*.

E. Specify *Username* and *Password*.

F. Enable *Secure Connection* and set *Protocol* to *LDAPS*.

G. For *Certificate*, select *LDAP server CA LDAPS-CA* from the list.

4.Configure user group:

A. Go to *User & Authentication* > *User Groups* to create a user group.

B. Enter a *Name*.

C. In *Remote Groups*, click *Add* to add *ldaps-server*.

5.Configure SSL VPN web portal:

A. Go to *VPN* > *SSL-VPN Portals* to edit the *full-access* portal.

This portal supports both web and tunnel mode.

B. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.

6.Configure SSL VPN settings:

A. Go to *VPN* > *SSL-VPN Settings*.

B. Select the *Listen on Interface(s)*, in this example, *wan1*.

C. Set *Listen on Port* to *10443*.

D. Set *Server Certificate* to the authentication certificate.

E. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.

F. Create new *Authentication/Portal Mapping* for group *ldaps-group* mapping portal *full-access*.

7.Configure SSL VPN firewall policy:

A. Go to *Policy & Objects* > *Firewall Policy*.

B. Fill in the firewall policy name, in this example, *sslvpn certificate auth*.

C. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.

D. Set the *Source Address* to *all* and *Source User* to *ldaps-group*.

E. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network, in this example, *port1*.

F. Set *Destination Address* to the internal protected subnet *192.168.1.0*.

G. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.

H. Enable *NAT*.

I. Configure any remaining firewall and security options as desired.

J. Click *OK*.

To configure SSL VPN using the CLI:

1. Configure the interface and firewall address:

```
config system interface
    edit "wan1"
       set vdom "root"
        set ip 172.20.120.123 255.255.255.0
    next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network:

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
    next
end
config firewall address
    edit "192.168.1.0"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

3. Import CA certificate into FortiGate:

A. Go to *System* > *Features Visibility* and ensure *Certificates* is enabled.

B. Go to *System* > *Certificates* and select *Import* > *CA Certificate*.

C. Select *Local PC* and then select the certificate file.

The CA certificate now appears in the list of *External CA Certificates*. In the example, it is called *CA_Cert_1*.

D. If you want, you can use CLI commands to rename the system-generated *CA_Cert_1* to be more descriptive:

```
config vpn certificate ca
    rename CA_Cert_1 to LDAPS-CA
end
```

4. Configure the LDAP server:

```
config user ldap
    edit "ldaps-server"
        set server "172.20.120.161"
        set cnid "cn"
        set dn "cn=Users,dc=qa,dc=fortinet,dc=com"
        set type regular
        set username
"CN=Administrator,cn=users,DC=qa,DC=fortinet,DC=com"
        set password **********
        set group-member-check group-object
        set secure ldaps
        set ca-cert "LDAPS-CA"
        set port 636
    next
end
```

5. Configure user group:

```
config user group
    edit "ldaps-group"
        set member "ldaps-server"
    next
end
```

6. **Configure SSL VPN web portal:**

```
config vpn ssl web portal
    edit "full-access"
        set tunnel-mode enable
        set web-mode enable
        set ip-pools "SSLVPN_TUNNEL_ADDR1"
        set split-tunneling disable
     next
end
```

7. **Configure SSL VPN settings:**

```
config vpn ssl settings
    set servercert "server_certificate"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set source-interface "wan1"
    set source-address "all"
    set default-portal "web-access"
    config authentication-rule
        edit 1
            set groups "ldaps-group"
            set portal "full-access"
        next
    end
end
```

8. **Configure one SSL VPN firewall policy to allow remote user to access the internal network:**

```
config firewall policy
    edit 1
        set name "sslvpn web mode access"
        set srcintf "ssl.root"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "192.168.1.0"
        set groups "ldaps-group"
        set action accept
        set schedule "always"
```

```
            set service "ALL"
            set nat enable
        next
    end
```

To see the results of web portal:

1. From a remote device, use a web browser to log into the SSL VPN web portal *http://172.20.120.123:10443*.
2. Enter the *ldu1* user credentials, then click *Login*.
3. Go to *Dashboard* > *Network* and expand the *SSL-VPN* widget to verify the user's connection.

To see the results of tunnel connection:

1. Download FortiClient from www.forticlient.com.
2. Open the FortiClient Console and go to *Remote Access* > *Configure VPN*.
3. Add a new connection:
   A. Set the connection name.
   B. Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
   C. Select *Customize Port* and set it to *10443*.
4. Save your settings.
5. Log in using the *ldu1* credentials.

To check the SSL VPN connection using the GUI:

1. Go to *Dashboard* > *Network* and expand the *SSL-VPN* widget to verify the user's connection.
2. Go to *Log & Report* > *System Events* and select the *VPN Events* card to view the details of the SSL VPN connection event log.
3. Go to *Log & Report* > *Forward Traffic* to view the details of the SSL VPN traffic.

To check the web portal login using the CLI:

```
# get vpn ssl monitor
SSL VPN Login Users:
 Index   User    Auth Type    Timeout    From           HTTP in/out HTTPS in/out
 0       ldu1    1(1)         229        10.1.100.254   0/0          0/0

SSL VPN sessions:
 Index   User    Source IP      Duration        I/O Bytes       Tunnel/Dest IP
```

To check the tunnel login using the CLI:

```
# get vpn ssl monitor
SSL VPN Login Users:
 Index   User    Auth Type    Timeout    From           HTTP in/out HTTPS in/out
 0       ldu1    1(1)         291        10.1.100.254   0/0          0/0

SSL VPN sessions:
 Index   User    Source IP      Duration    I/O Bytes      Tunnel/Dest IP
 0       ldu1    10.1.100.254   9           22099/43228    10.212.134.200
```

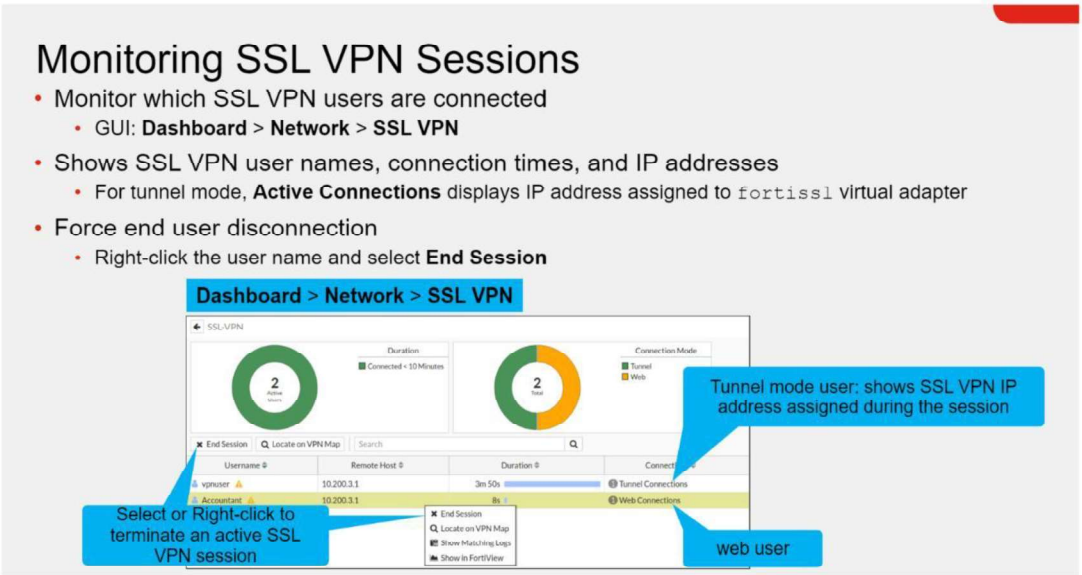
SSL VPN Protocols

1. **TLS 1.3 support**

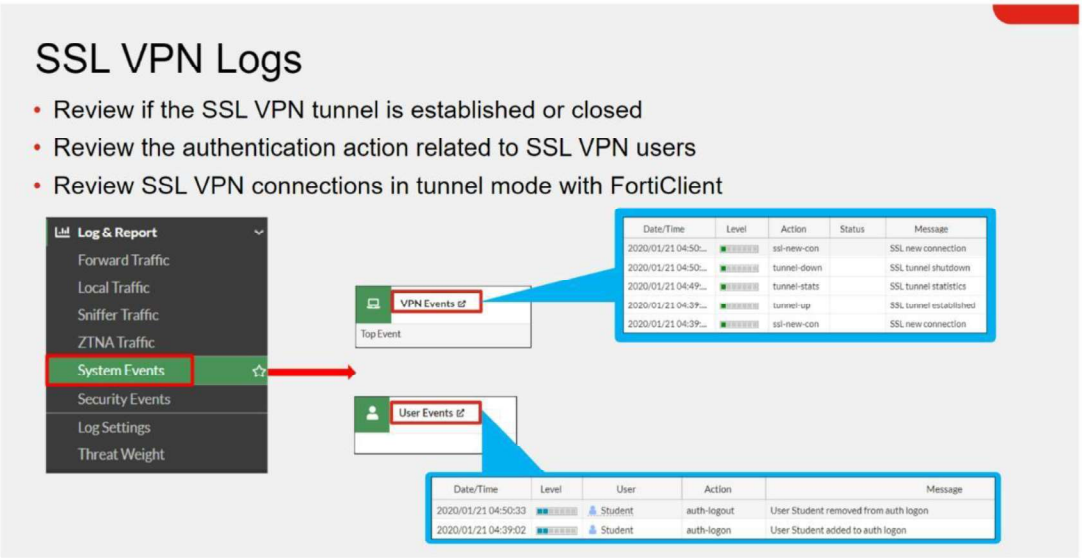
2. **SMBv2 support** On all FortiGate models, SMBv2 is enabled by default for SSL VPN. Client PCs can access the SMBv2 server using SSL VPN web-only mode.
3. **DTLS support** FortiOS Datagram Transport Layer Security (DTLS) allows SSL VPN to encrypt traffic using TLS and uses UDP as the transport layer instead of TCP. This avoids retransmission problems that can occur with TCP-in-TCP.

Monitoring SSL VPN Sessions

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.



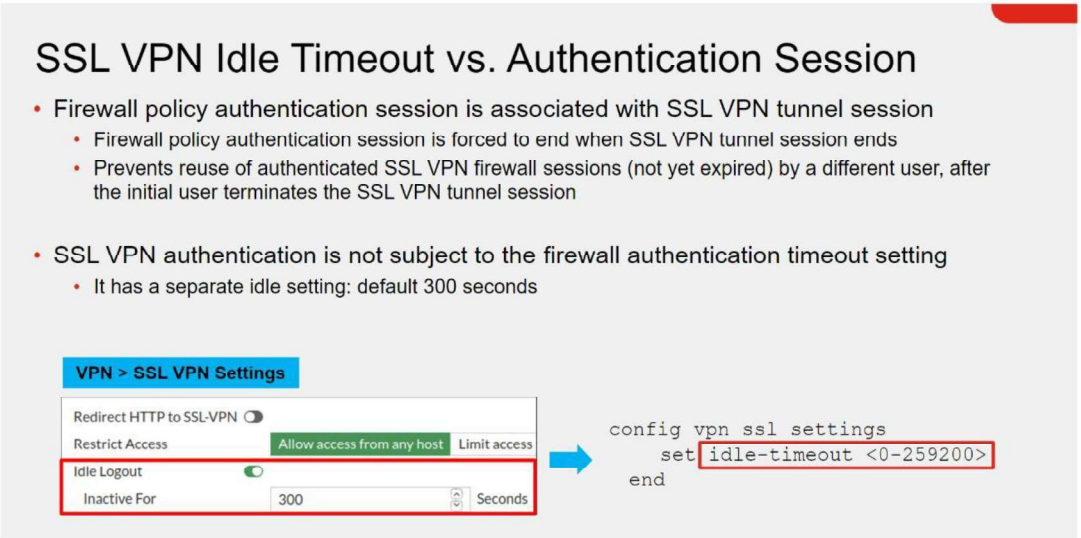
SSL VPN Logs



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.

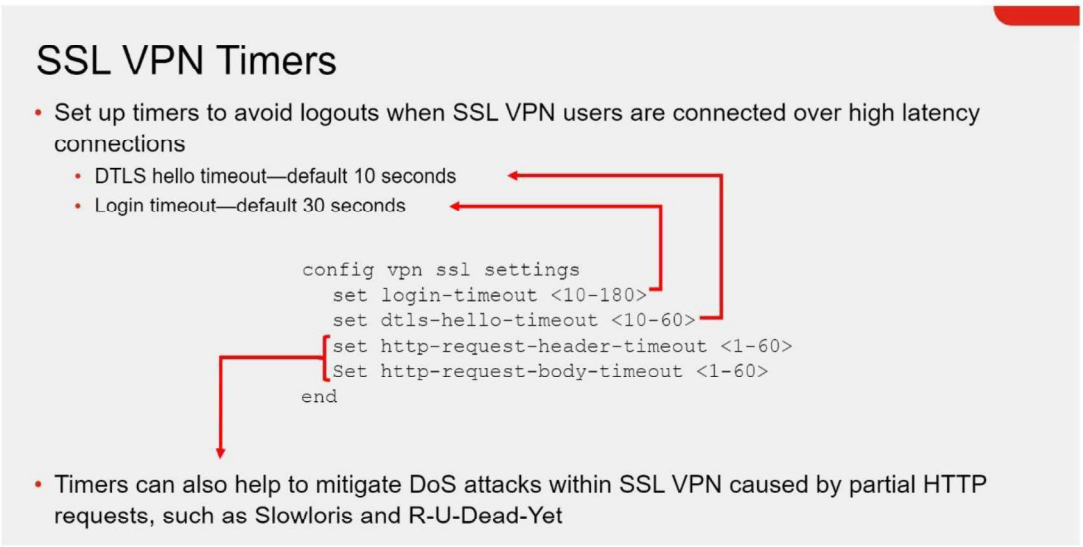
SSL VPN Idle Timeout vs. Authentication Session



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.

SSL VPN Timers

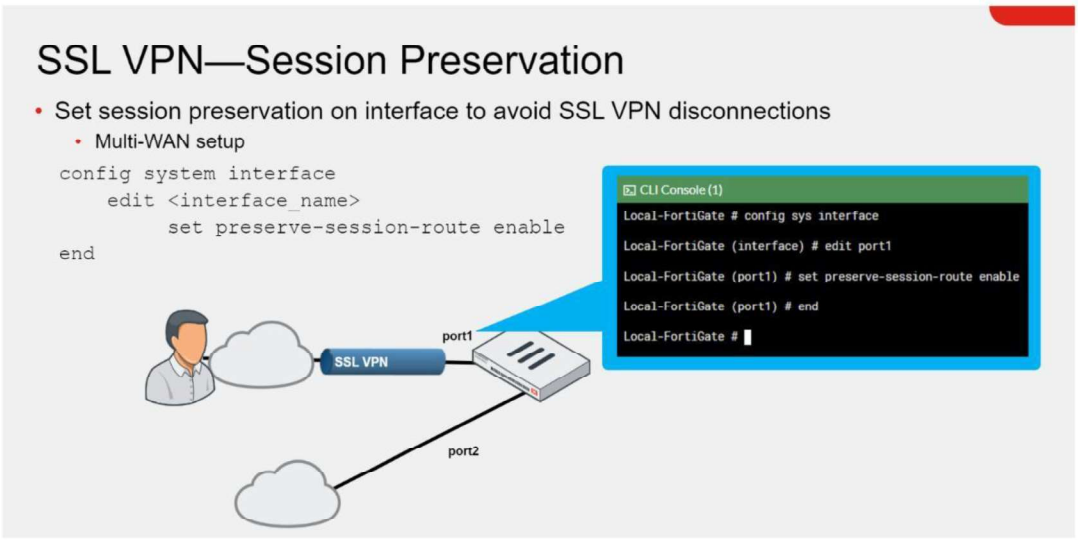


When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under **`config vpn ssl settings`**have been added to address this.

- 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 Prevention



In the typical enterprise network, there can be multiple WAN links. In the FortiGate, by default, any session with source NAT disabled goes 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.

Let's break down the explanation of the routing behavior in FortiGate in simpler terms:

The Scenario

In a typical enterprise network, you might have multiple WAN links (Internet connections) for redundancy or load balancing. For example:

- **WAN1 (port1)** might be your primary Internet connection.
- **WAN2 (port2)** could be a backup Internet connection.

FortiGate's Routing Behavior

- **Routing Table:** FortiGate uses a routing table to decide which interface (WAN link) to send traffic through.
- **Sessions:** When a new connection (session) is made, FortiGate checks the routing table to determine the best interface to use.

Problem with Route Changes in Multi-WAN Setup

- In a multi-WAN setup, the routing table can change due to:
  - **Link failures** (if WAN1 goes down, WAN2 becomes the primary).
  - **Load balancing** (traffic can be shared across both WAN1 and WAN2).
- When the routing table changes, FortiGate will **reevaluate existing sessions** if **source NAT (SNAT)** is **disabled**. This is called marking sessions "dirty" because the routing might need to be updated.
- As a result, a session could start on **WAN1 (port1)** and then, due to a routing change, **WAN2 (port2)** might become the new preferred path.
  - **Issue:** This can cause a situation where a request comes in from one interface (WAN1), but the response goes out through a different interface (WAN2). Many applications don’t handle this well, leading to connection drops.

Solution: set preserve-session-route

The command **set preserve-session-route** tells FortiGate to keep existing sessions on the same interface even if the routing table changes.

- **How it works:** When you enable this setting, FortiGate "locks" the session to the original interface it started on.

- For example, if an SSL VPN session was initiated through **WAN1 (port1)**, it will continue to use **WAN1 (port1)** even if **WAN2 (port2)** becomes the preferred route due to a routing change.
- This prevents issues where requests and responses go through different interfaces, thus avoiding disconnections.

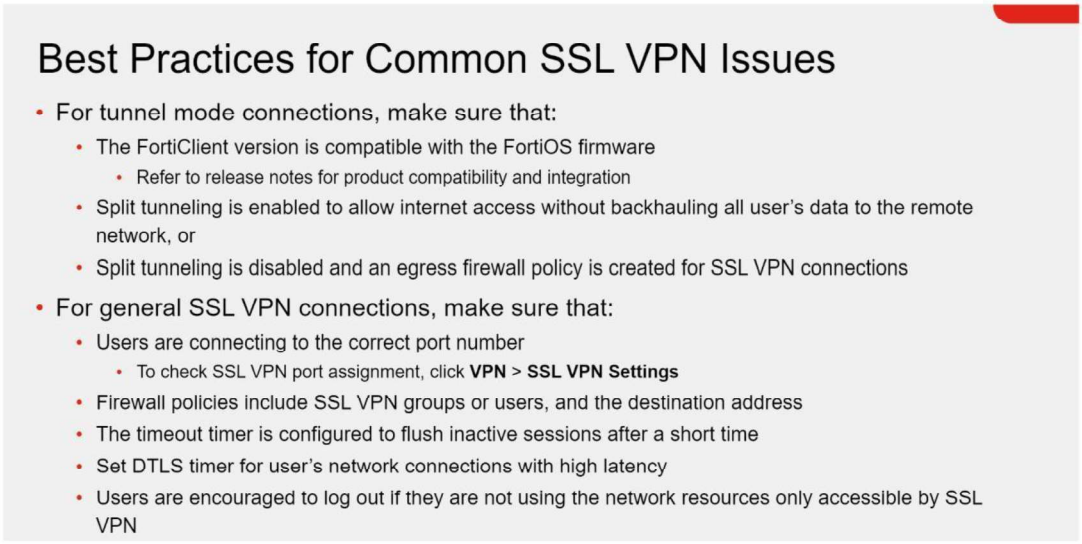
Example Explained

1. **Scenario:**
   - Port1 is reserved for SSL VPN connections.
   - Port2 is used for other services.
2. **Routing Change:**
   - If port2 becomes the primary connection (perhaps because port1 fails or load balancing changes the preference), FortiGate would, by default, try to route new sessions through port2.
3. **With set preserve-session-route Enabled:**
   - The existing SSL VPN sessions that started on port1 will continue to stay on port1, even if port2 becomes the primary connection.
   - This ensures that users with ongoing SSL VPN connections don't get disconnected due to the routing change.

Summary

The **set preserve-session-route** command ensures that once a session starts on a specific interface, it stays on that interface even if the routing table changes. This is especially important in multi-WAN setups to avoid connection issues when routing changes occur.

Best Practices for Common SSL VPN Issues

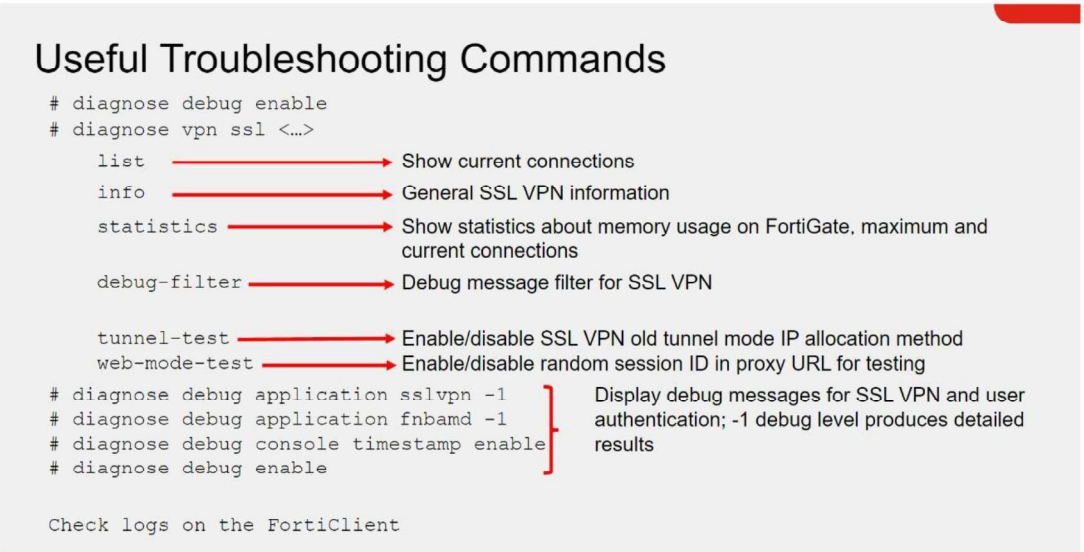


The following are some best practices to keep in mind when using SSL VPNs. These best practices can also be helpful in many SSL VPN troubleshooting situations:

- 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
- Select the appropriate SSL VPN mode: It may be possible that your users need only one of the SSL VPN modes. Use SSL VPN portals with the unused SSL mode disabled.
- Reduce administrative effort by using remote authentication servers: Avoid using local users if possible. Having a centralized authentication solution saves time and prevents human errors. This is especially true in bigger environments.
- Use a valid SSL certificate: Replace the default self-signed certificate with another one that is trusted by your users' devices. You can purchase a certificate from a trusted vendor, or you can implement your own PKI infrastructure to achieve this.

- Use the principle of least privilege when configuring firewall policies for VPN traffic: This is true for any firewall policy, but it is especially important when you are allowing remote devices to connect to your network.
- Use the client integrity check: For Windows clients, always verify that they have antivirus software, firewall software, or both, installed.
- If possible, do not allow connections from all locations: This is not always feasible, but it is ideal to restrict access to connection requests from specific public IP addresses trusted by your organization.

SSL VPN – Useful Troubleshooting Commands



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.

Lab

Configuring SSL VPN Tunnel Mode

In this lab, you will examine how to configure an SSL VPN connection in tunnel mode. You will also manage user groups and portals for an SSL VPN.

Objectives

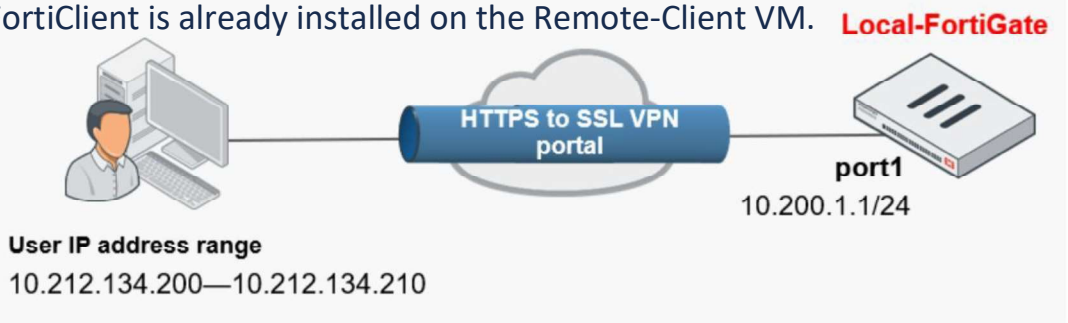
- Configure and connect to an SSL VPN
- Enable authentication security
- Configure a firewall policy for SSL VPN users to access private network resources
- Configure FortiClient for the SSL VPN connection in tunnel mode

Configuring SSL VPN Tunnel Mode

In this exercise, you will examine how to change the SSL VPN settings to allow remote access to the resources in the local subnet (10.0.1.0/24), but perform a connection in tunnel mode from the Remote-Client VM.

You will use the remote access module of FortiClient, which supports the Fortinet SSL VPN client.

FortiClient is already installed on the Remote-Client VM.



Configure the SSL VPN Settings

You will configure the SSL VPN settings to allow the remote connection shown in the following image:

By default, SSL VPN tunnel mode settings and the **VPN** > **SSL-VPN** menus are hidden on the GUI in FortiOS version 7.4. To enable the GUI menu, enter the following CLI commands:

```
config system settings

set gui-sslvpn enable

end
```

The configuration file is preconfigured for you to show the SSL VPN menus.

To create a user for SSL VPN connections:

1. Connect to the Local-FortiGate GUI.
2. Click **User & Authentication** > **User Definition**.
3. Click **Create New**.
4. Click **Local User**, and then click **Next**.
5. Type the following credentials for the remote user, and then click **Next**:

Username	student
Password	fortinet

6. Leave the contact information field empty, and then click **Next**.
7. In the **User Account Status** field, verify that **Enabled** is selected.
8. Enable **User Group**, click **+**, and then in the section on the right, select **SSL_VPN_USERS**.
9. Click **Submit**.

The **SSL_VPN_USERS** group was preconfigured for this lab.

To review the settings of this group, click **User & Authentication** > **User Groups**.

To configure the SSL VPN settings for access:

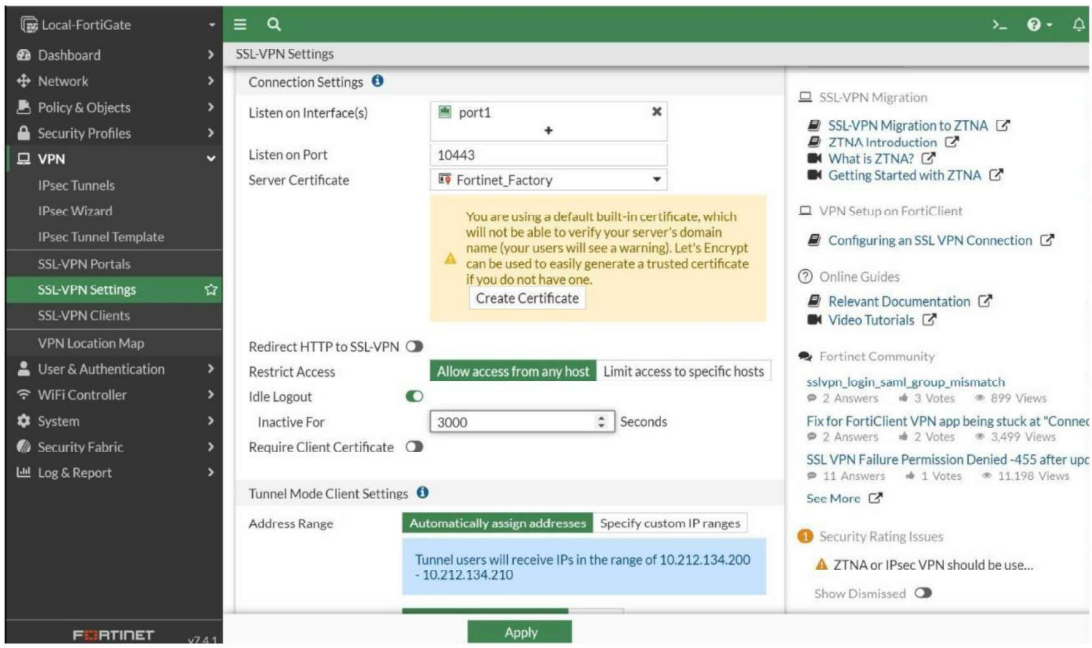
1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Settings**.

2. In the **Connection Settings** section, configure the following settings:

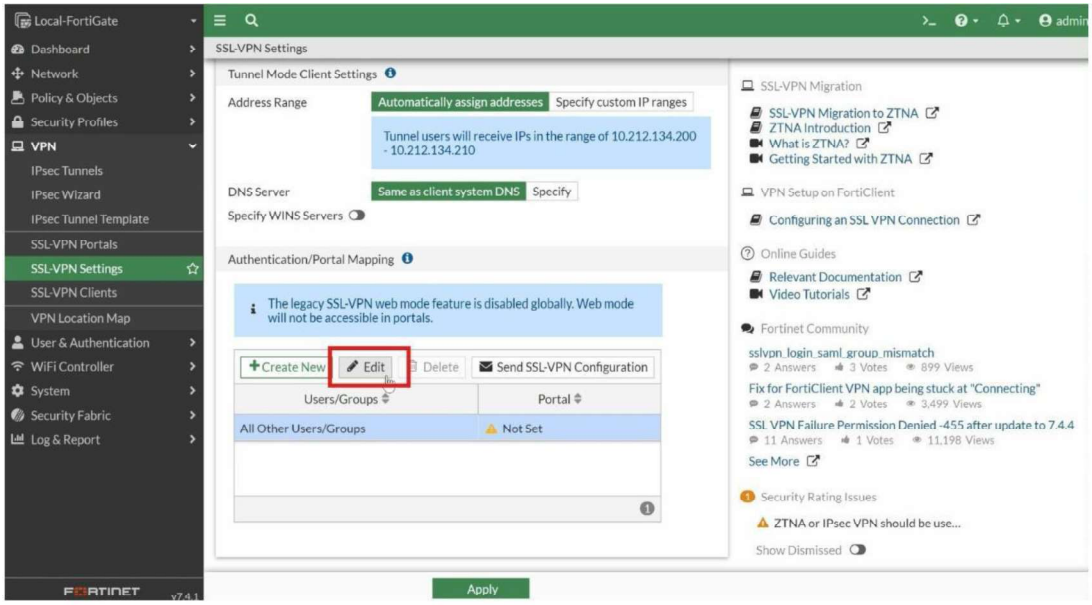
Field	Value
Listen on Interface(s)	port1
Listen on Port	10443
Server Certificate	Fortinet_Factory
Restrict Access	Allow access from any host
Inactive For	3000 seconds

3. In the **Tunnel Mode Client Settings** section, verify the following setting:

Field	Value
Address Range	Automatically assign addresses

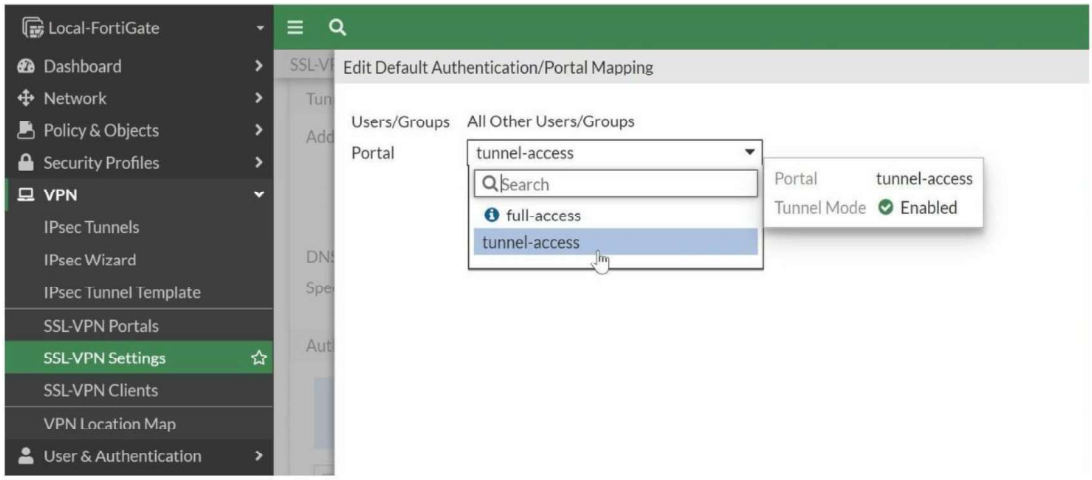


4. In the **Authentication/Portal Mapping** section, select **All Other Users/Groups**, and then click **Edit**.



5. In the **Portal** field, select **tunnel-access**, and then click **OK**.

6. Click **Apply** to save the changes.



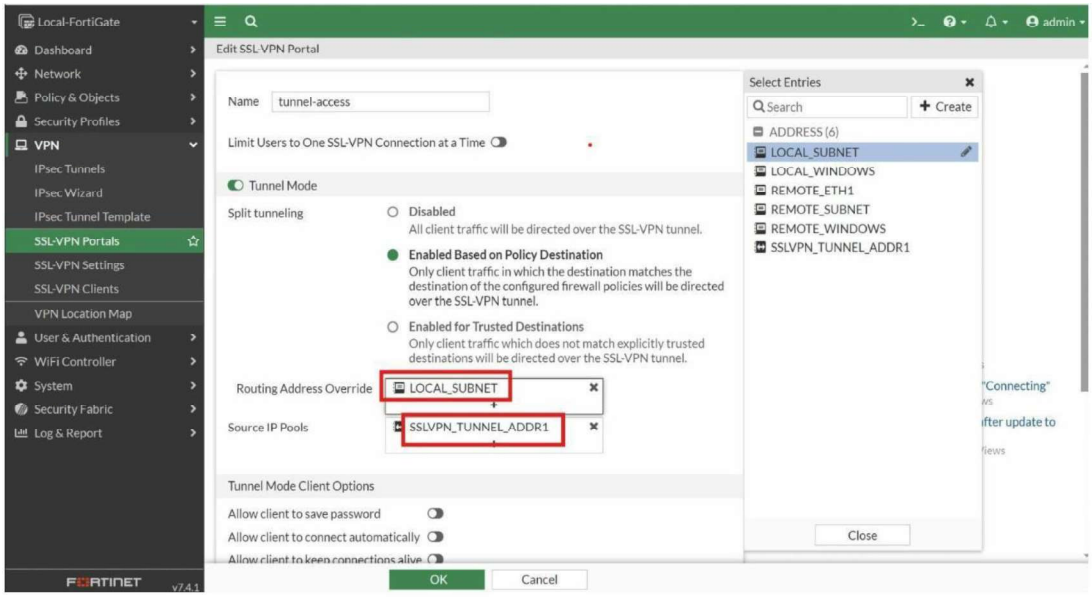
Configure the Routing for Tunnel Mode

You will establish the routing address to use in tunnel mode.

In tunnel mode, FortiClient establishes one or more routes in the SSL VPN user's host after the tunnel is connected. Traffic destined to the internal subnets is correctly routed through the tunnel.

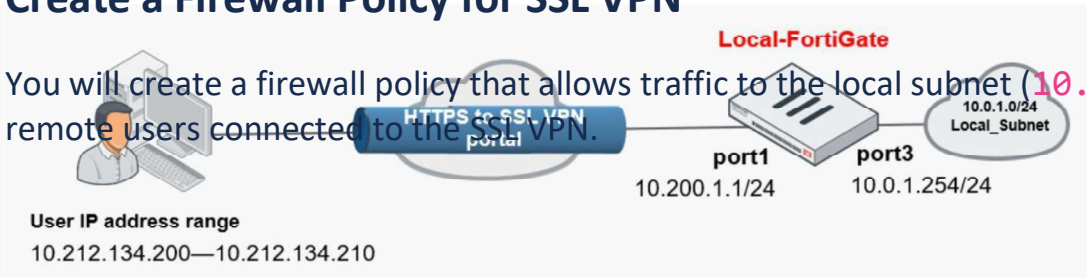
To configure the routing for tunnel mode:

1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Portals**.
2. Select the **tunnel-access** portal, and then click **Edit**.
3. In the **Tunnel Mode** section, in the **Routing Address Override** field, select **LOCAL_SUBNET**.



4. Click **OK**.

Create a Firewall Policy for SSL VPN



You will create a firewall policy that allows traffic to the local subnet (10.0.1.0/24) from remote users connected to the SSL VPN.

To create a firewall policy for SSL VPN:

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then configure the following firewall policy settings:

Field	Value
Name	SSL-VPN-Access
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port3
Source	Address > SSLVPN_TUNNEL_ADDR1 User > SSL_VPN_USERS
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT
Inspection mode	Flow-based
NAT	Disabled

3. Click **OK** to save the configuration.

Configure FortiClient for SSL VPN Connections

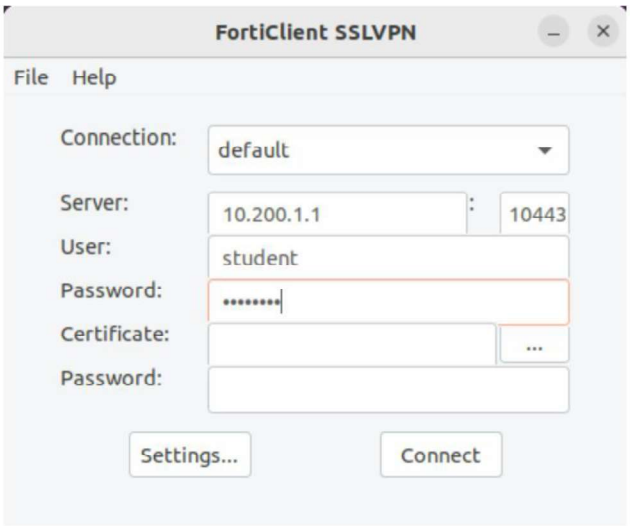
SSL VPN connections in tunnel mode require FortiClient. You will use FortiClient, which is installed on the Remote-Client VM, to test your configuration.

To configure FortiClient for SSL VPN in tunnel mode:

1. Connect to the Remote-Client VM.
2. Click **Desktop** > **forticlientsslvpn** > **64bit**, and then double-click **forticlientsslvpn** to configure SSL VPN client settings.
3. Configure the following settings for the FortiClient SSL VPN application:

Field	Value
Server	10.200.1.1
Customize port	10443

4. Continuing on the FortiClient SSL VPN application, in the **User** field, type `student`, and then in the **Password** field, type `fortinet`.



5. Click **Connect**.
6. Click **Continue** to accept the certificate.

The tunnel is connected.

To test the tunnel:

1. Continuing on the Remote-Client VM, open Firefox, and then access the following URL:

http://10.0.1.10

2. Look at the URL.

You are connected to the web server URL as if you were based in the local subnet (`10.0.1.0/24`).

Monitor an SSL VPN User

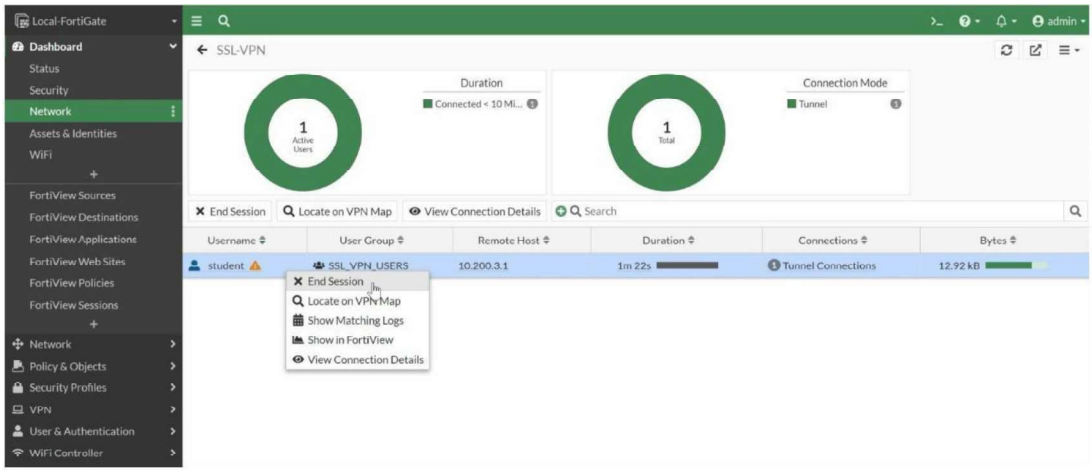
You will monitor and disconnect an SSL VPN user from the FortiGate GUI.

To monitor and disconnect an SSL VPN user:

1. Return to the Local-FortiGate GUI.
2. Click **Dashboard** > **Network**, and then view the **SSL-VPN** widget.

You can see that the student user is connecting from the remote host `10.200.3.1`.

3. Right-click **student**, and then select **End Session**.
4. Click **OK**.



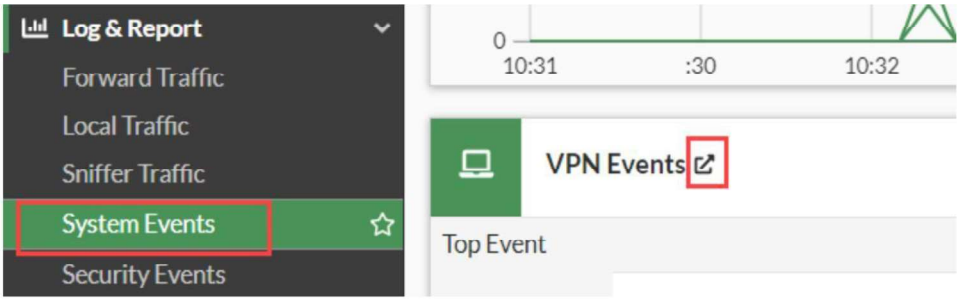
The student user no longer appears in the SSL VPN monitor.

Review VPN Events

You will review the VPN events for the SSL VPN connection you performed in this lab.

To review VPN events for the SSL VPN connection:

1. Connect to the Local-FortiGate GUI.
2. Click **Log & Report** > **System Events**, and then expand the **VPN Events** widget to view the logs.



3. View the log details of the **tunnel-up** log you see.

Hint: Use your log filters to filter on **Action** = **tunnel-up**.

The **tunnel-up** log in the VPN event list shows the SSL VPN connection in tunnel mode through FortiClient. Notice this log displays two IP addresses:

- **Remote IP**: IP address of the remote user's gateway (egress interface)
- **Tunnel IP**: IP address FortiGate assigns to the virtual network adapter `fortissl`