FortiOS™ Handbook - SSL VPN

VERSION 5.6.7

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdoc@fortinet.com

March 15, 2019

FortiOS™ Handbook - SSL VPN

01-564-112804-20180813

TABLE OF CONTENTS

Change log

Date	Change description
March 15, 2019	Minor updates.
January 30, 2019	ForitOS 5.6.7 document release. Minor updates.
2018-04-26	FortiOS 5.6.4 document release.

SSL VPN

This document provides a general introduction to SSL VPN technology, explains the features available with SSL VPN and gives guidelines to decide what features you need to use, and how the FortiGate unit is configured to implement the features.

The following chapters are included in this document:

Overview provides useful general information about VPN and SSL, how the FortiGate unit implements them, and gives guidance on how to choose between SSL and IPsec.

Basic configuration explains how to configure the FortiGate unit and the web portal. Along with these configuration details, this chapter also explains how to grant unique access permissions, how to configure the SSL encryption key algorithm, and describes the SSL VPN OS Patch Check feature that allows a client with a specific OS patch to access SSL VPN services.

The SSL VPN client provides an overview of the FortiClient software required for tunnel mode, where to obtain the software, how to install it, and the configuration information required for remote users to connect to the internal network.

The SSL VPN web portal provides an overview of the SSL VPN web portal, with explanations of how to use and configure the web portal features.

Setup examples explores several configuration scenarios with step-by-step instructions. While the information provided is enough to set up the described SSL VPN configurations, these scenarios are not the only possible SSL VPN setups.

Troubleshooting provides some general maintenance and troubleshooting procedures for SSL VPNs.

What's new in FortiOS 5.6

This chapter describes new SSL VPN features added to FortiOS 5.6.

FortiOS 5.6.4

These features first appeared in FortiOS 5.6.4.

- "Tunnel Mode Client Options logic" on page 28
- " HTTP header information" on page 77

FortiOS 5.6.3

These features first appeared in FortiOS 5.6.3.

Virtual desktop option no longer supported (442044)

The SSL VPN web portal no longer supports the virtual desktop and its option has been removed from the interface.

Option to disable FortiClient download in web portal (439736)

You can use the following commands to enable or disable allowing SSL VPN users to download FortiClient from the SSL VPN web portal. If `forticlient-download` is enabled, you can select the download method (`direct` or over the `ssl_vpn`). You can also optionally specify a custom URL for downloading the Windows and Mac OS versions of FortiClient.

Syntax

```
config vpn ssl web portal
   edit <portal name>
      set forticlient-download {enable | disable}
      set forticlient-download-method {direct | ssl-vpn}
      set customize-forticlient-download-url {enable | disable}
      set windows-forticlient-download-url <url>
      set macos-forticlient-download-url <url>
   end
```

Upgraded OpenSSL to 1.1.x (412033) (...)

OpenSSL has been upgraded to 1.1 to provide more cryptographic algorithms. All 3rd-party libraries that depend on OpenSSL have also been updated. OpenLDAP has been upgraded to 2.4.45 to be compatible with OpenSSL 1.1. Furthermore, the `sslv3` attribute has been removed from `vpn.ssl.settings` and `global.admin-https-ssl-version`.

FortiOS 5.6.1

These features first appeared in FortiOS 5.6.1.

Added a button to send Ctrl-Alt-Delete to the remote host for VNC and RDP desktop connections (401807)

Previously, users were unable to send **Ctrl-Alt-Delete** to the host machine in an SSL VPN remote desktop connection.

FortiOS 5.6.1 adds a new button that allows users to send **Ctrl-Alt-Delete** in remote desktop tools (also fixes 412456, preserving the SSL VPN realm after session timeout prompts a logout).

Improved SSL VPN Realms page (0392184)

Implemented minor functional changes to the dialog on the **SSL VPN > Realms** page:

- URL preview uses info message similar to that seen on the SSL VPN settings dialog.
- Virtual-Host input is now visible when set in the CLI.
- Added help tooltip describing what the virtual-host property does.

Customizable FortiClient Download URL in SSL VPN Web Portal (437883)

A new attribute, `customize-forticlient-download-url`, is added to vpn.ssl.web.portal.

The added attribute indicates whether to support a customizable download URI for FortiClient. This attribute is disabled by default. If enabled, two other attributes, `windows-forticlient-download-url` and `macos-forticlient-download-url`, will appear through which the user can customize the download URL for FortiClient.

Syntax

```
config vpn ssl web portal
   edit <portal>
      set customize-forticlient-download-url {enable | disable}
      set windows-forticlient-download-url <custom URL for Windows>
      set macos-forticlient-download-url <custom URL for Mac OS>
   next
end
```

SSL VPN SSO Support for HTML5 RDP (417248)

This feature adds support for SSO from the SSL VPN portal to an RDP bookmark. If SSO is used, then the credentials used to login to SSL VPN will be automatically used when connecting to a remote RDP server.

Syntax

```
conf vpn ssl web user-bookmark
   edit <name>
      config bookmarks
         edit <name>
```

```
            set apptype rdp
            set host "x.x.x.x"
            set port <value>
            set sso [disable | auto]
         next
      end
   next
end
```

FortiOS 5.6.0

These features first appeared in FortiOS 5.6.0.

Remote desktop configuration changes (410648)

If NLA security is chosen when creating an RDP bookmark, a username and password must be provided. However there may be instances where the user might want to use a blank password, despite being highly unrecommended. If a username is provided but the password is empty, the CLI will display a warning. See example CLI below, where the warning appears as a caution before finishing the command:

```
config vpn ssl web user-group-bookmark
   edit <group-name>
      config bookmarks
         edit <bookmark-name>
            set apptype rdp
            set host 172.16.200.121
            set security nla
            set port 3389
            set logon-user <username>
         next
      end
Warning: password is empty. It might fail user authentication and remote desktop
    connection would be failed.
end
```

If no username (`logon-user`) is specified, the following warning message will appear:

```
Please enter user name for RDP security method NLA. object set operator error, -2010
    discard the setting Command fail. Return code -2010
```

SSL VPN supports WAN link load balancing interface (396236)

This new feature allows you to set `virtual-wan-link` as the destination interface in a firewall policy (when SSL VPN is the source interface) for WAN link load balancing in the GUI and in the CLI. This lets you log into a FortiGate via SSL VPN for traffic inspection and then have outbound traffic load balanced by WAN link load balancing.

Syntax

```
config firewall policy
   edit <example>
      set dstintf virtual-wan-link
end
```

SSL VPN login timeout to support high latency (394583)

With long network latency, the FortiGate can timeout the client before it can finish negotiation processes, such as DNS lookup and time to enter a token. Two new CLI commands under `config vpn ssl settings` have been added that allow the login timeout to be configured, replacing the previous hard timeout value. The second command can be used to set the SSL VPN maximum DTLS hello timeout.

Syntax

```
config vpn ssl settings
   edit <example>
      set login-timeout [10-180] Default is 30 seconds.
      set dtls-hello-timeout [10-60] Default is 10 seconds.
end
```

SSL VPN supports Windows 10 OS check (387276)

A new CLI field has been added to the `os-check-list` under `config vpn ssl web portal` to allow OS checking for Windows 10.

Syntax

```
config vpn ssl web portal
   edit <example>
   set os-check enable
   config os-check-list windows-10
      set action {deny | allow | check-up-to-date}
   end
end
```

SSL VPN DNS suffix per portal and number of portals (383754)

A new CLI command under `config vpn ssl web portal` to implement a DNS suffix per SSL VPN portal. Each suffix setting for each specific portal will override the `dns-suffix` setting under `config vpn ssl settings`.

This feature also raises bookmark limits and the number of portals that can be supported, depending on what FortiGate series model is used:

- 650 portals on 1000D series
- 1300 portals on 2000E series
- 2600 portals on 3000D series

The previous limit for 1000D series models, for example, was 256 portals.

Syntax

```
config vpn ssl web portal
   edit <example>
      set dns-suffix <string>
end
```

New SSL VPN timeout settings (379870)

New SSL VPN timeout settings have been introduced to counter 'Slowloris' and 'R-U-Dead-Yet' vulnerabilities that allow remote attackers to cause a denial of service via partial HTTP requests.

The FortiGate solution is to add two attributes (`http-request-header-timeout` and `http-request-body-timeout`).

Syntax

```
config vpn ssl settings
   set http-request-header-timeout [1-60] (seconds)
   set http-request-body-timeout [1-60] (seconds)
end
```

Personal bookmark improvements (377500)

You can now move and clone personal bookmarks in the GUI and CLI.

Syntax

```
config vpn ssl web user-bookmark
   edit 'name'
      config bookmarks
      move bookmark1 after/before
      clone bookmark1 to
   next
end
```

New controls for SSL VPN client login limits (376983)

Removed the limitation of SSL VPN user login failure time, by linking SSL VPN user setting with `config user settings` and provided a new option to remove SSL VPN login attempts limitation. New CLI allows the administrator to configure the number of times wrong credentials are allowed before SSL VPN server blocks an IP address, and also how long the block would last.

Syntax

```
config vpn ssl settings
   set login-attempt-limit [0-10] Default is 2.
   set login-block-time [0-86400] Default is 60 seconds.
end
```

Unrated category removed from ssl-exempt (356428)

The "Unrated" category has been removed from the SSL Exempt/Web Category list.

Clipboard support for SSL VPN remote desktop connections (307465)

A remote desktop clipboard viewer pane has been added which allows user to copy, interact with and overwrite remote desktop clipboard contents.

Overview

As organizations have grown and become more complex, secure remote access to network resources has become critical for day-to-day operations. In addition, businesses are expected to provide clients with efficient, convenient services including knowledge bases and customer portals. Employees traveling across the country or around the world require timely and comprehensive access to network resources. As a result of the growing need for providing remote/mobile clients with easy, cost-effective and secure access to a multitude of resources, the concept of a Virtual Private Network (VPN) was developed.

SSL VPNs establish connectivity using SSL, which functions at Levels 4 - 5 (Transport and Session layers). Information is encapsulated at Levels 6 - 7 (Presentation and Application layers), and SSL VPNs communicate at the highest levels in the OSI model. SSL is not strictly a Virtual Private Network (VPN) technology that allows clients to connect to remote networks in a secure way. A VPN is a secure logical network created from physically separate networks. VPNs use encryption and other security methods to ensure that only authorized users can access the network. VPNs also ensure that the data transmitted between computers cannot be intercepted by unauthorized users. When data is encoded and transmitted over the Internet, the data is said to be sent through a “VPN tunnel”. A VPN tunnel is a non-application oriented tunnel that allows the users and networks to exchange a wide range of traffic regardless of application or protocol.

The advantages of a VPN over an actual physical private network are two-fold. Rather than utilizing expensive leased lines or other infrastructure, you use the relatively inexpensive, high-bandwidth Internet. Perhaps more important though is the universal availability of the Internet. In most areas, access to the Internet is readily obtainable without any special arrangements or long wait times.

SSL (Secure Sockets Layer) as HTTPS is supported by most web browsers for exchanging sensitive information securely between a web server and a client. SSL establishes an encrypted link, ensuring that all data passed between the web server and the browser remains private and secure. SSL protection is initiated automatically when a user (client) connects to a web server that is SSL-enabled. Once the successful connection is established, the browser encrypts all the information before it leaves the computer. When the information reaches its destination, it is decrypted using a secret (private) key. Any data sent back is first encrypted, and is decrypted when it reaches the client.

FortiOS supports the SSL and TLS versions defined below:

SSL and TLS version support table

Version	RFC
SSL 2.0	RFC 6176
SSL 3.0	RFC 6101
TLS 1.0	RFC 2246
TLS 1.1	RFC 4346
TLS 1.2	RFC 5246

SSL VPN modes of operation

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on username, password, and authentication domain. A successful login determines the access rights of remote users according to user group. The user group settings specify whether the connection will operate in web-only mode or tunnel mode.

Web-only mode

Web-only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Sun Java Runtime Environment (note that there is no minimum Java/JRE version requirement—any version of Java/JRE currently supported by the supplier of the Java/JRE for the operating system should work).

Support for SSL VPN web-only mode is built into FortiOS. The feature comprises of an SSL daemon running on the FortiGate unit, and a web portal, which provides users with access to network services and resources including HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP, and SSH.

In web-only mode, the FortiGate unit acts as a secure HTML5 HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal home page and the user can access the server applications behind the FortiGate unit.

When a user starts a connection to a server from the web portal, FortiOS starts the appropriate client application to communicate with the server. All connections to server applications are new connections from the FortiGate to the server. Communication between the FortiGate and the user continues to be over HTML5 HTTPS, so all user communication with the sever is secured by FortiOS. This includes all supported server protocols (HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP, and SSH).

When the FortiGate unit provides services in web-only mode, a secure connection between the remote client and the FortiGate unit is established through the SSL VPN security in the FortiGate unit and the SSL security in the web browser.

FortiGate SSL VPN web portals have a 1- or 2-column page layout and portal functionality is provided through small applets called widgets. Widget windows can be moved or minimized. The controls within each widget depend on its function. There are predefined web portals and the administrator can create additional portals.

Configuring the FortiGate unit involves selecting the appropriate web portal configuration in the user group settings. These configuration settings determine which server applications can be accessed. SSL encryption is used to ensure traffic confidentiality.

See the FortiOS release notes for information about the operating systems and web browsers supported by SSL VPN web-only mode.

Tunnel mode

In Tunnel mode, remote clients connect to a FortiGate unit that acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group.

The SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate unit through an SSL VPN tunnel over the HTTPS link between the user and the FortiGate unit. Another option is split

tunneling, which ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. This conserves bandwidth and alleviates bottlenecks.

When the user initiates a VPN connection with the FortiGate unit through the SSL VPN client, the FortiGate unit establishes a tunnel with the client and assigns the client a virtual IP address from a range of reserved addresses. The client uses the assigned IP address as its source address for the duration of the connection. After the tunnel has been established, the user can access the network behind the FortiGate unit.

Port forwarding mode

While tunnel mode provides a Layer 3 tunnel that users can run any application over, the user needs to install the tunnel client, and have the required administrative rights to do so. In some situations, this may not be desirable, yet the simple web mode does not provide enough flexibility for application support (for example, if you wish to use an email client that communicates with a POP3 server). The port forward mode, or proxy mode, provides this middle ground between web mode and tunnel mode.

SSL VPN port forwarding listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the FortiGate unit, which then forwards the traffic to the application server.

The port forward module is implemented with a Java applet, which is downloaded and runs on the user's computer. The applet provides the up-to-date status information such as addressing and bytes sent and received.

On the user end, the user logs into the FortiGate SSL VPN portal, and selects a port forward bookmark configured for a specific application. The bookmark defines the server address and port as well as which port to listen to on the user's computer.

The user must configure the application on the PC to point to the local proxy instead of the application server. For information on this configuration change, see the application documentation.

This mode only supports client/server applications that are using a static TCP port. It will not support client/server applications using dynamic ports or traffic over UDP.

Application support

With Citrix application servers, the server downloads an ICA configuration file to the user's PC. The client application uses this information to connect to the Citrix server. The FortiGate unit will read this file and append a SOCKS entry to set the SOCKS proxy to 'localhost'. The Citrix client will then be able to connect to the SSL VPN port forward module to provide the connection. When configuring the port forwarding module, a selection is available for Citrix servers.

For Windows Remote Desktop Connections, when selecting the RDP option, the tunnel will launch the RDP client and connect to the local loopback address after the port forward module has been initiated.

Note that the RDP/VNC web portals are **not** supported for the following platforms:

Platform	Model
FortiGate	80D, 92D, 200D, 200D-POE, 240D, 240D-POE, 600C, 800C, 1000C, 3240C, 3600C, and 5001C
FortiGate-Rugged	90D
FortiWiFi	92D

Antivirus and firewall host compatibility

The following tables list the antivirus and firewall client software packages that are supported in FortiOS.

Supported Windows XP antivirus and firewall software

Product supported	Antivirus	Firewall
Symantec Endpoint Protection V11	•	•
Kaspersky Antivirus 2009	•	
McAfee Security Center v8.1	•	•
Trend Micro Internet Security Pro	•	•
F-Secure Internet Security 2009	•	•

Supported Windows 7 32-bit and 64-bit antivirus and firewall software

Product supported	Antivirus	Firewall
CA Internet Security 2011	•	•
AVG Internet Security 2011		
F-Secure Internet Security 2011	•	•
Kaspersky Internet Security 2011	•	•
McAfee Internet Security 2011	•	•
Norton 360TM Version 4.0	•	•
NortonTM Internet Security 2011	•	•
Panda Internet Security 2011	•	•
Sophos Security Suite	•	•

Product supported	Antivirus	Firewall
Trend Micro Titanium Internet Security	•	•
ZoneAlarm Security Suite	•	•
Symantec Endpoint Protection Small Business Edition 12.0	•	•

SSL VPN conserve mode

FortiGate units perform all security profile processing in physical RAM. Since each model has a limited amount of memory, Kernel conserve mode is activated when the remaining free memory is nearly exhausted or the AV proxy has reached the maximum number of sessions it can service.

SSL VPN also has its own conserve mode. The FortiGate enters the SSL VPN conserve mode before the Kernel conserve mode in an attempt to prevent the Kernel conserve mode from triggering. During the SSL VPN conserve mode, no new SSL connections are allowed. It starts when free memory is <25% of the total memory (when the memory on the FortiGate is less than 512Mb) or <10% of the total memory (when the FortiGate has more than 512Mb built in).

To determine if the FortiGate has entered SSL VPN conserve mode - CLI

Run the following command in the CLI Console:

```
diagnose vpn ssl statistics
```

Result (showing conserve mode state in red):

```
SSLVPN statistics:
------------------
Memory unit:                    1
System total memory:            2118737920
System free memory:             218537984
SSLVPN memory margin:           314572800
SSLVPN state:                   conserve

Max number of users:            2
Max number of tunnels:          0
Max number of connections:      13

Current number of users:        1
Current number of tunnels:      0
Current number of connections: 1
```

Traveling and security

Because SSL VPN provides a means for “on-the-go” users to dial in to the network while away from the office, you need to ensure that wherever and however they choose to dial in is secure, and not potentially compromising the

corporate network.

Host check

To reinforce security, you can enable a host integrity checker to scan the remote client. The integrity checker probes the remote client computer to verify that it is safe before access is granted. Security attributes recorded on the client computer (for example, in the Windows registry, in specific files, or held in memory due to running processes) are examined and uploaded to the FortiGate unit. For more information, see Host check on page 41.

Host Check is only applicable for SSL VPN tunnel mode.

SSL VPN and IPv6

FortiOS supports SSL VPN with IPv6 addressing, and is available for all the java applets (Telnet, VNC, RDP, and so on). IPv6 configurations for security policies and addressing include:

- Policy matching for IPv6 addresses
- Support for DNS resolving in SSL VPN
- Support IPv6 for ping
- FTP applications
- SMB

In essentially any of the following instructions, replace **IPv4** with **IPv6** to achieve the same desired results, but for IPv6 addresses and configurations.

Basic configuration

Configuring SSL VPN involves a number of configurations within FortiOS that you need to complete to make it all come together. This chapter describes the components required, and how and where to configure them to set up the FortiGate unit as an SSL VPN server. The configurations and steps are high level, to show you the procedures needed, and where to locate the options in FortiOS. For real-world examples, see Setup examples on page 63.

There are three or four key steps to configuring an SSL VPN tunnel. The first three in the points below are mandatory, while the others are optional. This chapter outlines these key steps as well as additional configurations for tighter security and monitoring.

The key steps are:

- Create user accounts and user groups for the remote clients.
  (User accounts and groups on page 19)
- Create a web portal to define user access to network resources.
  (Configuring SSL VPN web portals on page 24)
- Configure the security policies.
  (Configuring security policies on page 33)
- For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.
  (Routing in tunnel mode on page 40)
- Setup logging of SSL VPN activities.
  (SSL VPN logs on page 46)

This section contains the following information:

User accounts and groups

The first step for an SSL VPN tunnel is to add the users and user groups that will access the tunnel. You may already have users defined for other authentication-based security policies.

The user group is associated with the web portal that the user sees after logging in. You can use one policy for multiple groups, or multiple policies to handle differences between the groups such as access to different services, or different schedules.

To create a user account:

- In the web-based manager, go to **User & Device > User Definition**, and select **Create New.**
- In the CLI, use the commands in `config user local`.

All users accessing the SSL tunnel must be in a firewall user group. User names can be up to 64 characters long.

To create user groups:

- In the web-based manager, go to **User & Device > User Groups** and select **Create New**.
- In the CLI, use the commands in `config user group`.

Guest group and SSO group have been removed from `config user group` and `config vpn ssl web user-group-bookmark`.

Authentication

Remote users must be authenticated before they can request services and/or access network resources through the web portal. The authentication process can use a password defined on the FortiGate unit or optionally use established external authentication mechanisms such as RADIUS or LDAP.

To authenticate users, you can use a plain text password on the local FortiGate unit, forward authentication requests to an external RADIUS, LDAP or TACACS+ server, or utilize PKI certificates.

FortiOS supports LDAP password renewal notification and updates through SSL VPN. Configuration is enabled using the CLI commands:

```
config user ldap
   edit <username>
       set server <domain>
       set password-expiry-warning enable
       set password-renewal enable
   next
end
```

MAC host check

When a remote client attempts to log in to the portal, you can have the FortiGate unit check against the client's MAC address to ensure that only a specific computer or device is connecting to the tunnel. This can ensure better security should a password be compromised.

MAC addresses can be tied to specific portals and can be either the entire MAC address or a subset of the address. MAC host checking is configured in the CLI using the folowing commands:

```
conf vpn ssl web portal
   edit portal
      set mac-addr-check enable
      set mac-addr-action allow
         config mac-addr-check-rule
            edit "rule1"
               set mac-addr-list 01:01:01:01:01:01 08:00:27:d4:06:5d
               set mac-addr-mask 48
         end
   end
```

IP addresses for users

After the FortiGate unit authenticates a request for a tunnel-mode connection, the FortiGate unit assigns the SSL VPN client an IP address for the session. The address is assigned from an IP Pool, which is a firewall address defining an IP address range.

Take care to prevent overlapping IP addresses. Do not assign to clients any IP addresses that are already in use on the private network. As a precaution, consider assigning IP addresses from a network that is not commonly used (for example, 10.254.254.0/24).

To set tunnel-mode client IP address range - web-based manager:

1. Go to **Policy & Objects > Addresses** and select **Create New**.
2. Enter an **Name**, for example, `SSL_VPN_tunnel_range`.
3. Select a **Type** of **IP Range**.
4. In the **Subnet/IP Range** field, enter the starting and ending IP addresses that you want to assign to SSL VPN clients, for example `10.254.254.[80-100]`.
5. In **Interface**, select **Any**.
6. Select **OK**.

To set tunnel-mode client IP address range - CLI:

If your SSL VPN tunnel range is for example 10.254.254.80 - 10.254.254.100, you could enter

```
config firewall address
   edit SSL_tunnel_users
      set type iprange
      set end-ip 10.254.254.100
      set start-ip 10.254.254.80
   end
```

Authentication of remote users

When remote users connect to the SSL VPN tunnel, they must perform authentication before being able to use the internal network resources. This can be as simple as assigning users with their own passwords, connecting to an LDAP server or using more secure options. FortiOS provides a number of options for authentication as well as security option for those connected users.

The web portal can include bookmarks to connect to internal network resources. A web (HTTP/HTTPS) bookmark can include login credentials so that the FortiGate unit automatically logs the user into the website. This means that the user logs into the SSL VPN and then does not have to enter any more credentials to visit preconfigured web sites.

Both the administrator and the end user can configure bookmarks, including SSO bookmarks. To add bookmarks as a web portal user, see Using the Bookmarks widget on page 56.

Setting the client authentication timeout

The client authentication timeout controls how long an authenticated user will remain connected. When this time expires, the system forces the remote client to authenticate again. As with the idle timeout, a shorter period of

time is more secure. The default value is 28800 seconds (8 hours). You can only modify this timeout value in the CLI.

For example, to change the authentication timeout to 18 000 seconds, enter the following commands in the CLI:

```
config vpn ssl settings
   set auth-timeout 18000
end
```

You can also set the idle timeout for the client, to define how long the user does not access the remote resources before they are logged out.

Additional timeout settings

SSL VPN timeout settings are also available to counter 'Slowloris' and 'R-U-Dead-Yet' vulnerabilities that allow remote attackers to cause a denial of service via partial HTTP requests.

The FortiGate solution involves two attributes (`http-request-header-timeout` and `http-request-body-timeout`).

CLI syntax

```
config vpn ssl settings
   set http-request-header-timeout [1-60] (seconds)
   set http-request-body-timeout [1-60] (seconds)
end
```

Allow one-time login per user

You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same credentials again.

To allow one-time login per user - web-based manager:

Go to **VPN > SSL-VPN Portals**, select a portal, and enable **Limit Users to One SSL-VPN Connection at a Time.** It is disabled by default.

To allow one-time login per user - CLI:

```
config vpn ssl web portal
   edit <portal_name>
      set limit-user-logins enable
end
```

Strong authentication with security certificates

The FortiGate unit supports strong (two-factor) authentication through X.509 security certificates (version 1 or 3). The FortiGate unit can require clients to authenticate using a certificate, and the client can require the FortiGate unit to authenticate using a certificate.

You can select the **Require Client Certificate** option so that clients must authenticate using certificates. The client browser must have a local certificate installed, and the FortiGate unit must have the corresponding CA certificate installed.

When the remote client initiates a connection, the FortiGate unit prompts the client browser for its client-side certificate as part of the authentication process.

To require client authentication by security certificates - web-based manager:

1. Go to **VPN > SSL-VPN Settings**.
2. Select **Require Client Certificate**.
3. Select **Apply**.

To require client authentication by security certificates - CLI:

```
config vpn ssl settings
   set reqclientcert enable
end
```

If your SSL VPN clients require strong authentication, the FortiGate unit must offer a CA certificate that the client browser has installed.

In the FortiGate unit SSL VPN settings, you can select which certificate the FortiGate offers to authenticate itself. By default, the FortiGate unit offers its factory installed (Fortinet_CA_SSLProxy) certificate from Fortinet to remote clients when they connect. If you leave the default setting, a warning appears that recommends you purchase a certificate for your domain and upload it for use.

To enable FortiGate unit authentication by certificate - web-based manager:

1. Go to **VPN > SSL-VPN Settings**.
2. From the **Server Certificate** list, select the certificate that the FortiGate unit uses to identify itself to SSL VPN clients.
3. Select **Apply**.

To enable FortiGate unit authentication by certificate - CLI:

For example, to use the `example_cert` certificate

```
config vpn ssl settings
   set servercert example_cert
end
```

FortiOS will check the server certificate to verify that the certificate is valid. Only valid server certificates should be used.

NSA Suite B cryptography support

FortiOS supports the use of ECDSA Local Certificates for SSL VPN Suite B. The National Security Agency (NSA) developed Suite B algorithms in 2005 to serve as a cryptographic base for both classified and unclassified information at an interoperable level.

FortiOS allows you to import, generate, and use ECDSA certificates defined by the Suite B cryptography set. To generate ECDSA certificates, use the following command in the CLI:

```
exec vpn certificate local generate ec <certificate-name_str> <elliptic-curve-name>
    <subject_str> [<optional_information>]
```

Configuring SSL VPN web portals

The SSL VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiGate administrators can configure login privileges for system users as well as the network resources that are available to the users.

FortiOS supports LDAP password renewal notification and updates through SSL VPN. Configuration is enabled using the CLI commands:

```
config user ldap
   edit <username>
       set server <domain>
       set password-expiry-warning enable
       set password-renewal enable
   next
end
```

This step in the configuration of the SSL VPN tunnel sets up the infrastructure; the addressing, encryption, and certificates needed to make the initial connection to the FortiGate unit. This step is also where you configure what the remote user sees with a successful connection. The portal view defines the resources available to the remote users and the functionality they have on the network.

SSL connection configuration

To configure the basic SSL VPN settings for encryption and login options, go to **VPN > SSL-VPN Settings.**

Listen on Interface(s)	Define the interface which the FortiGate will use to listen for SSL VPN tunnel requests. This is generally your external interface.
Listen on Port	Enter the port number for HTTPS access.

Redirect port 80 to this login port	Enable to redirect the admin HTTP port to the admin HTTPS port.
	
	There are two likely scenarios for this:
	• SSL VPN is not in use, in which case the admin GUI runs on port 443 or 10443, and port 80 is redirected.
	• SSL VPN runs on port 443, in which case port 80 is redirected to 443 and the admin port runs on 10443.
	
	If the administrator chooses to run SSL VPN on port 80, the redirect option is invalid.
	
	This can also be configured in the CLI as shown below (note that HTTPS-redirect is disabled by default):
	
	Syntax:
	
	`config vpn ssl settings`
	`  set https-redirect [enable | disable]`
	`end`

Restrict Access	Restrict accessibility to either **Allow access from any host** or to **Limit access to specific hosts** as desired. If selecting the latter, you must specify the hosts.
Idle Logout	Type the period of time (in seconds) that the connection can remain inactive before the user must log in again. The range is from 10 to 28800 seconds. Setting the value to 0 will disable the idle connection timeout. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.
Server Certificate	Select the signed server certificate to use for authentication. If you leave the default setting (Fortinet_CA_SSLProxy), the FortiGate unit offers its built-in certificate from Fortinet to remote clients when they connect. A warning appears that recommends you purchase a certificate for your domain and upload it for use.
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process.
Address Range	Select **Automatically assign addresses** or **Specify custom IP ranges**. The latter will allow you to select the range or subnet firewall addresses that represent IP address ranges reserved for tunnel-mode SSL VPN clients.

DNS Server	If you select **Specify**, you may enter up to two DNS servers (IPv4 or IPv6) to be provided for the use of clients.
	Note: It is possible to implement a unique DNS suffix per SSL VPN portal using the CLI. Each suffix setting for each specific portal will override the `dns-suffix` setting under `config vpn ssl settings`. This is a CLI-only option, using the following syntax:
	`config vpn ssl web portal`
	`edit <example>`
	`set dns-suffix <string>`
	`end`

Specify WINS Servers	Enable to access options for entering up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.
Allow Endpoint Registration	Select so that FortiClient registers with the FortiGate unit when connecting. If you configured a registration key by going to **System > Config > Advanced**, the remote user is prompted to enter the key. This only occurs on the first connection to the FortiGate unit.

Portal configuration

The portal configuration determines what the remote user sees when they log in to the portal. Both the system administrator and the user have the ability to customize the SSL VPN portal.

To view the portals settings page, go to **VPN > SSL-VPN Portals**.

There are three pre-defined default portal configurations available:

- *full-access*
- *tunnel-access*
- *web-access*

Each portal type includes similar configuration options. Select between the different portals by double-clicking one of the default portals in the list. You can also create a custom portal by selecting the **Create New** option at the top.

Portal Setting	Description
Name	The name for the portal.
Limit Users to One SSL-VPN Connection at a Time	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same credentials again. This option is disabled by default.
Tunnel Mode	These settings determine how tunnel mode clients are assigned IPv4 addresses.

Portal Setting		Description
	Enable Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route. If you enable split tunneling, you are required to set the **Routing Address**, which is the address that your corporate network is using. Traffic intended for the Routing Address will not be split from the tunnel.
	Source IP Pools	Select an IP Pool 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.
	Tunnel Mode Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. • **Allow client to save password** - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. • **Allow client to connect automatically** - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. • **Allow client to keep connections alive** - When enabled, if the user selects this option, the FortiClient should try to reconnect once it detects the VPN connection is down unexpectedly (not manually disconnected by user).
Enable Web Mode		Select to enable web mode access.
Portal Message		This is a text header that appears on the top of the web portal.
Theme		Select a color styling specifically for the web portal.
Show Session Information		The **Show Session Information** widget displays the login name of the user, the amount of time the user has been logged in and the inbound and outbound traffic statistics.
Show Connection Launcher		Displays the **Connection Launcher** widget in the web portal.
Show Login History		Select to include user login history on the web portal.

Portal Setting	Description
User Bookmarks	Enable to allow users to add their own bookmarks in the web portal.
Predefined Bookmarks	Select to include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window appears with the web page. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.

Tunnel Mode Client Options logic

The FortiGate will check the logic of Tunnel mode VPN client options.

If `auto-connect` or `keep-alive` is enabled, the following warning message will be shown: '*save-password should be enabled if either auto-connect or keep-alive is enabled*.'

At the end of editing the portal, if either `auto-connect` or `keep-alive` is enabled and `save-password` is not enabled, the following message will be shown, and adding or editing the portal is not permitted: '*save-password should be enabled as either auto-connect or keep-alive is enabled*.'

Options to allow firewall address to be used in routing table for SSL VPN

If destination **Named Address** is set in **Network > Static Routes** and **Address Range** is set to **Automatically assign addresses** in **VPN > SSL-VPN Settings**, SSL VPN should refresh the routing table automatically.

If your network configuration does not contain a default SSL VPN portal, you might receive the error message “Input value is invalid” when you attempt to access **VPN > SSL-VPN Portals**.

To enable a default portal - CLI:

```
config vpn ssl settings
   set default-portal <full-access | tunnel-access |
    web-access>
end
```

Adding bookmarks

A web bookmark can include login credentials to automatically log the SSL VPN user into the website. When the administrator configures bookmarks, the website credentials must be the same as the user’s SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the website.

To add a bookmark - web-based manager:

1. On the **VPN > SSL-VPN Portals** page, ensure **Enable User Bookmarks** is enabled.
2. Select **Create New** and enter the following information:

Category	Select a category, or group, to include the bookmark. If this is the first bookmark added, you will be prompted to add a category. Otherwise, select **Create** from the drop-down list.
Name	Enter a name for the bookmark.
Type	Select the type of link from the drop-down list. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.
URL	Enter the IP address source.
Description	Enter a brief description of the link.
Single Sign-On	Enable if you wish to use Single Sign-On (SSO) for any links that require authentication. When including a link using SSO, be sure to use the entire URL. For example, http://10.10.1.0/login, rather than just the IP address.

3. Select **OK**.

For more configuration options, see Configuring SSL VPN web portals on page 24.

Personal bookmarks

The administrator has be ability to view bookmarks the remote client has added to their SSL VPN login in the bookmarks widget. This enables the administrator to monitor and, if needed, remove unwanted bookmarks that do not meet with corporate policy.

To view and maintain remote client bookmarks, go to **VPN > SSL-VPN Personal Bookmarks**.

For more information about available bookmark applications, see Applications available in the web portal on page 55

To enable personal bookmarks:

1. Go to **System > Feature Visibility**.
2. Enable **SSL-VPN Personal Bookmark Management**.
3. Select **Apply**.

Moving and cloning bookmarks

The administrator also has the ability to move and clone personal bookmarks in the GUI and CLI.

CLI syntax

```
config vpn ssl web user-bookmark
   edit 'name'
      config bookmarks
      move bookmark1 after/before
      clone bookmark1 to
   next
end
```

Supporting browsers without plugins (Citrix/Port forward) - CLI only

CLI syntax

```
config vpn ssl web user-bookmark
   edit <name>
      config bookmarks
         edit "citrix-address"
            set apptype citrix
            set description "my citrix server"
            set usl "https://my.citrix.server.com"
            set sso enable
         next
      end
   next
end
```

Group-based SSL VPN bookmarks

The administrator can add bookmarks for groups of users. SSL VPN will only output the matched group-name entry to the client. This can only be done via the CLI.

To add group-based SSL VPN bookmarks - CLI:

```
config vpn ssl web portal
   edit "portal-name"
      set user-group-bookmark enable*/disable
   next
end
config vpn ssl web user-group-bookmark
   edit "group-name"
      config bookmark
         edit "bookmark1"
         ....
         next
      end
   next
end
```

Remote desktop bookmark creation with no password

If NLA security is chosen when creating an RDP bookmark, a username and password must be provided. However there may be instances where the user might want to use a blank password, despite being highly unrecommended. If a username is provided but the password is empty, the CLI will display a warning. See example CLI below, where the warning appears as a caution before finishing the command:

```
config vpn ssl web user-group-bookmark
   edit <group-name>
      config bookmarks
         edit <bookmark-name>
            set apptype rdp
            set host 172.16.200.121
            set security nla
            set port 3389
            set logon-user <username>
```

```
        next
      end
Warning: password is empty. It might fail user authentication and remote desktop
    connection would be failed.
end
```

If no username (`logon-user`) is specified, the following warning message will appear:

```
Please enter user name for RDP security method NLA. object set operator error, -2010
    discard the setting Command fail. Return code -2010
```

SSO support for HTML5 RDP

This feature adds support for SSO from the SSL VPN portal to an RDP bookmark. If SSO is used, then the credentials used to login to SSL VPN will be automatically used when connecting to a remote RDP server.

This option is only available in CLI.

To configure SSO support for HTML5 RDP - CLI:

```
conf vpn ssl web user-bookmark
   edit <name>
      config bookmarks
         edit <name>
            set apptype rdp
            set host "x.x.x.x"
            set port <value>
            set sso [disable | auto]
         next
      end
   next
end
```

SSL VPN Realms

You can go to **VPN > SSL-VPN Realms** and create custom login pages for your SSL VPN users. You can use this feature to customize the SSL VPN login page for your users and also to create multiple SSL VPN logins for different user groups.

In order to create a custom login page using the web-based manager, this feature must be enabled using **Feature Select**.

Before you begin, copy the default login page text to a separate text file for safe-keeping. Afterward, if needed, you can restore the text to the original version.

To configure SSL VPN Realms - web-based manager:

1. Configure a custom SSL VPN login by going to **VPN > SSL-VPN Realms** and selecting **Create New**. Users access different portals depending on the URL they enter.
2. The first option in the custom login page is to enter the path of the custom URL.
   This path is appended to the address of the FortiGate unit interface to which SSL VPN users connect. The actual path for the custom login page appears beside the URL path field.
3. You can also limit the number of users that can access the custom login at any given time.

4. You can use HTML code to customize the appearance of the login page.
5. After adding the custom login, you must associate it with the users that will access the custom login. Do this by going to **VPN > SSL-VPN Settings** and adding a rule to the **Authentication/Portal Mapping** section.
6. Under **Authentication/Portal Mapping**, click **Create New** and select the user group(s) and the associated Realm.

To configure SSL VPN Realms - CLI:

```
config vpn ssl web realm
   edit <url-path>
      set login-page <content_str>
      set max-concurrent-user <int>
      set virtual-host <hostname_str>
   end
```

Where the following variables are set:

Variable	Description	Default
`edit <url-path>`	Enter the URL path to access the SSL-VPN login page. Do not include “http://”.	No default.
`login-page <content_str>`	Enter replacement HTML for SSL-VPN login page.	No default.
`max-concurrent-user <int>`	Enter the maximum number of concurrent users allowed. Range 0-65 535. 0 means unlimited.	0
`virtual-host <hostname_str>`	Enter the virtual host name for this realm. Optional. Maximum length 255 characters.	No default.

Customizable FortiClient download URL

The attribute `customize-forticlient-download-url` (disabled by default) can be enabled to allow users to customize the download URL for FortiClient. This option is only available in CLI.

If enabled, two other attributes, `windows-forticlient-download-url` and `macos-forticlient-download-url`, will appear.

To configure a customizable FortiClient download URL- CLI:

```
config vpn ssl web portal
   edit <portal>
      set customize-forticlient-download-url {enable | disable}
      set windows-forticlient-download-url <custom URL for Windows>
      set macos-forticlient-download-url <custom URL for Mac OS>
   next
end
```

Disabling FortiClient download in the web portal

Use the following syntax to disable FortiClient download in the web portal.

```
config vpn ssl web portal
   edit <portal name>
      set forticlient-download disable
   next
end
```

Configuring security policies

You will need at least one SSL VPN security policy. This is an identity-based policy that authenticates users and enables them to access the SSL VPN web portal. The SSL VPN user groups named in the policy determine who can authenticate and which web portal they will use. From the web portal, users can access protected resources or download the SSL VPN tunnel client application.

This section contains the procedures needed to configure security policies for web-only mode operation and tunnel-mode operation. These procedures assume that you have already completed the procedures outlined in Configuring security policies on page 33.

If you will provide tunnel mode access, you will need a second security policy—an ACCEPT tunnel mode policy to permit traffic to flow between the SSL VPN tunnel and the protected networks.

Firewall addresses

Before you can create security policies, you need to define the firewall addresses you will use in those policies. For both web-only and tunnel mode operation, you need to create firewall addresses for all of the destination networks and servers to which the SSL VPN client will be able to connect.

For tunnel mode, you will already have defined firewall addresses for the IP address ranges that the FortiGate unit will assign to SSL VPN clients.

The source address for your SSL VPN security policies will be the predefined “all” address. Both the address and the netmask are `0.0.0.0`. The “all” address is used because VPN clients will be connecting from various addresses, not just one or two known networks. For improved security, if clients will be connecting from one or two known locations you should configure firewall addresses for those locations, instead of using the “all” address.

To create a firewall address, in the web-based manager, go to **Policy & Objects > Objects > Addresses**, and select **Create New.**

Create an SSL VPN security policy

At minimum, you need one SSL VPN security policy to authenticate users and provide access to the protected networks. You will need additional security policies only if you have multiple web portals that provide access to different resources. You can use one policy for multiple groups, or multiple policies to handle differences between the groups such as access to different services, or different schedules.

The SSL VPN security policy specifies:

- The incoming interface that corresponds to the ssl.root interface.
- The SSL VPN user groups that can use the security policy.
- The times (schedule) and types of services that users can access.
- The UTM features and logging that are applied to the connection.

Do not use ALL as the destination address. If you do, you will see the “Destination address of Split Tunneling policy is invalid” error when you enable Split Tunneling.

To create an SSL-VPN security policy - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New.**
2. Enter the following information:

Incoming Interface	Select the virtual SSL VPN interface, such as **ssl.root.**
Outgoing Interface	Select the FortiGate network interface that connects to the protected network.
Source	Select to allow access only to holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field. See Configuring security policies on page 33.
Destination Address	Select the firewall address you created that represents the networks and servers to which the SSL VPN clients will connect. If you want to associate multiple firewall addresses or address groups with the **Destination Interface/Zone**, from **Destination Address**, select the plus symbol. In the dialog box, move the firewall addresses or address groups from the **Available Addresses** section to the **Members** section, then select **OK**.
Schedule	Select **always**.
Service	Select services in the left list and use the right arrow button to move them to the right list. Select the ALL service to allow the user group access to all services.
Action	Select **Accept**.

Your identity-based policies are listed in the security policy table. The FortiGate unit searches the table from the top down to find a policy to match the client’s user group. Using the move icon in each row, you can change the order of the policies in the table to ensure the best policy will be matched first. You can also use the icons to edit or delete policies. Furthermore, you can drag and drop policies in the policy list to rearrange their order.

To create an SSL VPN security policy - CLI:

Create the SSL VPN security policy by entering the following CLI commands.

```
config firewall policy
   edit <id>
      set srcintf ssl.root(sslvpn tunnel interface)
      set dstintf port2
      set srcaddr all
      set dstaddr OfficeLAN
      set nat enable
   end
```

Create a tunnel mode security policy

If your SSL VPN will provide tunnel mode operation, you need to create a security policy to enable traffic to pass between the SSL VPN virtual interface and the protected networks. This is in addition to the SSL VPN security policy that you created in the preceding section.

The SSL VPN virtual interface is the FortiGate unit end of the SSL tunnel that connects to the remote client. It is named `ssl.<vdom_name>`. In the root VDOM, for example, it is named `ssl.root`. If VDOMs are not enabled on your FortiGate unit, the SSL VPN virtual interface is also named ssl.root.

To configure the tunnel mode security policy - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface, such as **ssl.root.**
Outgoing Interface	Select the FortiGate network interface that connects to the protected network.
Source Address	Select the firewall address you created that represents the IP address range assigned to SSL VPN clients, such as SSL_VPN_tunnel_users.
Source User(s)	Select to allow access only to holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field. See Configuring security policies on page 33.
Destination Address	Select the firewall address that represents the networks and servers to which the SSL VPN clients will connect. To select multiple firewall addresses or address groups, select the plus sign next to the drop-down list.
Schedule	Select **always**.
Service	Select services in the left list and use the right arrow button to move them to the right list. Select the ALL service to allow the user group access to all services.
Action	Select **Accept**.
Enable NAT	Select **Enable NAT. (Optional)**

To configure the tunnel mode security policy - CLI:

```
config firewall policy
   edit <id>
      set srcintf ssl.root(sslvpn tunnel interface)
      set dstintf <dst_interface_name>
      set srcaddr <tunnel_ip_address>
      set dstaddr <protected_network_address_name>
      set schedule always
      set service ALL
```

```
      set nat enable
   end
```

This policy enables the SSL VPN client to initiate communication with hosts on the protected network. If you want to enable hosts on the protected network to initiate communication with the SSL VPN client, you should create another Accept policy like the preceding one but with the source and destination settings reversed.

You must also add a static route for tunnel mode operation.

Routing for tunnel mode

If your SSL VPN operates in tunnel mode, you must add a static route so that replies from the protected network can reach the remote SSL VPN client.

To add the tunnel mode route - web-based manager:

1. Go to **Network > Static Routes** and select **Create New**.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the **Destination IP/Mask** of the tunnel IP address that you assigned to the users of the web portal.
3. Select the SSL VPN virtual interface for the **Device**.
4. Select **OK**.

To add the tunnel mode route - CLI:

If you assigned 10.11.254.0/24 as the tunnel IP range, you would enter:

```
config router static
   edit <id>
      set device ssl.root
      set dst 10.11.254.0/24
end
```

Split tunnel Internet browsing policy

With split tunneling disabled, all of the SSL VPN client's requests are sent through the SSL VPN tunnel. But the tunnel mode security policy provides access only to the protected networks behind the FortiGate unit. Clients will receive no response if they attempt to access Internet resources. You can enable clients to connect to the Internet through the FortiGate unit using a split tunnel Internet browsing policy.

To add an Internet browsing policy:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface (**ssl.root**, for example).
Outgoing Interface	Select the FortiGate network interface that connects to the Internet.
Source	Select the firewall address you created that represents the IP address range assigned to SSL VPN clients.

Destination Address	Select **All**.
Action	Select **Accept**.
Enable NAT	Select **Enable**.

To configure the Internet browsing security policy - CLI:

To enable browsing the Internet through port1, you would enter:

```
config firewall policy
   edit 0
      set srcintf ssl.root
      set dstintf port1
      set srcaddr SSL_tunne_users
      set dstaddr all
      set schedule always
      set service ALL
      set nat enable
end
```

Enabling a connection to an IPsec VPN

You might want to provide your SSL VPN clients access to another network, such as a branch office, that is connected by an IPsec VPN. To do this, you need only to add the appropriate security policy.

Route-based connection

To configure interconnection with a route-based IPsec VPN - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface (**ssl.root**, for example).
Outgoing Interface	Select the virtual IPsec interface for your IPsec VPN.
Source	Select the firewall address that represents the IP address range assigned to SSL VPN clients.
Destination Address	Select the address of the IPsec VPN remote protected subnet.
Action	Select **ACCEPT**.
Enable NAT	Enable.

To configure interconnection with a route-based IPsec VPN - CLI:

If, for example, you want to enable SSL VPN users to connect to the private network (address name OfficeAnet) through the toOfficeA IPsec VPN, you would enter:

```
config firewall policy
   edit 0
      set srcintf ssl.root
```

```
        set dstintf toOfficeA
        set srcaddr SSL_tunnel_users
        set dstaddr OfficeAnet
        set action accept
        set nat enable
        set schedule always
        set service ALL
    end
```

Policy-based connection

To configure interconnection with a policy-based IPsec VPN - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface (**ssl.root**, for example).
Outgoing Interface	Select the FortiGate network interface that connects to the Internet.
Source	Select the firewall address that represents the IP address range assigned to SSL VPN clients.
Destination Address	Select the address of the IPsec VPN remote protected subnet.

3. Configure inbound NAT from the CLI:

```
config firewall policy
   edit 0
      set natinbound enable
   end
```

To configure interconnection with a policy-based IPsec VPN - CLI:

If, for example, you want to enable SSL VPN users to connect to the private network (address name OfficeAnet) through the OfficeA IPsec VPN, you would enter:

```
config firewall policy
   edit 0
      set srcintf ssl.root
      set dstintf port1
      set srcaddr SSL_tunnel_users
      set dstaddr OfficeAnet
      set action ipsec
      set schedule always
      set service ALL
      set inbound enable
      set outbound enable
      set natinbound enable
      set vpntunnel OfficeA
end
```

In this example, port1 is connected to the Internet.

Configuring encryption key algorithms

The FortiGate unit supports a range of cryptographic cipher suites to match the capabilities of various web browsers. The web browser and the FortiGate unit negotiate a cipher suite before any information (for example, a user name and password) is transmitted over the SSL link. You can only configure encryption key algorithms for SSL VPN in the CLI.

To configure encryption key algorithms - CLI:

Use the following CLI command,

```
config vpn ssl settings
   set algorithm <cipher_suite>
end
```

where one of the following variables replaces *<cipher_suite>*:

Variable	Description
`low`	Use any cipher suite; AES, 3DES, RC4, DES, or ChaCha.
`medium`	Use a 128-bit or greater cipher suite; AES, 3DES, RC4, or ChaCha.
`high`	Use a cipher suite greater than 128 bits; AES or ChaCha.

Note that the `algorithm <cipher_suite>` syntax is only available when the `sslvpn-enable` attribute is set to **enable**.

Controlling the use of specific cipher suites

Administrators can ban the use of specific cipher suites in the CLI for SSL VPN, so PCI-DSS (Payment Card Industry Data Security Standard) certification can be met.

To ban the use of specific cipher suites for SSL VPN - CLI:

```
config vpn ssl settings
   set banned-cipher [RSA | DH | DHE | ECDH | ECDHE | DSS | ECDSA | AES | AESGCM |
       CAMELLIA | 3DES | SHA1 | SHA256 | SHA384 | STATIC]
```

Additional configuration options

Beyond the basics of setting up the SSL VPN, you can configure a number of other options that can help to ensure your internal network is secure and can limit the possibility of attacks and viruses entering the network from an outside source.

Routing in tunnel mode

If you are creating a SSL VPN connection in tunnel mode, you need to add a static route so that replies from the protected network can reach the remote SSL VPN client.

To add the tunnel mode route - web-based manager:

1. Go to **Network > Static Routes** and select **Create New**.
2. Enter the **Destination IP/Mask** of the tunnel IP address that you assigned to the users of the web portal.
3. Select the SSL VPN virtual interface for the **Device**.
4. Select **OK**.

To add the tunnel mode route - CLI:

If you assigned 10.11.254.0/24 as the tunnel IP range, you would enter:

```
config router static
   edit <id>
      set device ssl.root
      set dst 10.11.254.0/24
end
```

Changing the port number for web portal connections

You can specify a different TCP port number for users to access the web portal login page through the HTTPS link. By default, the port number is 443 and users can access the web portal login page using the following default URL:

`https://<FortiGate_IP_address>:443/remote/login`

where `<FortiGate_IP_address>` is the IP address of the FortiGate interface that accepts connections from remote users.

To change the SSL VPN port - web-based manager:

1. If **Current VDOM** appears at the bottom left of the screen, select **Global** from the list of VDOMs.
2. Go to **VPN > SSL-VPN Settings**.
3. Type an unused port number in the **Listen on Port** field and select **Apply**.

To change the SSL VPN port - CLI:

This is a global setting. For example, to set the SSL VPN port to 10443, enter the following:

```
config vpn ssl settings
   set port 10443
end
```

HTTP to HTTPS redirect support

The admin HTTP port can be redirected to the admin HTTPS port. This is enabled in **VPN > SSL-VPN Settings** using the option **Redirect port 80 to this login port**.

There are two likely scenarios for this:

- SSL VPN is not in use, in which case the admin GUI runs on port 443 or 10443, and port 80 is redirected.
- SSL VPN runs on port 443, in which case port 80 is redirected to 443 and the admin port runs on 10443.

If the administrator chooses to run SSL VPN on port 80, the redirect option is invalid.

This can also be configured in the CLI as described below:

To redirect HTTP to HTTPS port - CLI:

```
config vpn ssl settings
   set https-redirect [enable | disable] (default: disabled)
end
```

SSL offloading

To configure SSL offloading, which allows or denies client renegotiation, you must use the CLI. This helps to resolve the issues that affect all SSL and TLS servers that support renegotiation, identified by the Common Vulnerabilities and Exposures system in CVE-2009-3555. The SSL offloading renegotiation feature is considered a workaround until the IETF permanently resolves the issue.

The CLI command is `ssl-client-renegotiation` and is found under the `config firewall vip` syntax.

Host check

When you enable AV, FW, or AV-FW host checking in the web portal Security Control settings, each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for security software selected from the Host Check list. For more information, see Configuring SSL VPN web portals on page 24.

The Host Check list includes default entries for many security software products.

Host integrity checking is only possible with client computers running Microsoft Windows platforms.

Host Check is only applicable for SSL VPN tunnel mode.

To configure host checking - CLI:

To configure the full-access portal to check for AV and firewall software on client Windows computers, you would enter the following:

```
config vpn ssl web portal
   edit full-access
      set host-check av-fw
end
```

To configure the full-access portal to perform a custom host check for FortiClient Host Security AV and firewall software, you would enter the following:

```
config vpn ssl web portal
```

```
   edit full-access
      set host-check custom
      set host-check-policy FortiClient-AV FortiClient-FW
end
```

Replacing the host check error message

You can add your own host security check error message using either the web-based manager or the CLI. The default message reads: “Your PC does not meet the host checking requirements set by the firewall. Please check that your OS version or antivirus and firewall applications are installed and running properly or you have the right network interface.”

To replace the host check error message - web-based manager:

1. Navigate to **System > Replacement Messages** and select **Extended View** in the upper right corner.
2. Scroll down to **SSL VPN** and select **Hostcheck Error Message**.
3. Edit the text in the right-hand column below and select **Save**.
   If you are unhappy with the new message, you can restore the message to its default by selecting **Restore Default** instead of **Save**.

To replace the host check error message - CLI:

Configure the host check error message using the following command.

```
config system replacemsg sslvpn hostcheck-error
```

Creating a custom host check list

You can add your own software requirements to the host check list using the CLI. Host integrity checking is only possible with client computers running Microsoft Windows platforms. Enter the following commands:

```
config vpn ssl web host-check-software
   edit <software_name>
      set guid <guid_value>
      set type <av | fw>
      set version <version_number>
end
```

If known, enter the Globally Unique Identifier (GUID) for the host check application. Windows uses GUIDs to identify applications in the Windows Registry. The GUID can be found in the Windows registry in the HKEY_ CLASSES_ROOT section.

To obtain the exact versioning, in Windows, right-click on the .EXE file of the application and select **Properties**, then select the **Version** tab.

Example Tunnel Mode Host Check - Registry Key Check

- Check to see if a required registry key is present:

```
config vpn ssl web host-check-software
   edit <computer_name>
      config check-item-list
         edit 1
            set target "HKEY_LOCAL_
                MACHINE\\SYSTEM\\CurrentControlSet\\Control\\ComputerName\\ActiveCompute
                rName:ComputerName=WINXP32SP3B62"
```

```
            set type registry <<<-----
         next
      end
   next
end
```

Example Tunnel Mode Host Check - Application Running Check

- Check to see if a required application is isntalled and/or running:

```
config vpn ssl web host-check-software
   edit "calc"
      config check-item-list
         edit 1
            set target "calc.exe"
            set type process <<<-----
         next
      end
   next
end
```

Example Tunnel Mode Host Check - File Check

- Check to see if a specific file exists at a specific location:

```
config vpn ssl web host-check-software
   edit "putty"
      config check-item-list
         edit 1
            set target "C:\\software\\putty.txt"
            set md5s <ENC>
         next
      end
   next
end
```

Configuring client OS Check

The SSLVPN client OS Check feature can determine if clients are running the Windows 2000, Windows XP, Windows Vista, Windows 7, or Windows 10 operating system. You can configure the OS Check to do any of the following:

- Allow the client access.
- Allow the client access only if the operating system has been updated to a specified patch (service pack) version.
- Deny the client access.

The OS Check has no effect on clients running other operating systems.

The Windows patch check enables you to define the minimum Windows version and patch level allowed when connecting to the SSL VPN portal. When the user attempts to connect to the web portal, FortiOS performs a query on the version of Windows the user has installed. If it does not match the minimum requirement, the connection is denied. The Windows patch check is configured in the CLI.

To specify the acceptable patch level, you set the `latest-patch-level` and the `tolerance`. The lowest acceptable patch level is `latest-patch-level` minus `tolerance`. In this case, `latest-patch-level` is 3 and `tolerance` is 1, so 2 is the lowest acceptable patch level.

To configure OS Check:

OS Check is configurable only in the CLI.

```
config vpn ssl web portal
   edit <portal_name>
   set os-check enable
      config os-check-list [windows-2000 | windows-xp | windows-vista | windows-7 |
          windows-10]
         set action [allow | check-up-to-date | deny]
         set latest-patch-level [disable | 0 - 255]
         set tolerance <tolerance_num>
      end
   end
```

Host check for Windows firewall

The Windows built-in firewall does not have a GUID in root\securitycenter or root\securitycenter2, but you can use a registry value to detect the firewall status.

If Windows firewall is on, the following registry value will be set to 1:

- **KeyName:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
- **ValueName:** EnableFirewall

In FortiOS, use the registry-value-check feature to define the Windows Firewall software by entering the following in the CLI:

```
config vpn ssl web host-check-software
   edit "Microsoft-Windows-Firewall"
      config check-item-list
         edit 1
            set target
                "HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\Firew
                allPolicy\\StandardProfile:EnableFirewall==1"
            set type registry
         next
         edit 2
            set target
                "HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\Firew
                allPolicy\\PublicProfile:EnableFirewall==1"
            set type registry
         next
         edit 3
            set target
                "HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\Firew
                allPolicy\\DomainProfile:EnableFirewall==1"
            set type registry
         next
      end
   set type fw
next
set host-check custom
set host-check-policy Microsoft-Windows-Firewall
```

Adding WINS and DNS services for clients

You can specify the WINS or DNS servers that are made available to SSL-VPN clients.

DNS servers provide the IP addresses that browsers need to access web sites. For Internet sites, you can specify the DNS server that your FortiGate unit uses. If SSL VPN users will access intranet sites using URLs, you need to provide them access to the intranet's DNS server. You specify a primary and a secondary DNS server.

A WINS server provides IP addresses for named servers in a Windows domain. If SSL VPN users will access a Windows network, you need to provide them access to the domain WINS server. You specify a primary and a secondary WINS server.

To specify WINS and DNS services for clients - web-based manager:

1. Go to **VPN > SSL-VPN Settings**.
2. Next to **DNS Server** select **Specify**.
3. Enter the IP addresses of DNS servers in the **DNS Server** fields as needed. Fields are available for both IPv4 and IPv6 addresses.
4. Select **Specify WINS Servers**, and enter the IP addresses of WINS servers in the **WINS Server** fields as needed. Fields are available for both IPv4 and IPv6 addresses.
5. Select **Apply**.

To specify WINS and DNS services for clients - CLI:

```
config vpn ssl settings
   set dns-server1 <address_ipv4>
   set dns-server2 <address_ipv4>
   set wins-server1 <address_ipv4>
   set wins-server2 <address_ipv4>
end
```

Idle timeout

The idle timeout setting controls how long the connection can remain idle before the system forces the remote user to log in again. For security, keep the default value of 5000 seconds or less. Set the timeout value to 0 to disable idle timeouts.

To set the idle timeout - web-based manager:

1. Go to **VPN > SSL-VPN Settings** and enable **Idle Logout**.
2. In the **Inactive For** field, enter the timeout value.
   The valid range is from 10 to 28800 seconds.
3. Select **Apply**.

To set the idle timeout - CLI:

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

Login timeout

With long network latency, the FortiGate can timeout the client before it can finish negotiation processes, such as DNS lookup and time to enter a token. Two CLI commands under `config vpn ssl settings` allow the login timeout to be configured, replacing the previous hard timeout value. The second command can be used to set the SSL VPN maximum DTLS hello timeout.

CLI syntax

```
config vpn ssl settings
   edit <example>
      set login-timeout [10-180] Default is 30 seconds.
      set dtls-hello-timeout [10-60] Default is 10 seconds.
end
```

Login failure limit

The following CLI allows the administrator to configure the number of times wrong credentials are allowed before the SSL VPN server blocks an IP address, and also how long the block would last.

CLI syntax

```
config vpn ssl settings
   set login-attempt-limit [0-10] Default is 2.
   set login-block-time [0-86400] Default is 60 seconds.
end
```

SSL VPN logs

Logging is available for SSL VPN traffic so you can monitor users connected to the FortiGate unit and their activity.

To enable logging of SSL VPN events - web-based manager:

1. Go to **Log & Report > Log Settings**.
2. Enable **Event Logging**, and select **VPN activity event**.
3. Select **Apply**.

To view the SSL VPN log data, in the web-based manager, go to **Log & Report** and select either the **Event Log** or **Traffic Log**.

In event log entries, look for the sub-types “sslvpn-session” and “sslvpn-user”.

For information about how to interpret log messages, see the FortiGate Log Message Reference.

Monitoring active SSL VPN sessions

You can go to **User & Device > Monitor** to view a list of active SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time the connection was made. You can also see which services are being provided, and delete an active web session from the FortiGate unit.

To monitor SSL VPNs - web-based manager:

To view the list of active SSL VPN sessions, go to **Monitor > SSL-VPN Monitor**.

When a tunnel-mode user is connected, the **Description** field displays the IP address that the FortiGate unit assigned to the remote host.

If required, you can end a session/connection by selecting its checkbox and then clicking the **Delete** icon.

Importing and using a CA-signed SSL certificate

Use the following set of instructions to import a CA-signed SSL certificate and configure an SSL VPN using that certificate.

Import the signed certificate into your FortiGate device

1. Unzip the file downloaded from the CA.
   There should be two .CRT files: a CA certificate with bundle in the file name, and a local certificate.
2. Log in to your FortiGate unit and browse to **System > Certificates**.
3. Select **Create New > Local Certificate** to import the local certificate.
   The status of the certificate will change from PENDING to OK.
4. Import the CA certificate by selecting **Import > CA Certificate**.
   It will be listed in the CA Certificates section of the certificates list. You can now configure SSL VPN using the signed certificate.

Configure your FortiGate device to use the signed certificate

1. Log in to your FortiGate unit and browse to **VPN > SSL-VPN Settings**.
2. In the **Connection Settings** section, locate the **Server Certificate** field.
3. Select the new certificate from the drop-down menu.
4. Select **Apply** to configure SSL VPN to use the new certificate.

Implement post-authentication CSRF protection in SSL VPN web mode

This attribute can enable/disable verification of a referrer in the HTTP request header in order to prevent a Cross-Site Request Forgery attack.

CLI Syntax

```
config vpn ssl settings
   set check-referer [enable|disable]
end
```

DTLS support

The Datagram Transport Layer Security (DTLS) protocol is supported for SSL VPN connections. DTLS allows datagram-based applications to communicate in a way that prevents eavesdropping, tampering, or message forgery. It can also be used to improve upload/download throughput. It is similar to the Transport Layer Security (TLS) protocol.

DTLS support can be enabled in the CLI as described below.

CLI Syntax

```
config vpn ssl settings
   set dtls-tunnel [enable | disable] (default: enabled)
end
```

Allow firewall address to be used in routing table for SSL VPN

If destination **Named Address** is set in **Network > Static Routes** and **Address Range is set to Automatically assign addresses** is enabled in **VPN > SSL-VPN Settings**, SSL VPN should refresh the routing table automatically.

To view the routes in the routing table, go to **Monitor > Routing Monitor**.

WAN link load balancing

You can set `virtual-wan-link` as the destination interface in a firewall policy (when SSL VPN is the source interface) for WAN link load balancing. This allows logging into a FortiGate via SSL VPN for traffic inspection and then have outbound traffic load balanced by WAN link load balancing.

CLI syntax

```
config firewall policy
   edit <example>
      set dstintf virtual-wan-link
end
```

The SSL VPN client

The remote client connects to the SSL VPN tunnel in various ways, depending on the VPN configuration.

Tunnel mode establishes a connection to the remote protected network that any application can use. If the client computer runs Microsoft Windows, they can download the tunnel mode client from the web portal.
If the client computer runs Linux or Mac OS X, the user needs to download the tunnel mode client application from the Fortinet Support web site. See the Release Notes for your FortiOS firmware for the specific operating system versions that are supported.

The SSL VPN standalone client installer for Windows is no longer supported in FortiOS 5.4. Users should use the FortiClient installer with the "VPN Only" option instead.

FortiClient

Remote users can use the FortiClient software to initiate an SSL VPN tunnel to connect to the internal network. FortiClient uses local port TCP 1024 to initiate an SSL encrypted connection to the FortiGate unit, on port TCP 443. When connecting using FortiClient, the FortiGate unit authenticates the FortiClient SSL VPN request based on the user group options. The FortiGate unit establishes a tunnel with the client and assigns a virtual IP address to the client PC. Once the tunnel has been established, the user can access the network behind the FortiGate unit.

FortiClient software is available for download at www.forticlient.com and is available for Windows, Mac OS X, Apple iOS, and Android.

Tunnel mode client configuration

The FortiClient SSL VPN tunnel client requires basic configuration by the remote user to connect to the SSL VPN tunnel. When distributing the FortiClient software, provide the following information for the remote user to enter once the client software has been started. Once entered, they can select **Connect** to begin an SSL VPN session.

Connection Name	If you have pre-configured the connection settings, select the connection from the list and then select **Connect**. Otherwise, enter the settings in the fields below.
Remote Gateway	Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN.
Username	Enter your username.

Client Certificate	Use this field if the SSL VPN requires a certificate for authentication. Select the required certificate from the drop-down list. The certificate must be installed in the Internet Explorer certificate store.

The SSL VPN web portal

This chapter explains how to use and configure the web portal features. This chapter is written for end users as well as administrators.

The following topics are included:

Connecting to the FortiGate unit

You can connect to the FortiGate unit using a web browser. The URL of the FortiGate interface may vary from one installation to the next. If required, ask your FortiGate administrator for the URL of the FortiGate unit, and obtain a user name and password. You can connect to the web portal using an Android phone, iPhone, or iPad. The FortiGate unit will display the content of the portal to fit the device's screen.

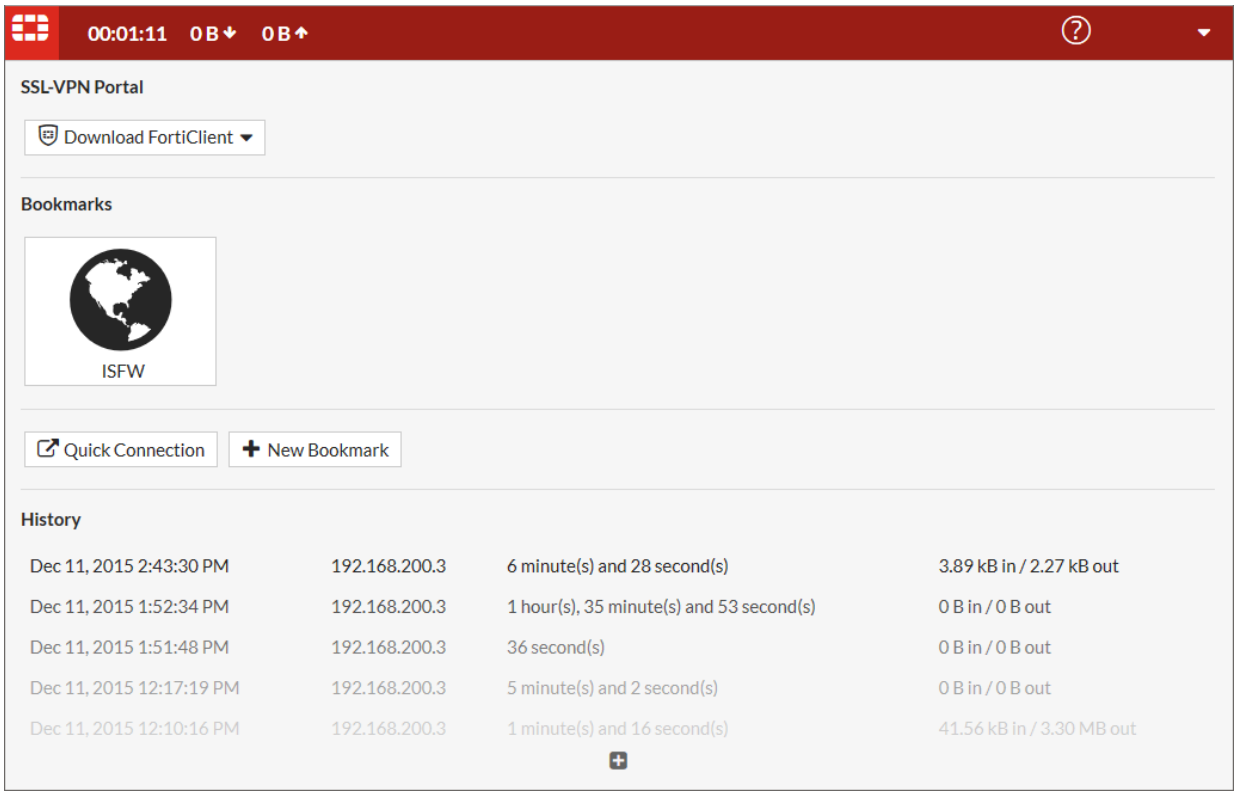
In addition, if you will be using a personal or group security (X.509) certificate to connect to the FortiGate unit, your web browser may prompt you for the name of the certificate. Your FortiGate administrator can tell you which certificate to select.

To log into the secure FortiGate HTTP gateway

1. Using the web browser on your computer, browse to the URL of the FortiGate unit (for example, `https://`<FortiGate_IP_address>`:443/remote/login`). The FortiGate unit may offer you a self-signed security certificate. If you are prompted to proceed, select **Yes**.
   A second message may be displayed to inform you that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. You can ignore the message.
2. When you are prompted for your user name and password:
   - In the **Name** field, type your user name.
   - In the **Password** field, type your password.
3. Select **Login**.
   The FortiGate unit will redirect your web browser to the FortiGate SSL VPN web portal home page automatically.

Web portal overview

After logging in to the web portal, the remote user is presented with a web portal page similar to the following:



Various widgets provide the web portal's features:

- **Session Information** displays the elapsed time since login and the volume of HTTP and HTTPS traffic, both inbound and outbound.
- **Quick Connection** enables you to connect to network resources without using or creating a bookmark.
- **Download Forticlient** provides access to the FortiClient tunnel application for various operating systems.
- **Bookmarks** provides links to network resources. You can use the administrator-defined bookmarks and you can add your own bookmarks.

While using the web portal, you can select the **Help** button to get information to assist you in using the portal features. This information displays in a separate browser window.

When you have finished using the web portal, select the **Logout** button in the top right corner of the portal window.

After making any changes to the web portal configuration, be sure to select **Apply**.

Portal configuration

The SSL VPN web portal enables users to access network resources through a secure channel using a web browser. Fortinet administrators can configure log in privileges for system users and which network resources are available to the users.

The portal configuration determines what the user sees when they log in to the portal. Both the system administrator and the user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- **full-access**: Includes all widgets available to the user - **Session Information**, **Tunnel Mode** options, **Connection Launcher**, **Remote Desktop**, and **Predefined Bookmarks**.
- **tunnel-access**: Includes **Session Information** and **Tunnel Mode** options.
- **web-access**: Includes **Session Information** and **Predefined Bookmarks** widgets.

You can also create your own web portal to meet your corporate requirements.

Portal page	
Create New	Creates a new web portal.
Edit	Select a portal from the list to enable the Edit option, and modify the portal configuration.
Delete	Removes a portal configuration. To remove multiple portals from the list, select the check box beside the portal names, then select **Delete**.
Name	The name of the web portal.
Ref.	Displays the number of times the object is referenced in other configurations on the FortiGate unit, such as security policies. To view the location of the referenced object, select the number in **Ref.** column. To view more information about how the object is used, select one of: **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. **Edit this object** – modifies settings within that particular setting that the object is referenced with. **View the details for this object** – similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with.

Portal settings

A web portal defines SSL VPN user access to network resources. The portal configuration determines what SSL VPN users see when they log in to the unit. Both the Fortinet administrator and the SSL VPN user have the ability to customize the web portal settings. Portal settings are configured in **VPN > SSL-VPN Portals**.

The following settings are available, allow you to configure general and security console options for your web portal.

Portal Setting	Description
Name	The name for the portal.
Limit Users to One SSL-VPN Connection at a Time	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same credentials again. This option is disabled by default.
Tunnel Mode	These settings determine how tunnel mode clients are assigned IPv4 addresses.
Enable Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route. If you enable split tunneling, you are required to set the **Routing Address**, which is the address that your corporate network is using. Traffic intended for the Routing Address will not be split from the tunnel.
Source IP Pools	Select an IP Pool 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.
Tunnel Mode Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. • **Allow client to save password** - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. • **Allow client to connect automatically** - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. • **Allow client to keep connections alive** - When enabled, if the user selects this option, the FortiClient should try to reconnect once it detects the VPN connection is down unexpectedly (not manually disconnected by user).
Enable Web Mode	Select to enable web mode access.
Portal Message	This is a text header that appears on the top of the web portal.

Portal Setting	Description
Theme	Select a color styling specifically for the web portal.
Show Session Information	The **Show Session Information** widget displays the login name of the user, the amount of time the user has been logged in and the inbound and outbound traffic statistics.
Show Connection Launcher	Displays the **Connection Launcher** widget in the web portal.
Show Login History	Select to include user login history on the web portal.
User Bookmarks	Enable to allow users to add their own bookmarks in the web portal.
Predefined Bookmarks	Select to include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window appears with the web page. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.

Predefined Bookmarks

Bookmarks are used as links to specific resources on the network. When a bookmark is selected from a bookmark list, a pop-up window appears with the requested web page. Telnet, RDP, and VNC pop up a window that requires a browser plug-in. FTP and Samba replace the bookmarks page with an HTML file-browser.

Note that the RDP/VNC web portals are **not** supported for the following platforms:

Platform	Model
FortiGate	80D, 92D, 200D, 200D-POE, 240D, 240D-POE, 600C, 800C, 1000C, 3240C, 3600C, and 5001C
FortiGate-Rugged	90D
FortiWiFi	92D

A web bookmark can include login credentials to automatically log the SSL VPN user into the web site. When the administrator configures bookmarks, the web site credentials must be the same as the user's SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the web site.

Applications available in the web portal

Depending on the web portal configuration and user group settings, one or more of the following server applications are available to you through **Predefined Bookmarks**, as well as the **Quick Connection** widget:

- Citrix makes use of SOCKS so that the Citrix client can connect to the SSL VPN port forward module to provide the connection.
- FTP (File Transfer Protocol) enables you to transfer files between your computer and a remote host.

- HTTP/HTTPS accesses web pages.
- Port Forward provides the middle ground between web mode and tunnel mode. When the SSL VPN receives data from a client application, the data is encrypted and sent to the FortiGate unit, which then forwards the traffic to the application server.
- RDP (Remote Desktop Protocol), similar to VNC, enables you to remotely control a computer running Microsoft Terminal Services.
- SMB/CIFS implements the Server Message Block (SMB) protocol to support file sharing between your computer and a remote server host.
- SSH (Secure Shell) enables you to exchange data between two computers using a secure channel.
- TELNET (Teletype Network emulation) enables you to use your computer as a virtual text-only terminal to log in to a remote host.
- VNC (Virtual Network Computing) enables you to remotely control another computer, for example, accessing your work computer from your home computer.

Some server applications may prompt you for a user name and password. You must have a user account created by the server administrator so that you can log in.

Windows file sharing through SMB/CIFS is supported through shared directories.

Group-based SSL VPN bookmarks

The administrator can add bookmarks for groups of users. SSL VPN will only output the matched group-name entry to the client. This can only be done via the CLI.

To add group-based SSL VPN bookmarks - CLI:

```
config vpn ssl web portal
   edit "portal-name"
      set user-group-bookmark enable*/disable
   next
end
config vpn ssl web user-group-bookmark
   edit "group-name"
      config bookmark
         edit "bookmark1"
         ....
         next
      end
   next
end
```

Using the Bookmarks widget

The Bookmarks widget shows both administrator-configured and user-configured bookmarks. Administrator bookmarks cannot be altered but you can add, edit or delete user bookmarks.

The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the My Bookmarks list. For more information, see Adding bookmarks on page 57.

If you want to access a web server or telnet server without first adding a bookmark to the My Bookmarks list, use the Connection Tool instead. For more information, see Using the Bookmarks widget on page 56.

Adding bookmarks

You can add frequently used connections as bookmarks. Afterward, select any hyperlink from the Bookmarks list to initiate a session.

To add a bookmark

1. In the web portal, select **New Bookmark**.
2. Enter the following information:

Name	Enter the name to display in the Bookmarks list.
Type	Select the abbreviated name of the server application or network service from the drop-down list.
Location	Enter the IP address or FQDN of the server application or network service. For RDP connections, you can append some parameters to control screen size and keyboard layout. See Using the Bookmarks widget on page 56.
Description	Optionally enter a short description. The description displays when you pause the mouse pointer over the hyperlink.
SSO	Single Sign On (SSO) is available for HTTP/HTTPS bookmarks only. **Disabled** — This is not an SSO bookmark. **Automatic** — Use your SSL VPN credentials or an alternate set. See the **SSO Credentials** field. **Static** — Supply credentials and other required information (such as an account number) to a web site that uses an HTML form for authentication. You provide a list of the form field names and the values to enter into them. This method does not work for sites that use HTTP authentication, in which the browser opens a pop-up dialog box requesting credentials.
SSO fields	
SSO Credentials	**SSL VPN Login** — Use your SSL VPN login credentials. **Alternative** — Enter **Username** and **Password** below.
Username	Alternative username. Available if **SSO Credentials** is **Alternative**.

Password	Alternative password. Available if **SSO Credentials** is **Alternative**.
Static SSO fields	These fields are available if **SSO** is **Static**.
Field Name	Enter the field name, as it appears in the HTML form.
Value	Enter the field value. To use the values from **SSO Credentials**, enter `%passwd%` for password or `%username%` for username.
Add	Add another **Field Name** / **Value** pair.

3. Select **OK** and then select **Done**.

Group-based SSL VPN bookmarks

This CLI-only feature allows administrators to add bookmarks for groups of users. SSL VPN will only output the matched group-name entry to the client.

Syntax:

```
config vpn ssl web portal
   edit "portal-name"
      set user-group-bookmark enable*/disable
   next
end
conf vpn ssl web user-group-bookmark
   edit "group-name"
      conf bookmark
         edit "bookmark1"
         ....
         next
      end
   next
end
```

Group-based SSL VPN bookmarks

This CLI-only feature allows administrators to add bookmarks for groups of users. SSL VPN will only output the matched group-name entry to the client.

Syntax:

```
config vpn ssl web portal
   edit <portal-name>
      set user-group-bookmark [enable | disable]
   next
end
config vpn ssl web user-group-bookmark
   edit <group-name>
      config bookmark
         edit <bookmark1>
         ....
         next
```

```
        end
    next
end
```

Using the Quick Connection Tool

The **Quick Connection Tool** widget enables a user to connect to a resource when it isn't a predefined bookmark.

You can connect to any type of server without adding a bookmark to the **Bookmarks** list. The fields in the **Quick Connection Tool** enable you to specify the type of server and the URL or IP address of the host computer.

See the following procedures:

- To connect to a web server on page 59
- To ping a host or server behind the FortiGate unit on page 59
- To start a Telnet session on page 60
- To start an FTP session on page 60
- To start an SMB/CIFS session on page 60
- To start an SSH session on page 61
- To start an RDP session on page 61
- To start a VNC session on page 61

Except for ping, these services require that you have an account on the server to which you connect.

When you use **Quick Connection Tool**, the FortiGate unit may offer you its self-signed security certificate. Select **Yes** to proceed. A second message may be displayed to inform you of a host name mismatch. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. Select **Yes** to proceed.

To connect to a web server

1. In **Type**, select **HTTP/HTTPS**.
2. In the **URL** field, type the URL of the web server.
   For example: `http://www.mywebexample.com` or `https://172.20.120.101`
3. Select **Launch**.
4. To end the session, close the browser window.

To ping a host or server behind the FortiGate unit

1. In **Type**, select **Ping**.
2. In the **Host** field, enter the IP address of the host or server that you want to reach.
   For example: `10.11.101.22`
3. Select **Launch**.
   A message stating whether the IP address can be reached or not is displayed.

To start a Telnet session

1. In **Type**, select **Telnet**.
2. In the **Host** field, type the IP address of the telnet host.
   For example: `10.11.101.12`
3. Select **Launch**.
   A Telnet window opens.
4. Select **Connect**.
5. A telnet session starts and you are prompted to log in to the remote host.
   After you log in, you may enter any series of valid telnet commands at the system prompt.
6. To end the session, select **Disconnect** (or type `exit`) and then close the TELNET connection window.

To start an FTP session

1. In **Type**, select **FTP**.
2. In the **Folder** field, type the IP address/folder of the FTP server.
   For example: `10.11.101.12/folder`
3. Select **Launch**.
   A login window opens.
4. Enter your user name and password and then select **Login**.
   You must have a user account on the remote host to log in.
5. Manipulate the files in any of the following ways:
   - To download a file, select the file link in the **Name** column.
   - To access a subdirectory (**Type** is **Folder**), select the link in the **Name** column.
   - To create a subdirectory in the current directory, select **New directory**.
   - To delete a file or subdirectory from the current directory, select its **Delete** icon.
   - To rename a file in the current directory, select its **Rename** icon.
   - To upload a file to the current directory from your client computer, select **Upload**.
   - When the current directory is a subdirectory, you can select **Up** to access the parent directory.
6. To end the FTP session, select **Logout**.

To start an SMB/CIFS session

1. In **Type**, select **SMB/CIFS**.
2. In the **Folder** field, type the IP address/folder of the SMB or CIFS server.
   For example: `10.11.101.12`
3. Select **Launch**.
4. Enter your user name and password and then select **Login**.
   You must have a user account on the remote host to log in.
5. Manipulate the files in any of the following ways:
   - To download a file, select the file link in the **Name** column.
   - To access a subdirectory (**Type** is **Folder**), select the file link in the **Name** column.
   - To create a subdirectory in the current directory, select **New Directory**.
   - To delete a file or subdirectory from the current directory, select its **Delete** icon.
   - To rename a file, select its **Rename** icon.

- To upload a file from your client computer to the current directory, select **Upload**.
- When the current directory is a subdirectory, you can select **Up** to access the parent directory.

6. To end the SMB/CIFS session, select **Logout** and then close the SMB/CIFS window.

To start an SSH session

1. In **Type**, select **SSH**.
2. In the **Host** field, type the IP address of the SSH host.
   For example: `10.11.101.12`
3. Select **Launch**.
   A login window opens.
4. Select **Connect**.
   A SSH session starts and you are prompted to log in to the remote host. You must have a user account to log in. After you log in, you may enter any series of valid commands at the system prompt.
5. To end the session, select **Disconnect** (or type `exit`) and then close the SSH connection window.

To start an RDP session

1. In **Type**, select **RDP**.
2. In the **Host** field, type the IP address of the RDP host.
   For example: `10.11.101.12`
3. To log in to the remote host, type your user name and password. You must have a user account on the remote host to log in. Note that the user name should be entered in User Principal Name (UPN) format.
4. Select **Launch**.
   A login window opens.
5. Select **Login**.
   If you need to send Ctrl-Alt-Delete in your session, use Ctrl-Alt-End.
6. To end the RDP session, Log out of Windows or select **Cancel** from the Logon window.

Some Windows servers require a specific Security to be set for RDP sessions, such as Network Level Authentication (NLA) or Transport Layer Security (TLS), not the standard RDP encryption security. For example, Windows 10 requires the use of TLS.

To start a VNC session

1. In **Type**, select **VNC**.
2. In the **Host** field, type the IP address of the VNC host.
   For example: `10.11.101.12`
3. Select **Launch**.
   A login window opens.
4. Type your user name and password when prompted to log in to the remote host.
   You must have a user account on the remote host to log in.
5. Select **OK**.
   If you need to send Ctrl-Alt-Delete in your session, press F8, then select **Send Ctrl-Alt-Delete** from the pop-up menu.
6. To end the VNC session, close the VNC window.

Note that the RDP/VNC web portals are **not** supported for the following platforms:

Platform	Model
FortiGate	80D, 92D, 200D, 200D-POE, 240D, 240D-POE, 600C, 800C, 1000C, 3240C, 3600C, and 5001C
FortiGate-Rugged	90D
FortiWiFi	92D

Using FortiClient

Remote users can use FortiClient Endpoint Security to initiate an SSL VPN tunnel to connect to the internal network. FortiClient uses local port TCP 1024 to initiate an SSL encrypted connection to the FortiGate unit, on port TCP 10443. When connecting using FortiClient, the FortiGate unit authenticates the FortiClient SSL VPN request based on the user group options. the FortiGate unit establishes a tunnel with the client and assigns a virtual IP address to the client PC. Once the tunnel has been established, the user can access the network behind the FortiGate unit.

For information on configuring the FortiGate unit for SSL VPN connectivity, see Basic configuration on page 19. For details on configuring FortiClient for SSL VPN connections, see the FortiClient documentation.

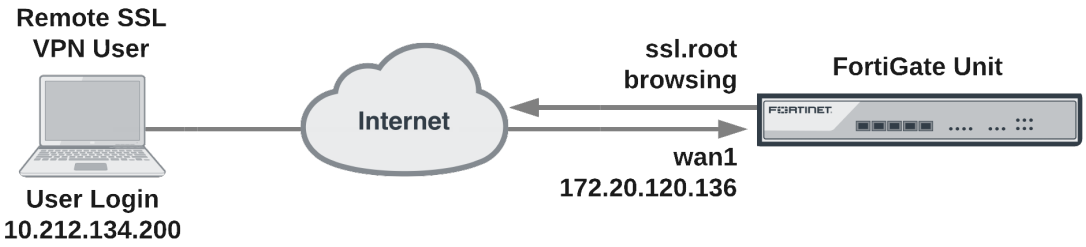
Setup examples

The examples in this chapter demonstrate the basic configurations needed for common connections to the SSL VPN tunnel and portals, applying the steps outlined in Basic configuration on page 19.

The following examples are included:

Secure Internet browsing

This example sets up an SSL VPN tunnel that provides remote users the ability to access the Internet while traveling, and ensures that they are not subject to malware and other dangers, by using the corporate firewall to filter all of their Internet traffic. Essentially, the remote user will connect to the corporate FortiGate unit to surf the Internet.



Using SSL VPN and FortiClient SSL VPN software, you create a means to use the corporate FortiGate to browse the Internet safely.

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to **VPN > SSL-VPN Portals** and select *tunnel-access*.
2. Disable **Split Tunneling**.
3. For **Source IP Pools** select **SSLVPN_TUNNEL_ADDR1**.
4. Select **OK**.

Creating the SSL VPN user and user group

1. Create the SSL VPN user and add the user to a user group configured for SSL VPN use.
2. Go to **User & Device > User Definition** and select **Create New** to add the user:

User Name	twhite
Password	password

3. Select **OK**.
4. Go to **User & Device > User Groups** and select **Create New** to add `twhite` to a group called `SSL VPN`:

Name	SSL VPN
Type	Firewall

5. Move **twhite** to the **Members** list.
6. Select **OK**.

Creating a static route for the remote SSL VPN user

Create a static route to direct traffic destined for tunnel users to the SSL VPN tunnel.

1. Go to **Network > Static Routes** and select **Create New** to add the static route.

Destination IP/Mask	10.212.134.0/255.255.255.0
Device	ssl.root

The **Destination IP/Mask** matches the network address of the remote SSL VPN user.

2. Select **OK**.

Creating security policies

Create an SSL VPN security policy with SSL VPN user authentication to allow SSL VPN traffic to enter the FortiGate unit.

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Add an SSL VPN security policy as below, and click *OK*.

Incoming Interface	ssl.root
Outgoing Interface	internal
Source Address	all
Source User Group	SSL VPN
Destination	all

3. Select **OK**.

Configuring authentication rules

1. Go to **VPN > SSL-VPN Settings** and select **Create New** under **Authentication/Portal Mapping**.
2. Add an authentication rule for the remote user:

Users/Groups	Tunnel
Portal	tunnel-access

3. Select **OK** and **Apply**.

Results

Using the FortiClient SSLVPN application, access the VPN using the address `https://172.20.120.136:443/` and log in as `twhite`. Once connected, you can browse the Internet.

From the FortiGate web-based manager, go to **Monitor > SSL-VPN Monitor** to view the list of users connected using SSL VPN. The **Subsession** entry indicates the split tunnel which redirects to the Internet.

Split Tunnel

In this configuration, remote users are able to securely access the head office internal network through the head office firewall, yet browse the Internet without going through the head office FortiGate. Split tunneling is enabled by default for SSL VPN on FortiGate units.

The solution below describes how to configure FortiGate SSL VPN split tunneling using the FortiClient SSL VPN software, available from the Fortinet Support site.

Without split tunneling, all communication from remote SSL VPN users to the head office internal network and to the Internet uses an SSL VPN tunnel between the user's PC and the head office FortiGate unit. Connections to the Internet are routed back out the head office FortiGate unit to the Internet. Replies come back into the head office FortiGate unit before being routed back through the SSL VPN tunnel to the remote user.

In short, enabling split tunneling protects the head office from potentially harmful access and external threats that may occur as a result of the end user's indiscretion while browsing the Internet. By contrast, disabling split tunneling protects the end user by forcing all their Internet traffic to pass through the FortiGate firewall.

Creating a firewall address for the head office server

1. Go to **Policy & Objects > Addresses** and select **Create New** and add the head office server address:

Category	Address
Name	Head office server
Type	Subnet
Subnet / IP Range	192.168.1.12
Interface	Internal

2. Select **OK**.

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to **VPN > SSL-VPN Portals** and select **tunnel-access**.
2. Enter the following:

Name	Connect to head office server
Enable Tunnel Mode	Enable
Enable Split Tunneling	Enable
Routing Address	Internal
Source IP Pools	SSLVPN_TUNNEL_ADDR1

3. Select **OK**.

Creating the SSL VPN user and user group

Create the SSL VPN user and add the user to a user group.

1. Go to **User & Device > User Definition**, select **Create New** and add the user:

User Name	twhite
Password	password

2. Select **OK**.
3. Go to **User & Device > User Groups** and select **Create New** to add the new user to the SSL VPN user group:

Name	Tunnel
Type	Firewall

4. Move **twhite** to the **Members** list.
5. Select **OK**.

Creating a static route for the remote SSL VPN user

Create a static route to direct traffic destined for tunnel users to the SSL VPN tunnel.

1. Go to **Network > Static Routes** and select **Create New**

Destination IP/Mask	10.212.134.0/255.255.255.0
Device	ssl.root

2. Select **OK**.

Creating security policies

Create an SSL VPN security policy with SSL VPN user authentication to allow SSL VPN traffic to enter the FortiGate unit. Create a normal security policy from ssl.root to wan1 to allow SSL VPN traffic to connect to the Internet.

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Complete the following:

Incoming Interface	ssl.root
Source Address	all
Source User(s)	Tunnel
Outgoing Interface	internal
Destination Address	Head office server

3. Select **OK**.
4. Add a security policy that allows remote SSL VPN users to connect to the Internet.
5. Select **Create New**.
6. Complete the following and select **OK**:

Incoming Interface	ssl.root
Source Address	all
Source User(s)	Tunnel
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Configuring authentication rules

1. Go to **VPN > SSL-VPN Settings** and select **Create New** under **Authentication/Portal Mapping**.
2. Add an authentication rule for the remote user:

Users/Groups	Tunnel
Portal	tunnel-access

3. Select **OK** and **Apply**.

Results

Using the FortiClient SSL VPN application on the remote PC, connect to the VPN using the address `https://172.20.120.136:443/` and log in with the `twhite` user account. Once connected, you can connect to the head office server or browse to web sites on the Internet.

From the web-based manager, go to **Monitor > SSL-VPN Monitor** to view the list of users connected using SSL VPN. The **Subsession** entry indicates the split tunnel which redirects SSL VPN sessions to the Internet.

Multiple user groups with different access permissions

You might need to provide access to several user groups with different access permissions. Consider the following example topology in which users on the Internet have controlled access to servers and workstations on private networks behind a FortiGate unit.

In this example configuration, there are two users:

- User1 can access the servers on Subnet_1.
- User2 can access the workstation PCs on Subnet_2.

You could easily add more users to either user group to provide them access to the user group's assigned web portal.

General configuration steps

1. Create firewall addresses for:
   - The destination networks.
   - Two non-overlapping tunnel IP address ranges that the FortiGate unit will assign to tunnel clients in the two user groups.
2. Create two web portals.
3. Create two user accounts, User1 and User2.
4. Create two user groups. For each group, add a user as a member and select a web portal. In this example, User1 will belong to Group1, which will be assigned to Portal1 (similar configuration for User2).
5. Create security policies:
   - Two SSL VPN security policies, one to each destination.
   - Two tunnel-mode policies to allow each group of users to reach its permitted destination network.
6. Create the static route to direct packets for the users to the tunnel.

Creating the firewall addresses

Security policies do not accept direct entry of IP addresses and address ranges. You must define firewall addresses in advance.

Creating the destination addresses

SSL VPN users in this example can access either Subnet_1 or Subnet_2.

To define destination addresses - web-based manager:

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New**, enter the following information, and select **OK**:

Name	Subnet_1
Type	Subnet
Subnet/IP Range	10.11.101.0/24
Interface	port2

3. Select **Create New**, enter the following information, and select **OK**:

Name	Subnet_2
Type	Subnet
Subnet/IP Range	10.11.201.0/24
Interface	port3

Creating the tunnel client range addresses

To accommodate the two groups of users, split an otherwise unused subnet into two ranges. The tunnel client addresses must not conflict with each other or with other addresses.

To define tunnel client addresses - web-based manager:

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New**, enter the following information, and select **OK**:

Name	Tunnel_group1
Type	IP Range
Subnet/IP Range	10.11.254.1-10.11.254.50
Interface	Any

3. Select **Create New**, enter the following information, and select **OK**.

Name	Tunnel_group2
Type	IP Range
Subnet/IP Range	10.11.254.51-10.11.254.100
Interface	Any

Creating the web portals

To accommodate two different sets of access permissions, you need to create two web portals, portal1 and portal2, for example. Later, you will create two SSL VPN user groups, one to assign to portal1 and the other to assign to portal2.

To create the portal1 web portal:

1. Go to **VPN > SSL-VPN Portals** and select **Create New**.
2. Enter `portal1` in the **Name** field.
3. In **Source IP Pools**, select **Tunnel_ group1**.
4. Select **OK**.

To create the portal2 web portal:

1. Go to **VPN > SSL-VPN Portals** and select **Create New**.
2. Enter `portal2` in the **Name** field and select **OK**.
3. In **IP Pools**, select **Tunnel_ group2**
4. Select **OK**.

Later, you can configure these portals with bookmarks and enable connection tool capabilities for the convenience of your users.

Creating the user accounts and user groups

After enabling SSL VPN and creating the web portals that you need, you need to create the user accounts and then the user groups that require SSL VPN access.

Go to **User & Device > User Definition** and create user1 and user2 with password authentication. After you create the users, create the SSL VPN user groups.

To create the user groups - web-based manager:

1. Go to **User & Device > User Groups**.
2. Select **Create New** and enter the following information:

Name	Group1
Type	Firewall

3. From the **Available** list, select **User1** and move it to the **Members** list by selecting the right arrow button.
4. Select **OK**.
5. Repeat steps 2 through 4 to create Group2, assigned to Portal2, with User2 as its only member.

Creating the security policies

You need to define security policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected networks behind the FortiGate unit. Before you create the security policies, you must define the source and destination addresses to include in the policy. See Creating the firewall addresses on page 68.

Two types of security policy are required:

- An SSL VPN policy enables clients to authenticate and permits a web-mode connection to the destination network. In this example, there are two destination networks, so there will be two SSL VPN policies. The authentication ensures that only authorized users can access the destination network.
- A tunnel-mode policy is a regular ACCEPT security policy that enables traffic to flow between the SSL VPN tunnel interface and the protected network. Tunnel-mode policies are required if you want to provide tunnel-mode connections for your clients. In this example, there are two destination networks, so there will be two tunnel-mode policies.

To create the SSL VPN security policies - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New.**
2. Enter the following information and click **OK**:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	All
Source User(s)	Group1
Outgoing Interface	port2
Destination Address	Subnet_1
Service	All

3. Select **Create New.**
4. Enter the following information:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	All
Source User(s)	Group2
Outgoing Interface	port3
Destination Address	Subnet_2
Service	All

5. Click **OK**.

Configuring authentication rules

1. Go to **VPN > SSL-VPN Settings** and select **Create New** under **Authentication/Portal Mapping**.
2. Add an authentication rule for the first remote group:

Users/Groups	Group1
Portal	Portal1

3. Select **OK** and **Apply**.
4. Select **Create New** and add an authentication rule for the second remote group:

Users/Groups	Group2
Portal	Portal2

5. Select **OK** and **Apply**.

To create the tunnel-mode security policies - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information, and select **OK**:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	Tunnel_group1
Source User(s)	Group1
Outgoing Interface	port2
Destination Address	Subnet_1
Service	All
Action	ACCEPT
Enable NAT	Enable

3. Select **Create New.**
4. Enter the following information, and select **OK**:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	Tunnel_group2
Source User(s)	Group2
Outgoing Interface	port3
Destination Address	Subnet_2
Service	All
Action	ACCEPT
Enable NAT	Enable

Create the static route to tunnel mode clients

Reply packets destined for tunnel mode clients must pass through the SSL VPN tunnel. You need to define a static route to allow this.

To add a route to SSL VPN tunnel mode clients - web-based manager:

1. Go to **Network > Static Routes** and select **Create New**.
2. Enter the following information and select **OK**.

Destination IP/Mask	`10.11.254.0/24` This IP address range covers both ranges that you assigned to SSL VPN tunnel-mode users. See Creating the tunnel client range addresses on page 69.
Device	Select the SSL VPN virtual interface, **ssl.root** for example.

In this example, the **IP Pools** field on the **VPN > SSL-VPN Settings** page is not used because each web portal specifies its own tunnel IP address range.

Client device certificate authentication with multiple groups

In the following example, we require clients connecting to a FortiGate SSL VPN to have a device certificate installed on their machine in order to authenticate to the VPN.

Employees (in a specific OU in AD) will be required to have a device certificate to connect, while vendors (in a separate OU in AD) will *not* be required to have a device certificate.

This can *only* be performed in the CLI console.

The Authentication-rule option is only available in theCLI as an advanced setting to achieve your requirements. It is not available on the GUI. So in **VPN > SSL-VPN Settings**, do *not* enable **Require Client Certificate**, but selectively enable `client-cert` in each authentication-rule based on the requirements through CLI instead.

Configuring SSL VPN shared settings and authentication rules - CLI:

The following example assumes that remote LDAP users/groups have been pre-configured.

```
config vpn ssl settings
   set servercert "Fortinet_Factory"
   set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
   set port 443
   set source-interface "wan1"
   set source-address "all"
```

```
    set default-portal "full-access"
       config authentication-rule
       edit 1
          set source-interface "wan1
          set source-address "all"
          set groups "Employees"
          set portal "full-access"
          set client-cert enable
       next
       edit 2
          set source-interface "wan1"
          set source-address "all"
          set groups "Vendors"
          set portal "full-access"
          set client-cert disable <-- Set by default and will not be displayed.
       next
    end
end
```

Configure the remainder of the SSL VPN tunnel as normal (creating a firewall policy allowing SSL VPN access to the internal network, including the VPN groups, necessary security profiles, etc.).

If configured correctly, only the 'Employees' group should require a client certificate to authenticate to the VPN.

Troubleshooting

This section contains tips to help you with some common challenges of SSL VPNs.

- Enter the following to display debug messages for SSL VPN:

  ```
  diagnose debug application sslvpn -1
  ```

  This command enables debugging of SSL VPN with a debug level of -1. The -1 debug level produces detailed results.

- Enter the following command to verify the debug configuration:

  ```
  diagnose debug info
  debug output: disable
  console timestamp: disable
  console no user log message: disable
  sslvpn debug level: -1 (0xffffffff)
  CLI debug level: 3
  ```

  This output verifies that SSL VPN debugging is enabled with a debug level of -1, and shows what filters are in place. The output above indicates that debug output is disabled, so debug messages are not displayed. The output also indicates that debugging has not been enabled for any software systems.

- Enter the following to enable displaying debug messages:

  ```
  diagnose debug enable
  ```

  To view the debug messages, log into the SSL VPN portal. The CLI displays debug output similar to the following:

  ```
  FGT60C3G10002814 # [282:root]SSL state:before/accept initialization (172.20.120.12)
  [282:root]SSL state:SSLv3 read client hello A (172.20.120.12)
  [282:root]SSL state:SSLv3 write server hello A (172.20.120.12)
  [282:root]SSL state:SSLv3 write change cipher spec A (172.20.120.12)
  [282:root]SSL state:SSLv3 write finished B (172.20.120.12)
  [282:root]SSL state:SSLv3 flush data (172.20.120.12)
  [282:root]SSL state:SSLv3 read finished A:system lib(172.20.120.12)
  [282:root]SSL state:SSLv3 read finished A (172.20.120.12)
  [282:root]SSL state:SSL negotiation finished successfully (172.20.120.12)
  [282:root]SSL established: DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
  ```

- Enter the following to stop displaying debug messages:

  ```
  diagnose debug disable
  ```

The following is a list of potential issues. The suggestions below are not exhaustive, and may not reflect your network topology.

There is no response from the SSL VPN URL.

- Go to **VPN > SSL-VPN Settings** and check the SSL VPN port assignment. Also, verify that the SSL VPN policy is configured correctly.
- Check the URL you are attempting to connect to. It should follow this pattern:

  ```
  https://<FortiGate IP>:<Port>/remote/login
  ```

- Ensure that you are using the correct port number in the URL.

FortiClient cannot connect.

Read the Release Notes to ensure that the version of FortiClient you are using is compatible with your version of FortiOS.

Tunnel-mode connection shuts down after a few seconds.

This issue can occur when there are multiple interfaces connected to the Internet (for example, a dual WAN). Upgrade to the latest firmware then use the following CLI command:

```
config vpn ssl settings
   set route-source-interface enable
end
```

When you attempt to connect using FortiClient or in Web mode, you are returned to the login page, or you receive the following error message: "*Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12).*"

- Ensure that cookies are enabled in your browser.
- If you are using a remote authentication server, ensure that the FortiGate is able to communicate with it.
- Access to the web portal or tunnel will fail if Internet Explorer has the privacy Internet Options set to High. If set to High, Internet Explorer will block cookies that do not have a compact privacy policy, and that use personally identifiable information without your explicit consent.

You receive an error message stating: "*Destination address of Split Tunneling policy is invalid.*"

The SSL VPN security policy uses the **ALL** address as its destination. Change the address to that of the protected network instead.

The tunnel connects but there is no communication.

Go to **Network > Static Routes** and ensure that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface.

You can connect remotely to the VPN tunnel but are unable to access the network resources.

Go to **Policy & Objects > IPv4 Policy** and examine the policy allowing VPN access to the local network. If the destination address is set to all, create a firewall address for the internal network. Change the destination address and attempt to connect remotely again.

Users are unable to download the SSL VPN plugin.

Go to **VPN > SSL-VPN Portals** to make sure that the option to **Limit Users to One SSL-VPN Connection at a Time** is disabled. This allows users to connect to the resources on the portal page while also connecting to the VPN through FortiClient.

Users are being assigned to the wrong IP range.

Ensure that the same IP Pool is used in VPN Portal and VPN Settings to avoid conflicts. If there is a conflict, the portal settings will be used.

Flow-based (vdom) AntiVirus profiles in SSL VPN web mode limitation

In flow mode vdom, SSL VPN web mode doesn't block antivirus even when `av-profile` is set (however, SSL VPN tunnel mode AV profile does work).

Sending tunnel statistics to FortiAnalyzer

By default, logged events include tunnel-up and tunnel-down status events. Other events, by default, will appear in the FortiAnalyzer report as "No Data Available". More accurate results require logs with `action=tunnel-stats`, which is used in generating reports on the FortiAnalyzer (rather than the tunnel-up and tunnel-down event logs). The FortiGate does not, by default, send `tunnel-stats` information.

To allow VPN `tunnel-stats` to be sent to FortiAnalyzer, configure the FortiGate unit as follows using the CLI:

```
config system settings
   set vpn-stats-log ipsec ssl
   set vpn-stats-period 300
end
```

HTTP header information

The X-Content-Type-Options header is added to internal pages of SSL VPN to comport with PCI-DSS compatibility. Strict-Transport-Security is added to the HTTP header for the same reason.