# SSL VPN

FortiOS™ Handbook v3

for FortiOS 4.0 MR3

***FortiOS™ Handbook: SSL VPN***

v3

24 June 2011

01-431-112804-20110624

for FortiOS 4.0 MR3



**Trademarks**

# Contents

# Introduction

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:

- Introduction to SSL VPN 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.
- Setting up the FortiGate unit 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, configure the SSL virtual interface (`ssl.root`), and describes the SSL VPN OS Patch Check feature that allows a client with a specific OS patch to access SSL VPN services.
- Using the web portal explains how to use a web portal and its widgets. Access to different network resource types, such as SMB, FTP, RDP is covered.
- Using the SSL VPN tunnel client explains how to install and use the tunnel mode clients for Windows, Linux, and Mac OS X.
- 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.

## Audience

This document is specifically addressed to system administrators responsible for configuring SSL VPN services for their business/enterprise. In addition, users who have full administrative rights over their computers and must connect to a local internal network may use this guide as a source of general SSL VPN information and also about the configuration of SSL clients.

This document is not intended for users who do not have administrative rights over their computers and therefore cannot connect to an internal network.

# Introduction to SSL VPN

Over the past several years, 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, and employees travelling across the country or around the world require timely and comprehensive access to network resources. Initial access to network resources used private networks and leased lines - options that were inflexible and costly. 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 was developed.

In the past, VPN tunneling was performed generally at the Network Layer (Layer 3) or lower, as is the case with IPsec. To enable remote access, encrypted network connectivity was established between a remote node and the internal network, thereby making the remoteness of the connection invisible to all layers above Layer 4. The applications functioned identically when users were in the office or when they were remote, except that when requests filtered to the network level, they were relayed over the network connection tied to the user's specific location. These connections required the installation and configuration of complicated client software on user's computers.

SSL VPNs establish connectivity using SSL, which functions at Levels 4 - 5 (Transport and Session). Information is encapsulated at Levels 6 - 7 (Presentation and Application), and SSL VPNs communicate at the highest levels in the OSI model. SSL is not strictly a web protocol - it is possible to use SSL to encrypt any application-level protocol.

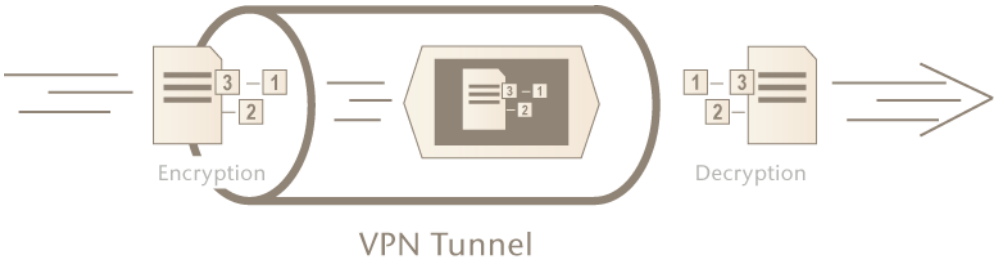
The following topics are included in this section:



## What is a VPN?

Virtual Private Network (VPN) technology 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.

**Figure 1: Encoded data going through a VPN tunnel**




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.

# What is SSL?

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.

## Goals of SSL

SSL has four main goals:

1. Confidentiality of communications
2. Integrity of data
3. Authentication of server
4. Authentication of client (non-repudiation)

Good security for a VPN requires confirming the identity of all communicating parties. You can ensure identity using password authentication (shared secrets) or digital certificates. A shared secret is a passphrase or password that is the same on both ends of a tunnel. The data is encrypted using a session key, which is derived from the shared secret. The gateways can encrypt and decrypt the data correctly only if they share the same secret. Digital certificates use public key-based cryptography to provide identification and authentication of end gateways. Cryptography, the art of protecting information by transforming it into an unreadable format, is an integral part of VPN technology. The basic building blocks of cryptographic configurations are cryptographic primitives. Cryptographic primitives are low-level cryptographic algorithms or routines that are used to configure computer security systems, such as SSL, SSH, and TLS. Each primitive is designed to do one very specific task, such as encryption of data or a digital signature on a set of data.

There are four cryptographic primitives that are specific to VPNs:

1. **Symmetric ciphers** (confidentiality) — Symmetric encryption uses a very fast block-level algorithm to encrypt and decrypt data, and is the primary primitive used to

protect data confidentiality. Both sides of the tunnel will use the same encrypt/decrypt key, which is the primary weakness of symmetric ciphers. A key is usually a large number that is fed to a cryptographic algorithm to encrypt plaintext data into ciphertext or to decrypt ciphertext data into plaintext.

2 **Asymmetric ciphers** (authenticity and non-repudiation) — To guarantee the identities of both parties in a transaction, SSL VPN uses asymmetric encryption. This involves the creation of a key pair for each party. The keys are related mathematically - data encrypted with one key can be decrypted only with the other key in the pair, and vice versa. One key is labeled the public key and can be freely distributed. The other key is the private key and it must be kept secret. The SSL VPN authenticates each party by checking that it has something that no other party should have - its private key.

   If the SSL VPN can decrypt a message from a party using that party's public key, the message must have been encrypted with that party's private key. As the private key is known only to the sending party, the sender's identity is proven. This proof of identity also makes it impossible for the sending party to later repudiate (deny sending) the message.

3 **Message digests** (integrity) — VPNs send sensitive data over the public Internet. To make sure that what is sent is the same as what is received, and vice versa, SSL VPN uses message digests. A message digest is an irreversible mathematical function that takes a message of any size and encodes it as a fixed length block of cipher text. The fixed length cipher is called the digest. It is essentially a cryptographic "summary" of the message. Every message has only one digest and no two messages should ever create the same digest — if only a single letter of our message is changed, the entire message digest will be different.

4 **Digital signatures** (authenticity and non-repudiation) — A digital signature or digital signature scheme is a type of asymmetric cryptography. For messages sent through an insecure channel, a correctly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. The signer cannot claim they did not sign a message, while also claiming their private key remains secret. In some cases, a non-repudiation scheme offers a time stamp for the digital signature, so that even if the private key is exposed, the signature is still valid.

In addition to identifying the user, authentication also defines the resources a user can access. A user must present specified credentials before being allowed access to certain locations on the network. Authentication can either take place through a firewall or through an external authentication server such as Remote Authentication Dial-In User Service (RADIUS). An authentication server is a trusted third party that provides authentication services to other systems on a network.

## SSL certificates

SSL certificates are a mechanism by which a web server can prove to users that the public key that it offers them for use with the SSL is in fact the public key of the organization with which the user intends to communicate. A trusted third-party signs the certificate thereby assuring users that the public key contained within the certificate belongs to the organization whose name appears in the certificate. Upon receiving a certificate from Your Company, a user can know for sure that the key within the certificate is Your Company's key and it is safe to use to encrypt any communications related to establishment of a session key. The web server transmits their public key to users at the beginning of an SSL session using an SSL certificate.

Encryption level is determined by the length of the encryption key. The longer the key, the stronger the encryption level, and the greater the security provided. Within a VPN, after the end points on a tunnel agree upon an encryption scheme, the tunnel initiator encrypts the packet and encapsulates it in an IP packet. The tunnel terminator recovers the packet, removes the IP information, and then decrypts the packet.

### Choosing the level of security for your SSL VPN tunnel

Performance and security requirements will dictate the level of encryption used in a particular configuration. Stronger encryption provides a greater level of security but impacts performance levels. For general-purpose tunnels, over which no sensitive data is to be passed, base encryption provides adequate security with good performance. For administrative and transactional connections, where exposure of data carries a high risk, strong encryption is recommended.

## Choosing between SSL and IPsec VPN

The FortiGate unit supports both SSL and IPsec VPN technologies. Each combines encryption and VPN gateway functions to create private communication channels over the Internet. Both enable you to define and deploy network access and security policies using a single management tool. In addition, both support a simple client/user authentication process (including optional X.509 security certificates). You have the freedom to use both technologies; however, one may be better suited to the requirements of your situation.

In general, IPsec VPNs are a good choice for site-to-site connections where appliance-based firewalls or routers are used to provide network protection, and company-sanctioned client computers are issued to users. SSL VPNs are a good choice for roaming users who depend on a wide variety of thin-client computers to access enterprise applications and/or company resources from a remote location.

SSL and IPsec VPN tunnels may operate simultaneously on the same FortiGate unit.

### Legacy versus web-enabled applications

IPsec is well suited to network-based legacy applications that are not web-based. As a Layer 3 technology, IPsec creates a secure tunnel between two host devices. IP packets are encapsulated by the VPN client and server software running on the hosts.

SSL is typically used for secure web transactions in order to take advantage of web-enabled IP applications. After a secure HTTPS link has been established between the web browser and web server, application data is transmitted directly between selected client and server applications through the tunnel.

### Authentication differences

IPsec is a well-established technology with robust features that support many legacy products such as smart cards and biometrics.

SSL supports a web single sign-on to a web portal front-end, from which a number of different enterprise applications may be accessed. The Fortinet implementation enables you to assign a specific port for the web portal and to customize the login page if desired.

### Connectivity considerations

IPsec supports multiple connections to the same VPN tunnel—a number of remote VPN devices effectively become part of the same network.

SSL forms a connection between two end points such as a remote client and an enterprise network. Transactions involving three (or more) parties are not supported because traffic passes between client and server applications only.

### Relative ease of use

Although managing IPsec VPNs has become easier, configuring SSL VPNs is simple in comparison. IPsec protocols may be blocked or restricted by some companies, hotels, and other public places, whereas the SSL protocol is usually unrestricted.

### Client software requirements

Dedicated IPsec VPN software must be installed on all IPsec VPN peers and clients and the software has to be configured with compatible settings.

To access server-side applications with SSL VPN, the remote user must have a web browser (Internet Explorer, Netscape, or Mozilla/Firefox), and if Telnet//RDP are used, Sun Java runtime environment. Tunnel-mode client computers must also have ActiveX (IE) or Java Platform (Mozilla/Firefox) enabled.

### Access control

IPsec VPNs provide secure network access only. Access to the network resources on a corporate IPsec VPN can be enabled for specific IPsec peers and/or clients. The amount of security that can be applied to users is limited.

SSL VPNs provide secure access to certain applications. Web-only mode provides remote users with access to server applications from any thin client computer equipped with a web browser. Tunnel-mode provides remote users with the ability to connect to the internal network from laptop computers as well as airport kiosks, Internet cafes, and hotels. Access to SSL VPN applications is controlled through user groups.

### Session failover support

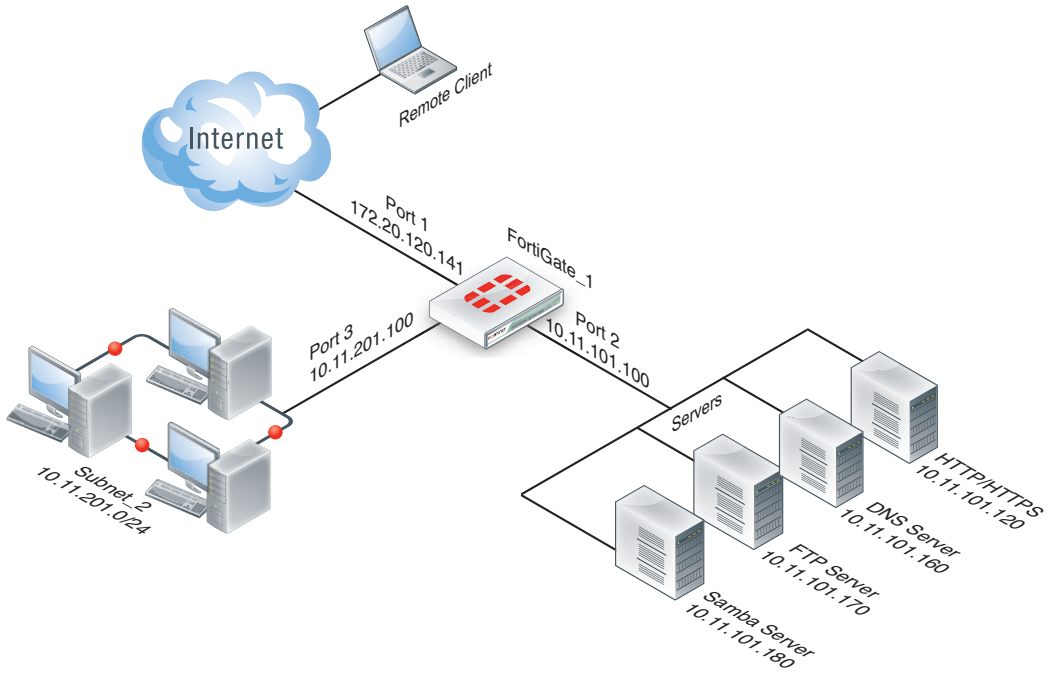
In a FortiGate high availability (HA) cluster with session pickup enabled, session failover is supported for IPsec VPN tunnels. After an HA failover, IPsec VPN tunnel sessions will continue with no loss of data.

Session failover is not supported by SSL VPN tunnels, however cookie failover is supported for communication between the SSL VPN client and the FortiGate unit. This means that after a failover, the SSL VPN client can re-establish the SSL VPN session without having to authenticate again. However, all sessions inside the SSL VPN tunnel with resources behind the FortiGate unit will stop, and will therefore have to be restarted.

## General topology

In the most common SSL VPN Internet scenario, the remote client connects to the Internet through an ISP that offers connections with dynamically assigned IP addresses. The client's packets are routed to the public interface of the FortiGate unit. For example, Figure 2 shows a FortiGate gateway that can be reached by a mobile user.

**Figure 2: Example SSL VPN configuration**




At the FortiGate unit, you configure a user group for SSL VPN authentication and define security policies for each network resource that users are permitted to access.

You can easily expand the resources available to your users by adding or changing security policies. If you want to provide different resource access to different users, you can create multiple user groups.

The general infrastructure requirements are quite simple:

- The FortiGate unit must be operating in NAT/Route mode and have a static public IP address.
- The ISP assigns IP addresses to remote clients before they connect to the FortiGate unit.

# SSL VPN modes of operation

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on user name, 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 (see “Web-only mode” on page 15) or tunnel mode (see “Tunnel mode” on page 15).

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.

You can enable a cache cleaner to remove any sensitive data that would otherwise remain on the remote computer after the session ends. For example, all cache entries, browser history, cookies, encrypted information related to user authentication, and any temporary data generated during the session are removed from the remote computer. If the client's browser cannot install and run the cache cleaner, the user is not allowed to access the SSL-VPN portal.

## 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.

Support for SSL VPN web-only mode is built into the FortiOS operating system. 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 HTTP/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 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. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

FortiGate SSL VPN web portals have a 1- or 2-column page layout with selectable color schemes. 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 enabling the SSL VPN feature and 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.

For information about client operating system and browser requirements, see the Release Notes for your FortiGate firmware.

For information on configuring a web portal see "Customizing the web portal login page" on page 25.

## Tunnel mode

Tunnel mode offers remote users the freedom to connect to the internal network using the traditional means of web-based access from laptop computers, as well as from airport kiosks, hotel business centers, and Internet cafés. If the applications on the client computers used by your user community vary greatly, you can deploy a dedicated SSL VPN client to any remote client through its web browser. 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 web browser and the FortiGate unit. Also available 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.

In tunnel mode, remote clients connect to the FortiGate unit and the web portal login page using Microsoft Internet Explorer, Mozilla Foundation/Firefox, Mac OS, or Linux. The FortiGate unit acts as a secure HTTP/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 dictated by the user group settings. If the user does not have the SSL VPN client installed, they will be prompted to download the SSL VPN client (an ActiveX or Java plugin) and install it using controls provided through the web portal. SSL VPN tunnel mode can also be initiated from a standalone application on Windows, Mac OS, and Linux.

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.

**Note:** If the tunnel mode and session information widgets are the only widgets configured, the user will automatically be logged into the SSL-VPN tunnel.

Configuring the FortiGate unit to establish a tunnel with remote clients involves enabling the feature through SSL VPN configuration settings and selecting the appropriate web portal configuration for tunnel-mode access in the user group settings. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

**Note:** The user account used to install the SSL VPN client on the remote computer must have administrator privileges.

**Note:** If you are using Windows Vista, you must disable UAC (User Account Control) before installing the SSL VPN tunnel client. This UAC setting must be disabled before the SSL VPN tunnel client is installed. IE7 in Windows Vista runs in Protected Mode by default. To install SSL VPN client ActiveX, you need to launch IE7 by using 'Run as administrator' (right-click the IE7 icon and select 'Run as administrator').

For information about client operating system requirements, see the Release Notes for your FortiGate firmware.

For information on configuring tunnel mode, see “Configuring tunnel mode settings” on page 30.

## Port forwarding mode

While tunnel mode provides a Layer 3 tunnel that users can run any application over it, 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, using an email client that needs to communicate with a POP3 server. The port foreward 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.

**Note:** 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.

For information on configuring a port forward tunnel, see "Configure a port forward tunnel" on page 32.

### 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, an 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.

## Single Sign On (SSO)

The web portal can provide bookmarks to connect to network resources. A web (HTTP/HTTPS) bookmark can include login credentials so that the FortiGate unit automatically logs the user into the web site. 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 "Adding bookmarks" on page 56.

# Setting up the FortiGate unit

Before you begin, install your choice of HTTP/HTTPS, telnet, SSH, FTP, SMB/CIFS, VNC, and/or RDP server applications on the internal network. As an alternative, these services may be accessed remotely through the Internet. All services must be running to be accessible. Users must have individual user accounts to access the servers (these user accounts are not related to FortiGate user accounts or FortiGate user groups). For information about creating such user accounts, refer to the documentation for the server applications or Internet-based services.

You can configure and manage the FortiGate unit through a secure HTTP (HTTPS) connection from any computer running a web browser. For information about how to connect to the web-based manager, see “Connecting to the web-based manager” in the *System Administration* Guide.

**Note:** As an alternative, you can connect the management computer to the Console connector of the FortiGate unit directly using a serial cable and configure the FortiGate unit through the Command Line Interface (CLI). The CLI can also be launched from within the web-based manager. For more information, see “Connecting to the FortiGate console” in the *FortiGate CLI Reference*.

For information on changing the password, configuring the interfaces of the FortiGate unit, and assigning basic operating parameters, including a default gateway, the *System Administration* Guide.

See also to the chapter, “Examples” on page 71, for example SSL VPN configurations.

This section describes how to configure the FortiGate unit as an SSL VPN server. The following topics are included in this section:

- General configuration steps
- Configuring SSL VPN settings
- Configuring SSL VPN web portals
- Configuring user accounts and user groups for SSL VPN
- Configuring security policies
- SSL VPN logs
- Monitoring active SSL VPN sessions
- Troubleshooting

# SSL VPN and IPv6

FortiOS supports SSL VPN using IPv6 addressing using IPv6 configurations for security policies and addressing including:

- Policy matching for IPv6 addresses
- Support for DNS resolving in SSL VPN
- Support IPv6 for ping
- FTP applications
- SMB
- Support IPV6 for all the java applets (Telnet, VNC, RDP and so on)

# General configuration steps

For best results in configuring FortiGate SSL VPN technology, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Enable SSL VPN connections and set the basic options needed to support SSL VPN configurations.

   See “Configuring SSL VPN settings” on page 20.
2. Create a web portal to define user access to network resources.

   If you want to provide different types of access to different groups of users, you need to create multiple web portals. See “Configuring SSL VPN web portals” on page 27.
3. Create user accounts for the remote clients.

   Create SSL VPN user groups and associate them with the web portal or portals that you created. Assign users to the appropriate SSL VPN user groups. See “Configuring user accounts and user groups for SSL VPN” on page 41.
4. Configure the security policies and the remaining parameters needed to support the VPN mode of operation.

   See “Configuring security policies” on page 42.
5. For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.

   See “Configuring routing for tunnel mode” on page 47.
6. Optionally, define SSL VPN event-logging parameters, and monitor active SSL VPN sessions.

   See SSL VPN logs, and “Monitoring active SSL VPN sessions” on page 51.

If you have problems during SSL VPN configuration in this chapter, see “Troubleshooting” on page 52 for assistance.

# Configuring SSL VPN settings

To configure SSL VPN operation, you must at minimum perform the following procedures:

- “Enabling SSL VPN operation” on page 21.
- “Specifying an IP address range for tunnel-mode clients” on page 21 (required only for tunnel-mode).

As part of the SSL VPN configuration, you can also make the modifications described in the following sections:

- "Adding WINS and DNS services for clients" on page 22.
- "Setting the idle timeout setting" on page 23.
- "Setting the client authentication timeout" on page 23.
- "Specifying the cipher suite for SSL negotiations" on page 23.
  The cipher suite determines the level of data security, but it must be compatible with the capabilities of the clients' browsers.
- "Enabling strong authentication through X.509 security certificates" on page 24.
- "Changing the port number for web portal connections" on page 25.
  By default, SSL VPN connections use port 10443.
- "Customizing the web portal login page" on page 25.

Most of these settings are on the *VPN* > *SSL* > *Config* page in the web-based manager and `config vpn ssl settings` in the CLI. You can configure multiple settings at the same time.

## Enabling SSL VPN operation

You must enable SSL VPN operation so that the FortiGate unit will respond to SSL VPN connection requests. Also, some elements of SSL VPN configuration are not available unless SSL VPN is enabled. Selecting the default SSL VPN settings will be sufficient for our purposes here.Enabling SSL VPN is performed using the CLI.

### To enable SSL VPN operation - CLI

```
config vpn ssl settings
  set sslvpn-enable enable
end
```

## Specifying an IP address range for tunnel-mode clients

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

You can specify tunnel-mode IP Pools in two places:

- The *VPN* > *SSL* > *Config* page *IP Pools* setting applies to all web portals that do not specify their own IP Pools.
- The web portal Tunnel Mode widget *IP Pools* setting, if used, applies only to the web portal and overrides the setting in *VPN* > *SSL* > *Config*. See "Configuring tunnel mode settings" on page 30.

**Caution:** 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 *Firewall Objects* > *Address* > *Address* and select *Create New*.

2 Enter an *Address Name*, for example, `SSL_VPN_tunnel_range`.

3 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]`.

4 In *Interface*, select *Any*.

5 Select *OK*.

6 Go to *VPN* > *SSL* > *Config*.

7 In *IP Pools*, select *Edit*.

**Note:** When you select Edit, a popup window will open. If your browser blocks popup windows, you will have to unblock it to continue with the following steps.

8 In the *Available* list, select the address you created for the SSL VPN tunnel range and then select the down arrow button to move it to the *Selected* list. Select *OK*.

9 Select *Apply*.

**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
end
config vpn ssl settings
  set tunnel-ip-pools SSL_tunnel_users
end
```

## 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* > *Config*.

2 Select the *Expand Arrow* to display the *Advanced* section.

3 Enter the IP addresses of DNS servers in the *DNS Server* fields as needed.

4 Enter the IP addresses of WINS servers in the *WINS Server* fields as needed.

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
```

## Setting the idle timeout setting

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 300 seconds (5 minutes) or less.

**To set the idle timeout - web-based manager**

1 Go to *VPN* > *SSL* > *Config*.

2 In the *Idle Timeout* 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
```

## Setting the client authentication timeout

The client authentication timeout controls how long an authenticated connection 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.

**Note:** 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:

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

## Specifying the cipher suite for SSL negotiations

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.

**To set the encryption algorithm - web-based manager**

1 Go to *VPN* > *SSL* > *Config*.

2 In *Encryption Key Algorithm*, select one of the following options:

- *Default - RC4(128 bits) and higher*

  If the web browser on the remote client is capable of matching a 128-bit or greater cipher suite.
- *High - AES(128/256 bits) and 3DES*

If the web browser on the remote client is capable of matching a high level of SSL encryption. This option enables cipher suites that use more than 128 bits to encrypt data.

- *Low - RC4(64 bits), DES and higher*

  If you are not sure which level of SSL encryption the remote client web browser supports. The web browser must at least support a 64-bit cipher length.

3 Select *Apply*.

**To set the encryption algorithm - CLI**

```
config vpn ssl settings
  set algorithm {default | high | low}
end
```

## Enabling strong authentication through X.509 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. Similarly, the client can require the FortiGate unit to authenticate using a certificate.

For information about obtaining and installing certificates, see the *User Authentication Guide*.

### Configuring the FortiGate unit to require strong client authentication

To require clients to authenticate using certificates, select the *Require Client Certificate* option in *SSL VPN settings*. 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* > *Config*.

2 Select *Require Client Certificate*.

3 Select *Apply*.

**To require client authentication by security certificates - CLI**

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

### Configuring the FortiGate unit to provide strong authentication

If your SSL VPN clients require strong authentication, the FortiGate unit must offer a certificate for which the client browser has the CA certificate 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 (self-signed) certificate from Fortinet to remote clients when they connect.

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

1 Go to *VPN* > *SSL* > *Config*.

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
```

## Changing the port number for web portal connections

You can optionally 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 10443 and users can access the web portal login page using the following default URL:

`https://<FortiGate_IP_address>:10443/remote/login`

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

**Note:** If you change the TCP port number, remember to notify your SSL VPN clients. They must use the new port number to connect to the FortiGate unit.

**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* > *Config*.

3 Type an unused port number in *SSLVPN Login Port*, and select *Apply*.

**Note:** Do not select port number 443 for user access to the web portal login page. Port number 443 is reserved to support administrative connections to the FortiGate unit through the web-based manager.

**To change the SSL VPN port - CLI**

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

```
config global
  config system global
    set sslvpn-sport 10443
  end
```

## Customizing the web portal login page

The default web portal login page shows only the Name and Password fields and the Login button, centred in the web browser window. You can customize the page with your company name or other information.

The login page is a replacement message composed of HTML code, which you can modify. Global replacement messages apply to all VDOMs by default, but individual VDOMs can define their own messages.

**To configure the SSL VPN login page - web-based manager**

1 If you want to edit the global login page and *Current VDOM* appears at the bottom left of the screen, select *Global* from the list of VDOMs.

2 Go to *System* > *Config* > *Replacement Messages*.

3 Expand the *SSL VPN* row and select the *Edit* icon for the *SSL VPN login message*.

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

4 Edit the HTML text, subject to the following restrictions:

- The login page must be an HTML page containing a form with `ACTION="%%SSL_ACT%%"` and `METHOD="%%SSL_METHOD%%"`
- The form must contain the `%%SSL_LOGIN%%` tag to provide the login form.
- The form must contain the `%%SSL_HIDDEN%%` tag.

5 Select *OK*.

### To configure the SSL VPN login page - CLI

Do one of the following:

- If VDOMs are enabled and you want to modify the global login page, enter:

```
config global
config system replacemsg sslvpn sslvpn-login
```

- If you want to modify the login page for a VDOM, enter:

```
config vdom
edit <vdom_name>
  config system replacemsg-group
  edit default
    config sslvpn
      edit sslvpn-login
```

To change the login page content, enter the modified page content as a string. In this example, the page title is changed to “Secure Portal login” and headings are added above the login dialog which say “example.com Secure Portal”:

```
    set buffer "<html><head><title>Secure Portal login</title>
       <meta http-equiv="Pragma" content="no-cache"><meta http-
       equiv="cache-control" content="no-cache"> <meta http-
       equiv="cache-control" content="must-revalidate"><link
       href="/sslvpn/css/login.css" rel="stylesheet"
       type="text/css"><script type="text/javascript">if (top &&
       top.location != window.location) top.location =
       top.location;if (window.opener && window.opener.top) {
       window.opener.top.location = window.opener.top.location;
       self.close(); }</script></head><body class="main">
       <center><table width="100%" height="100%" align="center"
       class="container" valign="middle" cellpadding="0"
       cellspacing="0"><tr valign=top><td align=center>
       <h1>example.com</h1><h3>Secure Portal</h3></td></tr><tr
       valign=top><td><form action="%%SSL_ACT%%"
       method="%%SSL_METHOD%%" name="f"><table class="list"
       cellpadding=10 cellspacing=0 align=center width=400
       height=180>%%SSL_LOGIN%%</table>%%SSL_HIDDEN%%</td></tr></
       table></form></center></body><script>document.forms[0].use
       rname.focus();</script></html>"
end
```

Your console application determines how the text wraps. It is easier to edit the code in a separate text editor and then paste the finished code into the `set buffer` command. Be sure to enclose the entire string in quotation (") marks.

# Configuring SSL VPN web portals

A web portal defines SSL VPN user access to network resources, such as HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP and SSH. The portal configuration determines what SSL VPN users see when they log in to the FortiGate. Both the FortiGate administrator and the SSL VPN user have the ability to customize the web portal.

At minimum, you need to set up one web portal. For each portal, you can configure additional security features:

- "Host checking" on page 36
  Check that client computers are running security software.
- "Configuring cache cleaning" on page 38
  Remove session information from the client's computer after logout.
- "Configuring virtual desktop" on page 39
  Provide a separate Windows desktop environment while connected to the VPN. Control which applications users can run on their virtual desktop using virtual desktop application control.
- "Configuring client OS Check" on page 40
  Check that the client's Windows operating system is up-to-date.

## Before you begin

To begin configuring web portals, you need to know how many distinct sets of user access privileges you need. For example, you might have users who are allowed only RDP access to their desktop PCs, other users who have access to office file shares, and a third category of users who will have both types of access. In this case, you need to create a web portal for each of these access types. Later, you will create SSL VPN user groups that assign the users to the appropriate portal.

One of the predefined web portals might meet your needs. See "Default web portal configurations" on page 27. If needed, you can modify these portals using the procedures in this section.

## Default web portal configurations

There are three predefined default web portal configurations available:

- *full-access*: Includes all widgets available to the user - *Session Information*, *Connection Tool*, *Bookmarks*, and *Tunnel Mode*.
- *tunnel-access*: Includes *Session Information* and *Tunnel Mode* widgets.
- *web-access*: Includes the *Session Information* widget.

You can modify a default portal or a portal that you have already defined. Select the *Edit* icon next to the web portal in the *Portal* list. The SSL VPN web portal you select will open.

**To configure basic web portal settings - web-based manager**

1. Go to *VPN* > *SSL* > *Portal* and select *Edit*.
2. Select *Settings*.
3. Enter the following information:

| | |
|---|---|
| **Name** | Enter a name to identify this web portal. |
| **Applications** | Select the applications that users can access through this web portal. |
| **Portal Message** | Enter the text that will appear at the top of the web portal window to a maximum of 31 characters. |
| **Theme** | Select the color scheme for this web portal. |
| **Page Layout** | Select either the single-column or two-column layout. |
| **Redirect URL** | The web portal can display a second HTML page in a popup window when the web portal home page is displayed. Enter the URL. |

4 Optionally, you can select the *Virtual Desktop* tab to configure the Virtual Desktop feature. See "Configuring virtual desktop" on page 39. Or, you can leave this configuration for later.

5 Optionally, you can select the *Security Control* tab to configure cache cleaning and client check. Or, you can leave this configuration for later.

For information on these features, see "Configuring cache cleaning" on page 38 and "Host checking" on page 36.

6 Select *OK* then *Apply*.

### To configure basic web portal settings - CLI

To use the orange theme with a two-column layout and allow users all types of access with the full-access portal, you could enter:

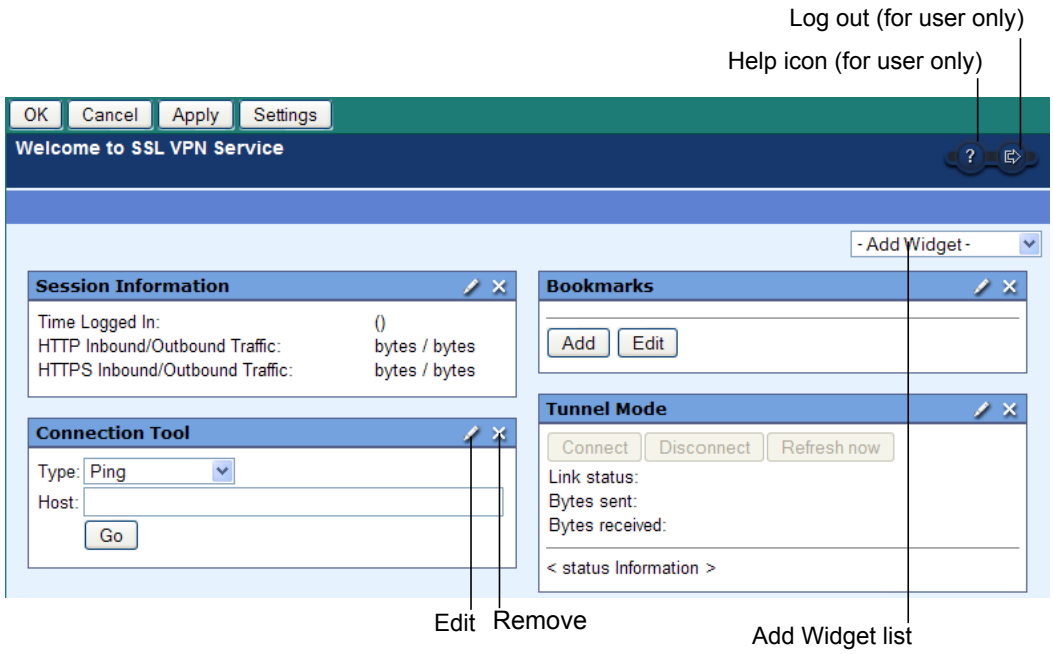
```
config vpn ssl web portal
  edit full-access
    set allow-access ftp ping rdp smb ssh telnet vnc web
    set heading "Welcome to the example.com web portal"
    set theme orange
    set page-layout double-column
  end
```

In the `config vpn ssl web portal` command, you can also configure client check, client OS check, cache cleaning, and virtual desktop. Or, you can leave this configuration for later. These features are described later in this chapter.

## Configuring the web portal page layout

You can determine which widgets are displayed on the web portal page and adjust the layout.

**Figure 3: Configuring the SSL VPN web portal page**




### To configure the web portal page - web-based manager

On the web portal page itself, you, as administrator, can make several adjustments to the appearance of the portal:

- Arrange widgets on the page by dragging them by their title bar.
- Add a widget by choosing a widget from the *Add Widget* list.
- Remove a widget by selecting the *Remove* icon in the widget title bar.
- Configure a widget by selecting the *Edit* icon in the widget title bar. For configuration information about each widget type, see the following sections:
  - “Configuring tunnel mode settings” on page 30
  - “The Session Information widget” on page 33
  - “The Connection Tool widget” on page 35
- To modify the color scheme and other basic settings, select the *Settings* button. You can also configure several advanced features. For more information, see
  - “The Connection Tool widget” on page 35
  - “Configuring cache cleaning” on page 38
  - “Configuring virtual desktop” on page 39
  - “Configuring client OS Check” on page 40 (CLI only)

When you have finished configuring the web portal page, select *Apply* to save the modifications.

**To configure the web portal page - CLI**

You can also define a portal layout using CLI commands. Unlike configuring with the web-based manager, a new portal created in the CLI has by default no heading and no widgets. Also, the widgets do not have default names. You must specify all of this information.

For example, to create the portal layout shown in Figure 3 on page 29, you would enter:

```
config vpn ssl web portal
  set heading "Welcome to SSL VPN Service"
  set page-layout double-column
  set theme blue
  edit myportal
    config widget
      edit 0
        set type info
        set name "Session Information"
        set column one
      next
      edit 0
        set type bookmark
        set name "Bookmarks"
        set column one
      next
      edit 0
        set type tunnel
        set name "Tunnel Mode"
        set column two
      next
      edit 0
        set type tool
        set name "Connection Tool"
        set column two
      end
```

**Note:** When you use `edit 0`, as in this example, the CLI automatically assigns an unused index value when you exit the edit shell by typing `end`.

## Configuring tunnel mode settings

If your web portal provides tunnel mode access, you need to configure the Tunnel Mode widget. These settings determine how tunnel mode clients are assigned IP addresses.

If this web portal will assign a different range of IP addresses to clients than the IP Pools you specified on the *VPN* > *SSL* > *Config* page, you need to define a firewall address for the IP address range that you want to use. You will then need to specify this address in the Tunnel Mode widget *IP Pools* setting.

**Note:** If the tunnel mode and session information widgets are the only widgets configured, the user will automatically be logged into the SSL-VPN tunnel.

Optionally, you can enable a split tunneling configuration so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route.

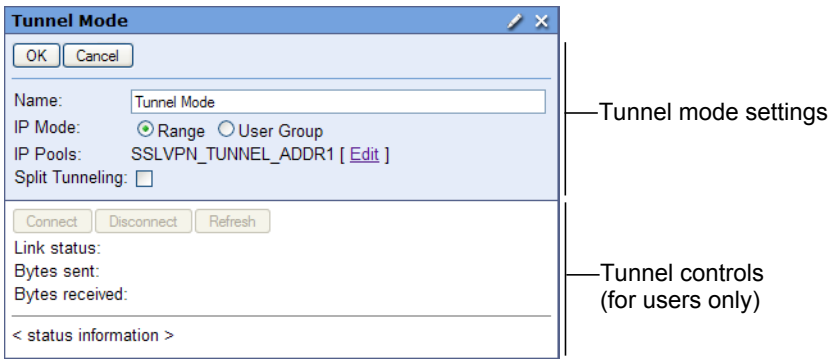
### To configure tunnel mode settings - web-based manager

1 Go to *VPN* > *SSL* > *Portal* and select *Create New*.

2 If the Tunnel Mode widget is missing, add it by selecting *Tunnel Mode* from the *Add Widget* list in the top right corner of the window.

3 Select the *Edit* icon in the *Tunnel Mode* widget title bar.

**Figure 4: Tunnel Mode widget - edit mode**




4 Enter the following information:

**Name** Enter a name for the *Tunnel Mode* widget. The default is “Tunnel Mode”.

**IP Mode** Select the mode by which the IP address is assigned to the user.

**Range** The user IP address is allocated from the IP address ranges specified by *IP Pools*.

**User Group** The user is assigned the IP address specified in the Framed-IP-Address field of the user’s record on the RADIUS server. This option is valid only for users authenticated by a RADIUS server.

**IP Pools** Leave this field empty to use the IP address range specified by the *IP Pools* field on the *VPN* > *SSL* > *Config* page.

If you want to specify an IP address range for clients of this portal only, select *Edit*. From the *Available* list, select the appropriate firewall address. You must configure the desired IP address range as a firewall address before you can select it here.

**Split Tunneling** Select to enable split tunneling. When enabled, only traffic that requires the SSL VPN is sent through the tunnel. Other traffic follows the user’s regular routing.

When split tunneling is disabled, all of the user’s traffic with other networks passes through the tunnel. This does not affect traffic between the user’s computer and hosts on the local network.

For enhanced security, some administrators prefer to force all traffic through the SSL VPN tunnel, including traffic between the user and the user’s local network. To do this, use the CLI tunnel mode settings to enable `exclusive-routing`.

The remaining items in the widget are controls that are available to the user during an SSL VPN session.

5 Select *OK* in the *Tunnel Mode* widget.

6 Select *Apply*.

**To configure tunnel mode settings - CLI**

To enable tunnel mode operation for portal2 portal users and assign them addresses from the `SSLVPN_TUNNEL_ADDR2` range, you would enter:

```
config vpn ssl web portal
  edit portal2
    config widget
      edit 0
        set type tunnel
        set tunnel-status enable
        set ip-mode range
        set ip-pools SSLVPN_TUNNEL_ADDR2
      end
  end
```

The preceding example applies to a web portal that does not already have a tunnel mode widget. To modify the settings on an existing tunnel mode widget, you need to determine the widget's number. Enter:

```
config vpn ssl web portal
  edit portal1
    config widget
    show
```

In the output, you will see, for example,

```
      edit 3
        set name "Tunnel Mode"
        set type tunnel
        ...
```

You can now enter `edit 3` and modify the tunnel mode widget's settings.

**To force all traffic through the tunnel - CLI**

If you disable split tunneling, all of the user's traffic to other networks passes through the SSL VPN tunnel. But, this does not apply to traffic between the user and the user's local network. For enhanced security, some administrators prefer to force all of the user's traffic, including traffic with the local network, to pass through the SSL VPN tunnel. To do this, enable `exclusive-routing` in the tunnel widget settings. For example:

```
config vpn ssl web portal
  edit portal2
    config widget
      edit 0
        set type tunnel
        set tunnel-status enable
        set ip-mode range
        set ip-pools SSLVPN_TUNNEL_ADDR2
        set split-tunneling disable
        set set exclusive-routing enable
      end
  end
```

## Configure a port forward tunnel

Port forwarding provides a method of connecting to application servers without configuring a tunnel mode connection, and requiring the installation of tunnel mode client. Set up the portal as described at "Configuring SSL VPN web portals" on page 27.To configure the application, create a bookmark with the *Type* of *PortForward*.

**To configure a port forward tunnel - web-based manager**

1 Go to *VPN* > *SSL* > *Portal* and select an existing web portal configuration.
2 Select to add a bookmark.
3 Enter the *Name* of the application.
4 Select the *Type* of *PortForward*.
5 Enter the *Location* of the server.
6 Entre the *Remote Port* of the server and the *Listening Port* on the user's PC.
7 Select *OK*.

**To configure a port forward tunnel - CLI**

```
...
  config bookmarks
    edit <bookmark_name>
      set apptype portforward
      set host <hostname_or_IP>
      set remote-port <server_port>
      set listening-port <client_port>
    next
end
```

## The Session Information widget

The *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 of HTTP and HTTPS. You can change the widget name.

To edit the session information, in the *Session Information* widget select *Edit* and enter the session name.

**To configure Session Information settings - CLI**

To change the name of the web-access Session Information widget to "My Session", you would enter:

```
config vpn ssl web portal
  edit web-access
    config widget
      edit 4
        set name "My Session"
      end
```

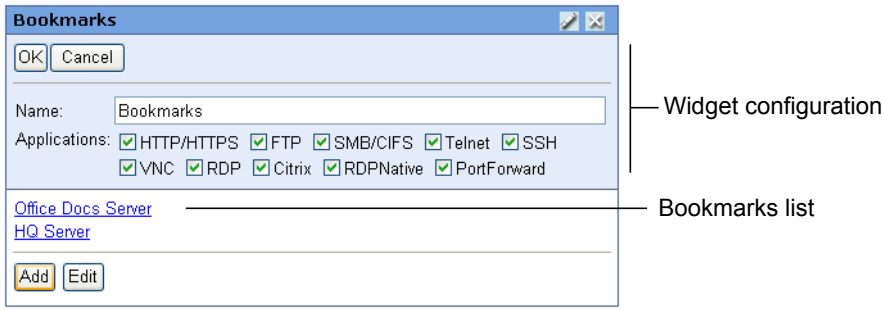
## The Bookmarks widget

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, VNC, and RDP all pop up a window that requires a browser plug-in. FTP and Samba replace the bookmarks page with an HTML file-browser.

**To configure the Bookmarks widget**

1 Go to *VPN* > *SSL* > *Portal*, and select *Create New*.
2 If the *Bookmarks* widget is missing, add it by selecting *Bookmarks* from the *Add Widget* list in the top right corner of the web portal window.

3 Select the *Edit* icon in the *Bookmarks* widget title bar.




4 Optionally, you can change the *Name* of the *Bookmarks* widget.

5 Select the *Applications* check boxes for the types of bookmarks that you want to support.

6 To add a bookmark, select *Add*.

7 Enter or edit the following information:

| | |
|---|---|
| **Name** | Enter a name for the bookmark. |
| **Type** | Select the type of application to which the bookmark links. For example, select HTTP/HTTPS for a web site.<br>Only the application types that you configured for this widget are in the list. You can select Edit in the widget title bar to enable additional application types. |
| **Location** | Enter the destination of the bookmark. |
| **Description** | Optionally, enter a descriptive tooltip for the bookmark. |
| **SSO** | A Single Sign-On (SSO) bookmark automatically enters the login credentials for the bookmark destination. Select one of:<br>**Disabled** — This is not an SSO bookmark.<br>**Automatic** — Use the user's SSL VPN credentials for login.<br>**Static** — Use the login credentials defined below. |

***Single Sign-On settings available when SSO is Static***

| | |
|---|---|
| **Field Name** | Enter a required login page field name, "User Name" for example. |
| **Value** | Enter the value to enter in the field identified by *Field Name*.<br>If you are an administrator configuring a bookmark for users:<br>• Enter `%usrname%` to represent the user's SSL VPN user name.<br>• Enter `%passwd%` to represent the user's SSL VPN password. |
| **Add** | Enter another *Field Name* / *Value* pair, for the password for example.<br>A new set of *Field Name* / *Value* fields is added. Fill them in. |

8 Select *OK*.

9 Select *Apply* at the top of the web portal page to save the changes that you made.

### To configure the Bookmarks widget and add/edit bookmarks - CLI

To allow only FTP and web connections on the web-access portal and to configure a bookmark to example.com, you would enter:

```
config vpn ssl web portal
  edit web-access
    config widget
      edit 1
        set type bookmark
        set allow-apps ftp web
```

```
    config bookmarks
      edit "example"
        set apptype web
        set description "example bookmark"
        set url "http://example.com"
      end
    end
  end
```

**To delete bookmarks - CLI**

To delete the bookmark added above, you would enter:

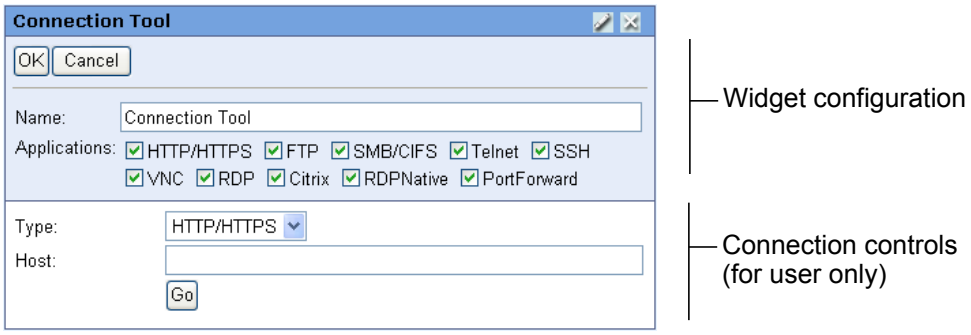
```
config vpn ssl web portal
  edit web-access
    config widget
      edit 1
        config bookmarks
          delete example
        end
      end
    end
```

## The Connection Tool widget

The *Connection Tool* enables a user to connect to resources for which there are no bookmarks.

**To configure the Connection Tool widget**

1. Go to *VPN* > *SSL* > *Portal*, and select *Create New*.
2. If the *Connection Tool* widget is missing, add it by selecting *Connection Tool* from the *Add Widget* list in the top right corner of the web portal window.
3. Select the *Edit* icon in the *Connection Tool* widget title bar.




4. Optionally, enter a new *Name* for the widget.
5. Select the types of *Applications* that the Connection Tool is enabled to access.
6. Select *OK*.

**To configure the Connection Tool widget - CLI**

To change, for example, the full-access portal Connection Tool widget to allow all application types except Telnet, you would enter:

```
config vpn ssl web portal
  edit full-access
    config widget
      edit 3
        set allow-apps ftp rdp smb ssh vnc web
      end
    end
  end
```

## Host checking

Host checking enables you to increase the security of your network, by verifying the SSL VPN client has a specific antivirus, firewall or other software installed on their computers. Only clients that meet the requirements are permitted to log on. When the client attempts to log in to the VPN network, FortiOS uses the host check information to verify a specific application and/or version is installed on the client computer. If not, the user cannot log into the portal.

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

**To configure host checking - web-based manager**

1. Go to *VPN* > *SSL* > *Portal*.
2. Select the web portal and then select *Edit*.
3. Select the *Settings* button.
4. Select the *Security Control* tab and enter the following information:

| | |
|---|---|
| **Host Check** | Select the type of host check to perform. |
| **AV** | Check for a running antivirus application recognized by the Windows Security Center. |
| **FW** | Check for a running firewall application recognized by the Windows Security Center. |
| **AV-FW** | Check for both an antivirus application and a firewall application recognized by the Windows Security Center. |
| **Custom** | Check for security applications that you choose from the *VPN* > *SSL* > *Host Check* page. See the *Policy* field. |
| **None** | Select to disable host checking. |
| **Interval** | Select how often to recheck the host. Range is every 120 seconds to 259 200 seconds. Enter 0 to not recheck the host during the session. |
| **Policy** | This field is available if *Host Check* is *Custom*. It lists the acceptable security applications for clients.<br>Select *Edit* to choose the acceptable security applications. Use the arrow buttons to move applications between the *Available* and *Selected* lists. Clients will be checked for the applications in the *Selected* list. Select *OK*.<br>The *Available* list contains the applications from *VPN* > *SSL* > *Host Check* page. You can add or remove applications from the Host Check list. See "Configuring the custom host check list" on page 37. |

5. Select *OK*.

### 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
```

## Configuring the custom host check list

If you configure a custom host check for your web portal (see “Host checking” on page 36), you choose security applications from the list on the *VPN* > *SSL* > *Host Check* page. The *Host Check* list includes default entries for many security software products. You can add, remove, or modify entries in this list.

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

### To add an entry to the Host Check list - web-based manager

1 Go to *VPN* > *SSL* > *Host Check.*

2 Select *Create New* and enter the following information:

| | |
|---|---|
| **Name** | Enter a name of the application. The name does not need to match the actual application name. |
| **Type** | Select the type of security application. Can be AV for antivirus or FW for firewall. |
| **GUID** | Enter the Globally Unique IDentifier (GUID) for the host check application, if known. 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. |
| **Version** | The version of the security application. To get the exact versioning, in Windows right-click on the .EXE file of the application and select *Properties*. Select the *Version* tab. |
| **Create New** | If you do not know the GUID, add alternative checks for the application. The security software is considered found only if all checks succeed. |
| **Type** | Select how to check for the application:<br>• **File** — Look for a file. This could be the application’s executable file or any other file that would confirm the presence of the application. In *File/Path*, enter the full path to the file. Where applicable, you can use environment variables enclosed in percent (%) marks. For example, `%ProgramFiles%\Fortinet\FortiClient\FortiClient.exe`<br>• **Process** — Look for the application as a running process. In *Process,* enter the application’s executable file name.<br>• **Registry** — Search for a Windows Registry entry. In *Registry,* enter a registry item, for example `HKLM\SOFTWARE\Fortinet\FortiClient\Misc` |

| | |
|---|---|
| **Action** | Select one of<br>**Require** — If the item is found, the client meets the check item condition.<br>**Deny** — If the item is found, the client is considered to not meet the check item condition. Use this option if it is necessary to prevent use of a particular security product. |
| **MD5 Signatures** | If *Type* is *File* or *Process*, enter one or more known MD5 signatures for the application executable file.You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application. |

3 Select *OK*.

# Windows OS check

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.

The following example shows how you would add an OS check to the g1portal web portal. This OS check accepts all Windows XP users and Windows 2000 users running patch level 3.

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.

```
config vpn ssl web portal
  edit g1portal
    set os-check enable
    config os-check-list windows-2000
      set action check-up-to-date
      set latest-patch-level 3
      set tolerance 1
    end
    config os-check-list windows-xp
      set action allow
    end
  end
```

## Configuring cache cleaning

When the SSL VPN session ends, the client browser cache may retain some information. To enhance security, cache cleaning clears this information just before the SSL VPN session ends.

**Note:** The cache cleaner is effective only if the session terminates normally. The cache is not cleaned if the session ends due to a malfunction, such as a power failure.

### To enable cache cleaning - web-based manager

1 Go to *VPN* > *SSL* > *Portal,* select the web portal and then select *Edit*.

2 Select the *Settings* button.

3 Select the *Security Control* tab.

4 Select *Clean Cache*.

5 Select *OK* then *Apply*.

**To enable cache cleaning - CLI**

To enable cache cleaning on the full-access portal, you would enter:

```
config vpn ssl web portal
  edit full-access
    set cache-cleaner enable
  end
```

Cache cleaning requires a browser plug-in. If the user does not have the plug-in, it is automatically downloaded to the client computer.

## Configuring virtual desktop

Available for Windows XP, Windows Vista, and Windows 7 client PCs, the virtual desktop feature completely isolates the SSL VPN session from the client computer's desktop environment. All data is encrypted, including cached user credentials, browser history, cookies, temporary files, and user files created during the session. When the SSL VPN session ends normally, the files are deleted. If the session ends due to a malfunction, files might remain, but they are encrypted, so the information is protected.

When the user starts an SSL VPN session which has virtual desktop enabled, the virtual desktop replaces the user's normal desktop. When the virtual desktop exits, the user's normal desktop is restored.

Virtual desktop requires the Fortinet cache cleaner plugin. If the plugin is not present, it is automatically downloaded to the client computer.

**To enable virtual desktop - web-based manager**

1 Go to *VPN* > *SSL* > *Portal,* select the web portal and then select *Edit*.

2 Select the *Settings* button.

3 Select the *Virtual Desktop* tab.

4 Select *Enable Virtual Desktop*.

5 Enable the other options as needed.

6 Optionally, select an Application Control List.

See "Configuring virtual desktop application control".

7 Select *OK*.

8 Select *Apply*.

**To enable virtual desktop - CLI**

To enable virtual desktop on the full-access portal and apply the application control list List1, for example, you would enter:

```
config vpn ssl web portal
  edit full-access
    set virtual-desktop enable
    set virtual-desktop-app-list List1
  end
```

## Configuring virtual desktop application control

You can control which applications users can run on their virtual desktop. To do this, you create an Application Control List of either allowed or blocked applications. When you configure the web portal, you select the list to use.

There are two types of application control list:

- allow the listed applications and block all others

or

- block the listed applications and allow all others.

You can create multiple application control lists, but each in web portal you can select only one list to use.

**To create an Application Control List - web-based manager**

1. Go to *VPN* > *SSL* > *Virtual Desktop Application Control* and select *Create New*.
2. Enter a *Name* for the list.
3. Select one of the following:
   - *Allow the applications on this list and block all others*
   - *Block the applications on this list and allow all others*
4. Select *Add*.
5. Enter a *Name* for the application.

   This can be any name and does not have to match the official name of the application.
6. Enter one or more known *MD5 Signatures* for the application executable file.

   You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application.
7. Select *OK*.
8. Repeat steps 4 through 7 for each additional application.
9. Select *OK*.

**To create an Application Control List - CLI**

If you want to add BannedApp to List1, a list of blocked applications, you would enter:

```
config vpn ssl web virtual-desktop-app-list
  edit "List1"
    set action block
    config apps
      edit "BannedApp"
        set md5s "06321103A343B04DF9283B80D1E00F6B"
      end
  end
```

## Configuring client OS Check

The SSLVPN client OS Check feature can determine if clients are running the Windows 2000, Windows XP, Windows Vista or Windows 7 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.

**To configure OS Check - CLI**

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}
      set action {allow | check-up-to-date | deny}
      set latest-patch-level {disable | 0 - 255}
      set tolerance {tolerance_num}
    end
  end
```

# Configuring user accounts and user groups for SSL VPN

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.

You need to create a user account for each user and then add the users to an SSL VPN user group. The user group specifies the web portal that users can access after they authenticate.

**Note:** FortiOS supports LDAP password renewal notification and updates through SSL VPN.

Configuration is enabled using the CLI commands:

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

For more information, see the *User Authentication Guide*.

## Creating user accounts

The following procedure explains how to create a user account. To authenticate users, you can use a plain text password on the FortiGate unit (Local domain), forward authentication requests to an external RADIUS, LDAP or TACACS+ server, or utilize PKI certificates.

For information about how to create RADIUS, LDAP, TACACS+ or PKI user accounts and certificates, see the *User Authentication Guide*.

**To create a user account - web-based manager**

1. Go to *User* > *User*, select *Create New*
2. Enter the *User Name*.
3. Enter a password for the user to store the password on the FortiGate unit.

   The password should be at least six characters long.
4. Alternatively, select the authentication type and configure as required by the option.
5. Select *OK*.

**To create a user account - CLI**

If you want to create a user account, for example User_1 with the password “1_user”, you would enter:

```
config user local
  edit User_1
    set passwd "1_User"
    set status enable
    set type password
  end
```

### Creating a user group for SSL VPN users

You must add users to a firewall user group. As part of configuring the user group, you select the SSL VPN web portal that the members of this group access after authenticating.

**To create an SSL VPN user group - web-based manager**

1. Go to *User* > *User Group* > *User Group*, select *Create New*.
2. Enter a name for the user group.
3. Select *Firewall*.
4. Select the check box for *Allow SSL-VPN Access* and select the web portal for the user group to use.
5. Add users to the group by selecting the user name and selecting the right arrow.
6. Select *OK*.

**To create an SSL VPN user group - CLI**

To create the user group web_only associated with the web-access portal and add members User_1, User_2, and User_3, you would enter:

```
config user group
  edit web_only
    set group-type sslvpn
    set member User_1 User_2 User_3
    set sslvpn-portal web-access
  end
```

## Configuring security policies

Security policies permit traffic to pass through the FortiGate unit. The FortiGate unit checks incoming connection attempts against the list of security policies, looking to match:

- source and destination interfaces
- source and destination firewall addresses
- services
- time/schedule

If no policy matches, the connection is dropped. You should order the security policy list top to bottom from most specific to most general. Only the first matching security policy is applied to a connection, and you want the best match to occur first.

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 user accounts and user groups for SSL VPN" on page 41.

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.

## Configuring 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. See "Specifying an IP address range for tunnel-mode clients" on page 21.

The source address for your SSL VPN security policies will be the predefined "all" address. If this address is missing, you can add it. 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

1. Go to *Firewall Objects* > *Address* > *Address* and select *Create New*.
2. Enter the *Address Name*.
3. Select a *Type* of *Subnet/IP Range*.
4. Enter the IP address and subnet mask.
5. Select the interface associated with the address.
6. Select *OK*.

### To create a firewall address - CLI

To create, for example, the address OfficeLAN for the protected network you would enter:

```
config firewall address
  edit OfficeLAN
    set type ipmask
    set subnet 10.11.101.0/24
    set associated-interface port2
  end
```

## Configuring the 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.

If you provide tunnel mode access, you will need a second security policy to permit traffic between the SSL VPN tunnel and the protected networks. See “Configuring the tunnel mode security policy” on page 46.

The SSL VPN security policy is an identity-based policy that permits members of a specified SSL VPN user group to access specified services according to a specified schedule. The policy can also apply UTM features, traffic shaping and logging of SSL VPN traffic.

The user group is associated with the web portal that the user sees after logging in. If you have multiple portals, you will need multiple user groups. 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 source address that corresponds to the IP address of the remote user.
- the destination address that corresponds to the IP address or addresses that remote clients need to access.

  The destination address may correspond to an entire private network, a range of private IP addresses, or the private IP address of a server or host.

**Note:** 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.

- the level of SSL encryption to use and the authentication method.
- which SSL VPN user groups 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.

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

1 Go to *Policy* > *Policy* > *Policy* and select *Create New.*

2 Enter the following information:

| | |
|---|---|
| **Source Interface/Zone** | Select the name of the FortiGate network interface to that connects to the Internet. |
| **Source Address** | Select *all*. |
| **Destination Interface/Zone** | Select the FortiGate network interface that connects to the protected network. |
| **Destination Address** | Select the firewall address you created that represents the networks and servers to which the SSL VPN clients will connect.<br>If you want to associate multiple firewall addresses or address groups with the *Destination Interface/Zone*, from *Destination Address*, select *Multiple*. In the dialog box, move the firewall addresses or address groups from the *Available Addresses* section to the *Members* section, then select *OK*. |
| **Action** | Select *SSL-VPN*. This option is available only if there is at least one user group with SSL VPN access enabled. |
| **SSL Client Certificate Restrictive** | 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 "Enabling strong authentication through X.509 security certificates" on page 24. |
| **Cipher Strength** | Select the bit level of SSL encryption. The web browser on the remote client must be capable of matching the level that you select: *Any*, *High >= 164*, or *Medium >= 128*. |
| **Configure SSL-VPN Users** | A security policy for an SSL VPN is automatically an identity-based policy. |
| **Add** | Add a user group to the policy. The Edit Authentication Rule window opens on top of the security policy. Enter the following information and then select OK. You can select Add again to add more groups. |
| **User Group** | Select user groups in the left list and use the right arrow button to move them to the right list. |
| **Service** | Select service in the left list and use the right arrow button to move them to the right list. Select the ANY service to allow the user group access to all services. |

3 Select *OK*.

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.

### To create an SSL VPN security policy - CLI

To create the security policy by entering the following CLI commands.

```
config firewall policy
  edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr all
    set dstaddr OfficeLAN
    set action ssl-vpn
    set nat enable
    config identity-based-policy
      edit 0
```

```
        set groups SSL-VPN
        set schedule always
        set service ANY
      end
  end
```

## Configuring the 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.

Similar to an IPsec virtual interface, 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* > *Policy*> *Policy* and select *Create New*.

2 Enter the following information and select *OK*.

| | |
|---|---|
| **Source Interface/Zone** | Select the virtual SSL VPN interface, such as *ssl.root*. |
| **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. |
| **Destination Interface/Zone** | Select the FortiGate network interface that connects to the protected network. |
| **Destination Address** | Select the firewall address you created that represents the networks and servers to which the SSL VPN clients will connect.<br>To select multiple firewall addresses or address groups, select *Multiple*. In the dialog box, move the firewall addresses or address groups from the *Available Addresses* section to the *Members* section, then select *OK*. |
| **Action** | Select *Accept*. |
| **NAT** | Select *Enable NAT* |
| **Comments** | Optionally, add information about the policy. The maximum length is 63 characters. |

### To configure the tunnel mode security policy - CLI

```
config firewall policy
  edit <id>
    set srcintf ssl.root
    set dstintf <dst_interface_name>
    set srcaddr <tunnel_ip_address>
    set dstaddr <protected_network_address_name>
    set schedule always
    set service ANY
    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.

### Configuring routing for tunnel mode

If you 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 *Router* > *Static* > *Static Route* 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
    set gateway <gateway_IP>
  end
```

## Adding an 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. Optionally, you can enable clients to connect to the Internet through the FortiGate unit.

**To add an Internet browsing policy**

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

| | |
|---|---|
| **Source Interface/Zone** | Select the virtual SSL VPN interface, *ssl.root*, for example. |
| **Source Address** | Select the firewall address you created that represents the IP address range assigned to SSL VPN clients. |
| **Destination Interface/Zone** | Select the FortiGate network interface that connects to the Internet. |
| **Destination Address** | Select *all*. |
| **Action** | Select *Accept*. |
| **NAT** | Enable. |

Leave other settings at their default values.

**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 ANY
    set nat enable
  end
```

## Enabling 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. For information about route-based and policy-based IPsec VPNs, see the *IPsec VPN Guide*.

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

1 Go to *Policy* > *Policy* > *Policy* and select *Create New*.

2 Enter the following information and select *OK*.

| | |
|---|---|
| **Source Interface/Zone** | Select the virtual SSL VPN interface, *ssl.root*, for example. |
| **Source Address** | Select the firewall address you created that represents the IP address range assigned to SSL VPN clients. |
| **Destination Interface/Zone** | Select the virtual IPsec interface for your IPsec VPN. |
| **Destination Address** | Select the address of the IPsec VPN remote protected subnet. |
| **Action** | Select *ACCEPT*. |
| **NAT** | Enable. |

Leave other settings at their default values.

### 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 ANY
  end
```

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

1 Go to *Firewall* > *Policy* > *Policy* and select *Create New*.

2 Enter the following information and select *OK*.

| | |
|---|---|
| **Source Interface/Zone** | Select the virtual SSL VPN interface, *ssl.root*, for example. |
| **Source Address** | Select the firewall address you created that represents the IP address range assigned to SSL VPN clients. |
| **Destination Interface/Zone** | Select the FortiGate network interface that connects to the Internet. |
| **Destination Address** | Select the address of the IPsec VPN remote protected subnet. |

| | |
|---|---|
| **Action** | Select *IPSEC*. |
| **VPN tunnel** | Select the Phase 1 configuration name of your IPsec VPN. |
| **Allow inbound** | Enable |
| **Allow outbound** | Enable |
| **NAT inbound** | Enable |

Leave other settings at their default values.

### 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 ANY
    set inbound enable
    set outbound enable
    set natinbound enable
    set vpntunnel toOfficeA
  end
```

In this example, port1 is connected to the Internet.

# SSL VPN logs

Logging is available for SSP VPN traffic.

### To enable logging - web-based manager

1 Go to *Log&Report* > *Log Config* > *Log Setting*.

2 Enable the storage of log messages to one or more locations:

**Note:** If available on your FortiGate unit, you can enable the storage of log messages to a system hard disk. In addition, as an alternative to the options listed above, you may choose to forward log messages to a remote computer running a WebTrends firewall reporting server. For more information about enabling either of these options through CLI commands, see the “log” chapter of the *FortiGate CLI Reference*.

3 If the options are concealed, select the expand arrow beside each option to reveal and configure associated settings.

4 If logs will be written to system memory, from the Log Level list, select *Information*. For more information, see the *Logging and Reporting Guide*.

5 Select *Apply*.

### To enable logging - CLI

```
config log {fortianalyzer | memory | syslog} setting
  set status enable
end
```

For some log locations, there are additional options available.

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

1 Go to *Log&Report* > *Log Config* > *Event Log*.
2 Select *Enable*, and then select one or more of the following options:
- SSL VPN user authentication event
- SSL VPN administration event
- SSL VPN session event

3 Select *Apply*.

**To enable logging of SSL VPN events - CLI**

```
config log {fortianalyzer | memory | syslog} filter
  set event enable
  set sslvpn-log-adm enable
  set sslvpn-log-auth enable
  set sslvpn-log-session enable
end
```

**To enable logging of SSL VPN traffic - web-based manager**

1 Go to *Firewall* > *Policy* > *Policy*.
2 Select your SSL VPN policy and then select *Edit*.
3 For each identity-based policy, select its *Edit* icon, select *Log Allowed Traffic*, then select *OK*.
4 Select *OK*.
5 Select the *Edit* icon for your tunnel-mode policy.
6 Select *Log Allowed Traffic* and then select *OK*.

**To enable logging of SSL VPN traffic - CLI**

Your SSL VPN security policy is number 2 with a single identity-based policy, and your tunnel-mode policy is number 5, you would enable traffic logging by entering:

```
config firewall policy
  edit 2
    config identity-based-policy
      edit 1
        set logtraffic enable
      end
  edit 5
    set logtraffic enable
  end
```

**To view SSL VPN logs - web-based manager**

1 Go to *Log&Report* > *Log Access* and select the *Memory* or *Disk* tab.
2 From the *Log Type* list select *Event Log* or *Traffic Log*, as needed.

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

In the traffic logs, look for the sub-type “allowed”. For web-mode traffic, the source is the host IP address. For tunnel-mode traffic, the source is the address assigned to the host from the SSL VPN address pool.

**To view SSL VPN logs - CLI**

```
execute log filter category {event | traffic}
execute log filter device {fortianalyzer | memory | syslog}
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the command

```
execute log filter start-line 1
```

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

# Monitoring active SSL VPN sessions

You can go to *User* > *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 *VPN* > *SSL* > *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 check box and then selecting the *Delete* icon.

**To monitor SSL VPNs - CLI**

To list all of the SSL VPN sessions and their index numbers:

```
get vpn ssl monitor
```

To delete tunnel-mode or web-mode sessions:

```
execute vpn sslvpn del-tunnel <index_int>
execute vpn sslvpn del-web <index_int>
```

# Troubleshooting

Here is a list of common SSL VPN problems and the likely solutions.

| | |
|---|---|
| No response from SSL VPN URL | Check that SSL VPN is enabled.<br>Check SSL VPN port assignment (default 10443).<br>Check SSL VPN security policy. |
| Error: “The web page cannot be found.” | Check URL:<br>https://<FortiGate_IP>:<SSLVPN_port>/remote/login |
| Tunnel connects, but there is no communication. | Check that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface. See “Configuring routing for tunnel mode” on page 47. |
| Tunnel-mode connection shuts down after a few seconds | This issue occurs when there are multiple interfaces connected to the Internet, for example, a dual WAN configuration. Upgrade the FortiGate unit firmware to at least v3.0 MR4 or higher, then use the following CLI command:<br>`config vpn ssl settings`<br>`  set route-source-interface enable`<br>`end` |
| Error: “Destination address of Split Tunneling policy is invalid.” | The SSL VPN security policy uses the ALL address as its destination. Specify the address of the protected network instead. |
| When trying to connect using FortiClient SSL VPN (standalone) the following error message “Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12)” is returned.<br>When trying to login to the web portal, login and password are entered and login page will be sent back. | Cookies must be enabled for SSL VPN to function in Web portal or with the FortiClient SSL client.<br>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:<br>• Block cookies that do not have a compact privacy policy.<br>• Block cookies that use personally identifiable information without your explicit consent. |

# Using the web portal

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

The following topics are included in this section:



## 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 in to the FortiGate secure HTTP gateway**

1. Using the web browser on your computer, browse to the URL of the FortiGate unit (for example, `https://`<FortiGate_IP_address>`:10443/remote/login`).

   The FortiGate unit may offer you a self-signed security certificate. If you are prompted to proceed, select Yes.

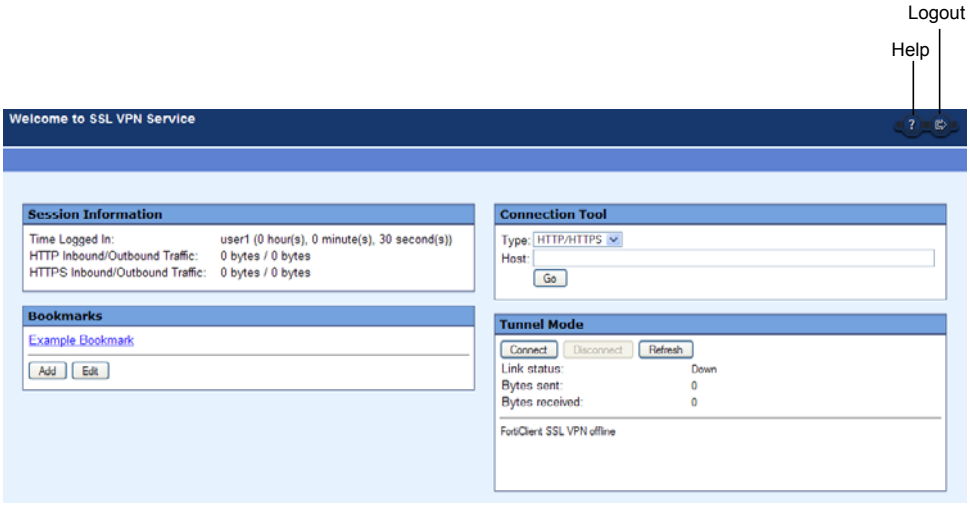
   A second message may be displayed to inform you that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. You can ignore the message.
2. When you are prompted for your 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 you log in, you see a web portal page like the following:

**Figure 5: FortiGate SSL VPN web portal page**




Four “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.
- *Bookmarks* provides links to network resources. You can use the administrator-defined bookmarks and you can add your own bookmarks. See “Using the Bookmarks widget” on page 55.
- *Connection Tool* enables you to connect to network resources without using or creating a bookmark.
- *Tunnel Mode* connects and disconnects the tunnel mode SSL connection to the FortiGate unit. While the tunnel is active, the widget displays the amount of data that is sent and received. For more information, see “Tunnel-mode features” on page 63.

  Tunnel mode requires a downloadable client application. If your computer is running Microsoft Windows, the Tunnel Mode widget provides a download link if you need to install the client on your computer. If you are using Macintosh or Linux, you can obtain and install an appropriate client application from the Fortinet Support site. For more information, see “Downloading the SSL VPN tunnel mode client” on page 66.

Depending on the web portal configuration and user group settings, some widgets might not be present. For example, the predefined web-access portal contains only the Session Information and Bookmarks widgets.

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.

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

### 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 Bookmarks or the Connection Tool:

- Ping enables you to test whether a particular server or host is reachable on the network.
- HTTP/HTTPS accesses web pages.
- Telnet (Teletype Network emulation) enables you to use your computer as a virtual text-only terminal to log in to a remote host.
- SSH (Secure Shell) enables you to exchange data between two computers using a secure channel.
- FTP (File Transfer Protocol) enables you to transfer files between your computer and a remote host.
- SMB/CIFS implements the Server Message Block (SMB) protocol to support file sharing between your computer and a remote server host.
- VNC (Virtual Network Computing) enables you to remotely control another computer, for example, accessing your work computer from your home computer.
- RDP (Remote Desktop Protocol), similar to VNC, enables you to remotely control a computer running Microsoft Terminal Services.

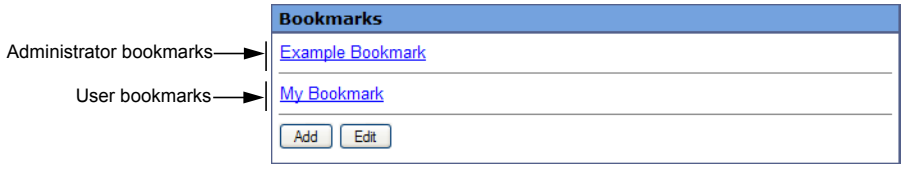
Some server applications may prompt you for a user name and password. You must have a user account created by the server administrator so that you can log in.

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

## 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.

**Figure 6: Bookmarks widget**




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”.

**Note:** 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 Connection Tool” on page 57.

## 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 *Bookmarks* widget, select *Add*.

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.<br>For RDP connections, you can append some parameters to control screen size and keyboard layout. See "To start an RDP session" on page 60. |
| **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.<br>**Disabled** — This is not an SSO bookmark.<br>**Automatic** — Use your SSL VPN credentials or an alternate set. See the *SSO Credentials* field.<br>**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.<br>**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.<br>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*.

# Using the Connection Tool

You can connect to any type of server without adding a bookmark to the My Bookmarks list. The fields in the 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 57
- "To ping a host or server behind the FortiGate unit" on page 57
- "To start a telnet session" on page 57
- "To start an FTP session" on page 58
- "To start an SMB/CIFS session" on page 59
- "To start an SSH session" on page 60
- "To start an RDP session" on page 60
- "To start a VNC session" on page 62


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

**Note:** When you use the 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 *Host* field, type the URL of the web server.

For example: `http://www.mywebexample.com` or `https://172.20.120.101`

3 Select *Go*.

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 *Go*.

A message stating whether the IP address can be reached or not is displayed.

### To start a telnet session

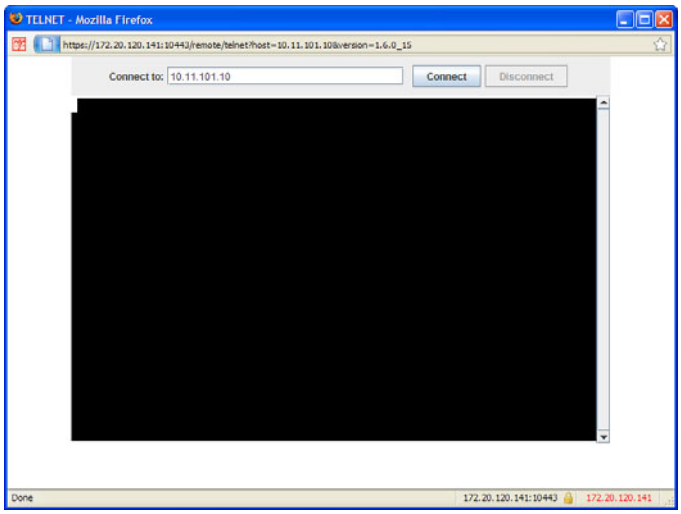
1 In *Type*, select *Telnet*.

2 In the *Host* field, type the IP address of the telnet host.

For example: `10.11.101.12`

3 Select *Go*.

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 *Host* field, type the IP address of the FTP server.

For example: `10.11.101.12`

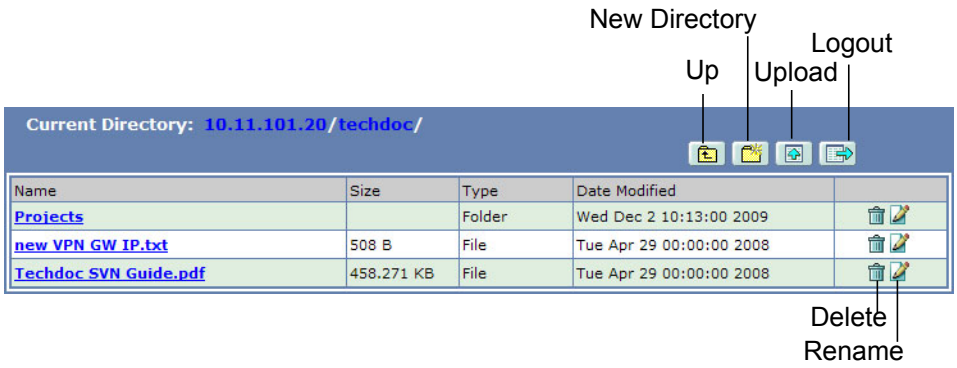
3 Select *Go*.

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.

**Figure 7: An FTP session**



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 *Host* field, type the IP address of the SMB or CIFS server.

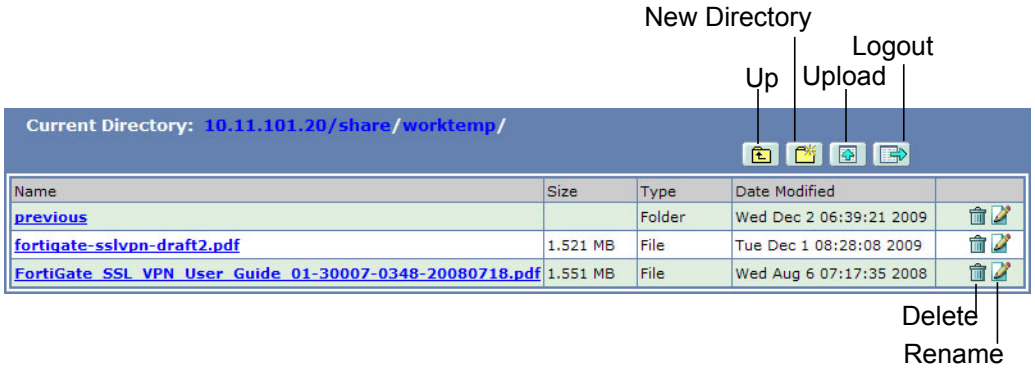
For example: `10.11.101.12`

3 Select *Go*.

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 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.

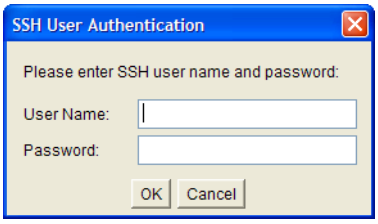
For example: `10.11.101.12`

3 Select *Go*.

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`

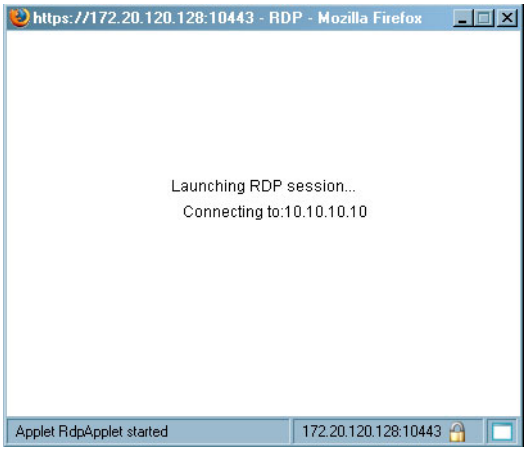
3 Optionally, you can specify additional options for RDP by adding them to the *Host* field following the host address. See "RDP options" on page 61 for information about the available options.

For example, to use a French language keyboard layout you would add the `-m` parameter:

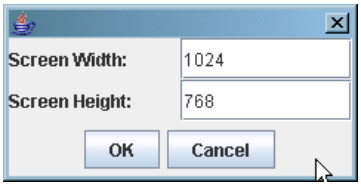
```
10.11.101.12 -m fr
```

4 Select *Go*.

A login window opens.

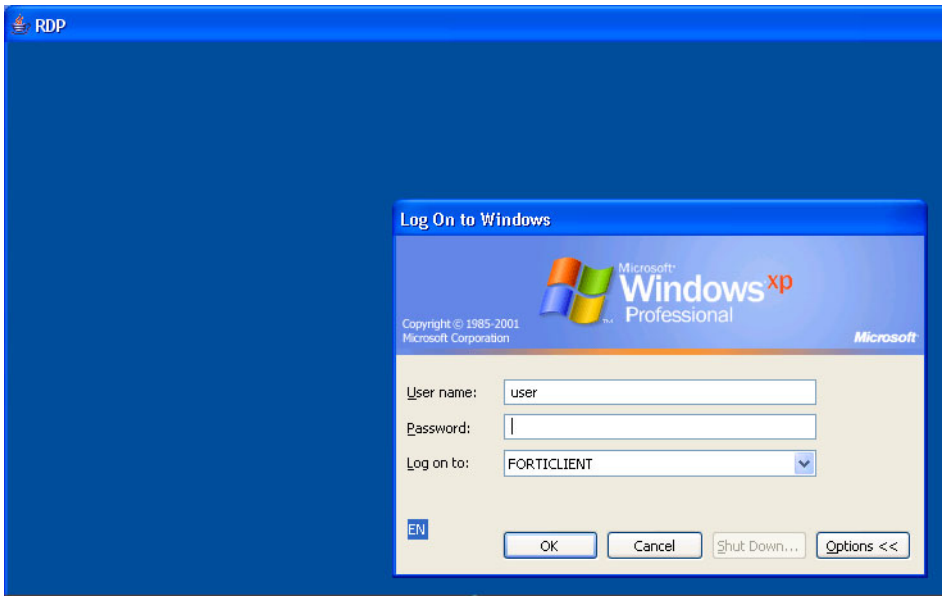


5 When you see a screen configuration dialog, click *OK*.




The screen configuration dialog does not appear if you specified the screen resolution with the host address.

6 When you are prompted 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.




7 Select *Login*.

If you need to send Ctrl-Alt-Delete in your session, use Ctrl-Alt-End.

8 To end the RDP session, Log out of Windows or select *Cancel* from the Logon window.

## RDP options

When you specify the RDP server address, you can also specify other options for your remote desktop session.

| | |
|---|---|
| **Screen resolution**<br>Use this command to make the RDP window full screen or a specific the window size. | `-f` Make RDP full-screen. |
| | `-g <width>x<height>`<br>`<width>` and `<height>` are in pixels<br>Example: `-g 800x600` |
| **Authentication**<br>Use these options to send your authentication credentials with the connection request, instead of entering them after the connection is established. | `-u <user name>`<br>`-p <password>`<br>`-d <domain>` |

| | |
|---|---|
| **Locale/Keyboard**<br>Use this option if the remote computer might not use the same keyboard layout as your computer. Select the locale code that matches your computer. | `-m <locale>`<br>The supported values of `<locale>` are:<br>ar Arabic<br>da Danish<br>de German<br>de-ch Swiss German<br>en-gb British English<br>en-uk UK English<br>en-us US English<br>es Spanish<br>fi Finnish<br>fr French<br>fr-be Belgian French<br>fr-ca Canadian French<br>fr-ch Swiss French<br>hr Croatian<br>hu Hungarian<br>it Italian<br>ja Japanese<br>lt Lithuanian<br>lv Latvian<br>mk Macedonian<br>no Norwegian<br>pl Polish<br>pt Portuguese<br>pt-br Brazilian Portuguese<br>ru Russian<br>sl Slovenian<br>sv Sudanese<br>tk Turkmen<br>tr Turkish |

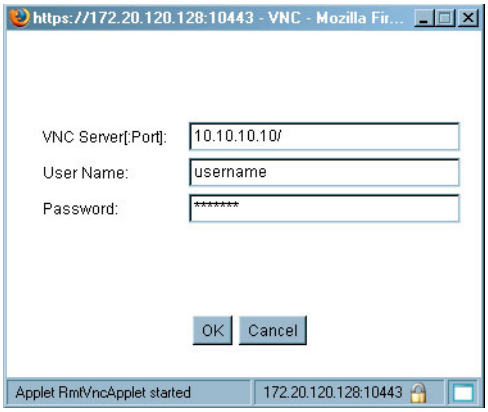
### To start a VNC session

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 *Go*.

   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.



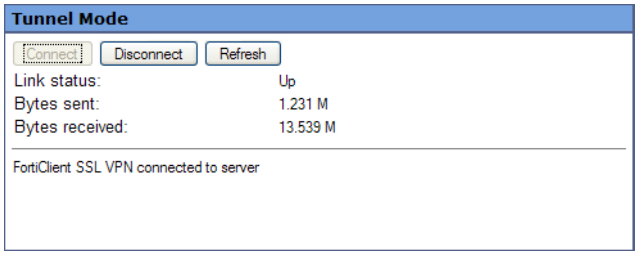

5. Select *OK*.

   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.

# Tunnel-mode features

For Windows users, the web portal Tunnel Mode widget provides controls for your tunnel mode connection and also provides status and statistics about its operation. You can also control and monitor tunnel mode operation from the standalone client application. For more information, see “Using the tunnel mode client” on page 67.

**Figure 8: Fortinet SSL VPN tunnel mode widget**




| | |
|---|---|
| **Connect** | Initiate a session and establish an SSL VPN tunnel with the FortiGate unit. |
| **Disconnect** | End the session and close the tunnel to the FortiGate unit. |
| **Refresh** | Refresh the status and statistics immediately. |
| **Link Status** | The state of the SSL VPN tunnel:<br>• *Up* — an SSL VPN tunnel with the FortiGate unit has been established.<br>• *Down* — a tunnel connection has not been initiated. |
| **Bytes Sent** | The number of bytes of data transmitted from the client to the FortiGate unit since the tunnel was established. |
| **Bytes Received** | The number of bytes of data received by the client from the FortiGate unit since the tunnel was established. |

# Using the SSL VPN Virtual Desktop

The virtual desktop feature is available for Windows only. When you start an SSL VPN session, the virtual desktop replaces your normal desktop. When the virtual desktop exits, your regular desktop is restored. Virtual desktop information is encrypted so that no information from it remains available after your session ends.

To use the SSL VPN virtual desktop, simply log in to an SSL VPN that requires the use of the virtual desktop. Wait for the virtual desktop to initialize and replace your desktop with the SSL VPN desktop, which has a Fortinet SSL VPN logo as wallpaper. Your web browser will open to the web portal page.

You can use the virtual desktop just as you use your regular desktop, subject to the limitations that virtual desktop application control imposes. See “Configuring virtual desktop application control” on page 40.

If it is enabled in the web portal virtual desktop settings, you can switch between the virtual desktop and your regular desktop. Right-click the *SSL VPN Virtual Desktop* icon in the taskbar and select *Switch Desktop*.

To see the web portal virtual desktop settings, right-click the *SSL VPN Virtual Desktop* icon in the taskbar and select *Virtual Desktop Option*.

When you have finished working with the virtual desktop, right-click the *SSL VPN Virtual Desktop* icon in the taskbar and select *Exit*. Select *Yes* to confirm. The virtual desktop closes and your regular desktop is restored.

# 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 SSL, 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 SSL VPN example” on page 71.

## FortiClient for Windows configuration

**To set up FortiClient for Microsoft Windows**

1. Go to *Start* > *All Programs* > *FortiClient* > *FortiClient*.
2. Go to *VPN* > *Connection*.
3. Select *Advanced* and select *Add*.
4. In the *Connection Name*, enter the name of the SSL VPN tunnel.
5. Select *SSL VPN* for the *VPN Type*.
6. Enter the IP address of the *Remote Gateway*.
7. Enter the *Username* and *Password* if required.
8. Select *OK*.

See the *VPN Connections* window displays to verify the SSL VPN tunnel is up.

# Using the SSL VPN tunnel client

This section provides information about installing and using the SSL VPN tunnel client for Windows, Linux, and Mac OS X.

The following topics are included in this section:



## Client configurations

There are several configurations of SSL VPN applications available.

- web mode
- tunnel mode
- virtual desktop

### Web mode

SSL VPN web mode requires nothing more than a web browser. Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari browsers are supported. For detailed information about supported browsers see the Release Notes for your FortiOS firmware.

### Tunnel mode

SSL VPN tunnel mode establishes a connection to the remote protected network that any application can use. This requires a tunnel client application specific to your computer operating system. The tunnel client application installs a network driver that sends and receives data through the SSL VPN tunnel.

If your computer runs Microsoft Windows, you can download the tunnel mode client from the web portal Tunnel Mode widget. After you install the client, you can start and stop tunnel operation from the Tunnel Mode widget, or you can open the tunnel mode client as a standalone application. You can find the tunnel mode client on the Start menu at *All Programs* > *FortiClient* > *FortiClient SSL VPN*.

If your computer runs Linux or Mac OS X, you can obtain an appropriate 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. On Linux and Mac OS X platforms, tunnel mode operation cannot be initiated from the web portal Tunnel Mode widget. You must use the standalone tunnel client application.

When a system configuration must involve more secure disposal of cached data, the SSL VPN Virtual Desktop should be used. (Available on Windows only).

### Virtual desktop application

The virtual desktop application creates a virtual desktop on a user's PC and monitors the data read/write activity of the web browser running inside the virtual desktop. When the application starts, it presents a 'virtual desktop' to the user. The user starts the web browser from within the virtual desktop and connects to the SSL VPN web portal. The browser file/directory operation is redirected to a new location, and the data is encrypted before it is written to the local disk. When the virtual desktop application exits normally, all the data written to the disk is removed. If the session terminates abnormally (power loss, system failure), the data left behind is encrypted and unusable to the user. The next time you start the virtual desktop, the encrypted data is removed.

## Downloading the SSL VPN tunnel mode client

SSL VPN standalone tunnel client applications are available for Windows, Linux, and Mac OS X systems (see the Release Notes for your FortiOS firmware for the specific versions that are supported). There are separate download files for each operating system.

**Note:** Windows users can also download the tunnel mode client from an SSL VPN web portal that contains the Tunnel Mode widget.

The most recent version of the SSL VPN standalone client applications can be found at: http://support.fortinet.com/

**To download the SSL VPN tunnel client**

1. Log in to Fortinet Support at http://support.fortinet.com/.
2. In the Download area, select Firmware Images.
3. Select FortiGate.
4. Select *v4.00* and then select the latest firmware release.
5. Select *SSL VPN Clients*.
6. Select the appropriate client.

   Windows: `SslvpnClient.exe` or `SslvpnClient.msi`

   Linux: `forticlientsslvpn_linux_`<version>`.tar.gz`

   Mac OS X: `forticlientsslvpn_macosx_`<version>`.dmg`

**Note:** The location of the SSL VPN tunnel client on the Support web site is subject to change. If you have difficulty finding the appropriate file, contact Customer Support.

# Installing the tunnel mode client

Follow the instructions for your operating system.

## Windows

Double-click the `SslvpnClient.exe` or `SslvpnClient.msi` file and follow the on-screen instructions.

## Linux

1. Extract the `forticlientsslvpn_linux_`<version>`.tar.gz` package file to a folder and run the client program `forticlientsslvpn`.

   When you run the install program for the first time, you will have to set up system parameters (root privileges) before you run the program or before other users without administrator privileges can use the application.
2. In the *First Run* dialog, select *OK*.

After this initial setup is complete, a user with a normal (non-administrator) account can establish an SSL VPN tunnel session.

## MAC OS client

1. Double-click on the `forticlientsslvpn_macosx_`<version>`.dmg` file.
2. Double-click the forticlientsslvpn.pkg file inside the disk image and follow the instructions.

   The application installs the program `forticlientsslvpn.app` in the Applications folder

# Using the tunnel mode client

Follow the instructions for your operating system.

## Windows client

**To use the SSL VPN standalone tunnel client (Windows)**

1. Go to *Start* > *All Programs* > *FortiClient* > *FortiClient SSL VPN*.
2. Enter the following information. Use the *Connect* and *Disconnect* buttons to control the tunnel connection.

| | |
|---|---|
| **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.<br>To pre-configure connection settings, see "To configure tunnel client settings (Windows)" on page 68. |
| **Server Address** | Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN. |
| **Username** | Enter your user name. |
| **Password** | Enter the password associated with your user account. |
| **Client Certificate** | Use this field if the SSL VPN requires a certificate for authentication.<br>Select the required certificate from the drop-down list. The certificate must be installed in the Internet Explorer certificate store. |

| | |
|---|---|
| **Connection** | Status: Connected or Disconnected<br>Duration: Hours, minutes, seconds since session started<br>Bytes Sent / Bytes Received: amount of data transferred |
| **Settings...** | Select to open the *Settings* dialog. See "To configure tunnel client settings (Windows)" on page 68. |
| **Connect** | Start tunnel mode operation. |
| **Disconnect** | Stop tunnel mode operation. |
| **Exit** | Close the tunnel mode client application. |

### To configure tunnel client settings (Windows)

1. Go to *Start* > *All Programs* > *FortiClient* > *FortiClient SSL VPN*.
2. Select *Settings...*.
3. Select *New Connection*, or select an existing connection and then select *Edit*.
4. Enter the *Connection Name*.
5. Enter the connection information. You can also enter a *Description*. Select *OK*.

   See "To use the SSL VPN standalone tunnel client (Windows)" on page 67 for information about the fields.
6. Select *Keep connection alive until manually stopped* to prevent tunnel connections from closing due to inactivity.
7. Select *OK*.

## Linux client

### To use the SSL VPN standalone tunnel client (Linux)

1. Go to the folder where you installed the Linux tunnel client application and double-click on '`forticlientsslvpn`'.
2. Enter the following information. Use the *Connect* and *Stop* buttons to control the tunnel connection.

| | |
|---|---|
| **Connection** | 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.<br>To pre-configure connection settings, see "To configure tunnel client settings (Windows)" on page 68. |
| **Server** | Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN. In the smaller field, enter the SSL VPN port number (default 10443). |
| **User** | Enter your user name. |
| **Password** | Enter the password associated with your user account. |
| **Certificate** | Use this field if the SSL VPN requires a certificate for authentication.<br>Select the certificate file (PKCS#12) from the drop-down list, or select the Browse (...) button and find it. |
| **Password** | Enter the password required for the certificate file. |
| **Settings...** | Select to open the *Settings* dialog. See "To configure tunnel client settings (Linux)" on page 68. |

### To configure tunnel client settings (Linux)

1. Go to the folder where you installed the Linux tunnel client application and double-click `forticlientsslvpn`.
2. Select *Settings...*.

3 Select *Keep connection alive until manually stopped* to prevent tunnel connections from closing due to inactivity.

4 Select *Start connection automatically.*

The next time the tunnel mode application starts, it will start the last selected connection.

5 If you use a proxy, enter in *Proxy* the proxy server IP address and port. Enter proxy authentication credentials immediately below in *User* and *Password*.

6 Select the + button to define a new connection, or select from the list an existing connection to modify.

For a new connection, the *Connection* window opens. For an existing connection, the current settings appear in the *Settings* window and you can modify them.

7 Enter the connection information. If you are creating a new connection, select *Create* when you are finished.

See "To use the SSL VPN standalone tunnel client (Linux)" on page 68 for information about the fields.

8 Select *Done*.

## MAC OS X client

### To use the SSL VPN standalone tunnel client (Mac OS X)

1 Go to the Applications folder and double-click on `forticlientsslvpn.app`.

2 Enter the following information. Use the *Connect* and *Stop* buttons to control the tunnel connection.

| | |
|---|---|
| **Connection** | 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.<br>To pre-configure connection settings, see "To configure tunnel client settings (Mac OS X)" on page 69. |
| **Server** | Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN. In the smaller field, enter the SSL VPN port number (default 10443). |
| **User** | Enter your user name. |
| **Password** | Enter the password associated with your user account. |
| **Certificate** | Use this field if the SSL VPN requires a certificate for authentication.<br>Select the certificate file (PKCS#12) from the drop-down list, or select the Browse (...) button and find it. |
| **Password** | Enter the password required for the certificate file. |
| **Settings...** | Select to open the *Settings* dialog. See "To configure tunnel client settings (Mac OS X)" on page 69. |

### To configure tunnel client settings (Mac OS X)

1 Go to the Applications folder and double-click on `forticlientsslvpn.app`.

2 Select *Settings...*.

3 Select *Keep connection alive until manually stopped* to prevent tunnel connections from closing due to inactivity.

4 Select *Start connection automatically.*

The next time the tunnel mode application starts, it will start the last selected connection.

5 If you use a proxy, enter in *Proxy* the proxy server IP address and port. Enter proxy authentication credentials immediately below in *User* and *Password*.

6 Select the + button to define a new connection, or select from the list an existing connection to modify.

7 Enter the connection information. If you are creating a new connection, select *Create* when you are finished.

See "To use the SSL VPN standalone tunnel client (Mac OS X)" on page 69 for information about the fields.

8 Select *Done*.

# Uninstalling the tunnel mode client

If you want to remove the tunnel mode client application, follow the instructions for your operating system.

### To uninstall from Windows

1 In the *Control Panel*, select *Programs and Features (Add or Remove Programs* in Windows XP).

2 Select *FortiClient SSL VPN* and then *Remove*.

### To uninstall from Linux

Remove/delete the folder containing all the SSL VPN client application files.

### To uninstall from Mac OS X

In the Applications folder, select `forticlientsslvpn.app` and drag it into the Trash.

# Examples

In the most common Internet scenario, the remote client connects to an ISP that offers connections with dynamically assigned IP addresses. The ISP forwards packets from the remote client to the Internet, where they are routed to the public interface of the FortiGate unit.

At the FortiGate unit, you configure user groups and security policies to define the server applications and IP address range or network that remote clients will be able to access behind the FortiGate unit.

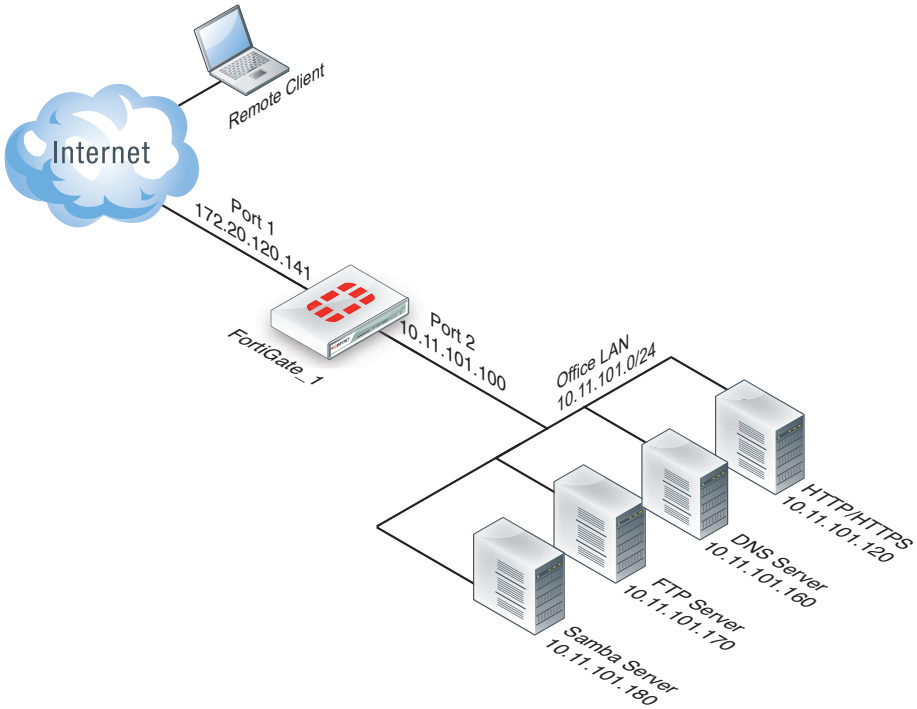
This section contains the following topics:



## Basic SSL VPN example

A common application for an SSL VPN is to provide access to the office network for employees traveling or working from home. For example, Figure 9 shows a FortiGate gateway (FortiGate_1) that connects the office network to the Internet. Users on the office network have access to the Internet, but access to the office network from the Internet is available only to authenticated users of the SSL VPN.

**Figure 9: Example SSL VPN configuration**



### Infrastructure requirements

- The FortiGate unit must be operating in NAT mode and have a static public IP address.
- The ISP assigns IP addresses to remote clients before they connect to the FortiGate unit.

For information about client operating system and browser requirements, see the Release Notes for your FortiGate firmware.

## General configuration steps

1. Create firewall addresses for
   - the destination networks
   - the IP address range that the FortiGate unit will assign to tunnel-mode clients
2. Create the web portal.
3. Create user accounts.
4. Create the SSL VPN user group and add the users. In the user group configuration, you specify the web portal to which the users are directed.
5. Create the security policies:
   - The SSL VPN security policy enables web mode access to the protected network.
   - The tunnel-mode policy enables tunnel mode access to the protected network.
6. Create a static route to direct packets destined for tunnel users to the SSL VPN 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 address

SSL VPN users in this example can access the office network on port 2. You need to define a firewall address that represents the OfficeLAN subnet IP address.

**To define destination addresses - web-based manager**

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

| | |
|---|---|
| **Address Name** | OfficeLAN |
| **Type** | Subnet / IP Range |
| **Subnet / IP Range** | 10.11.101.0/24 |
| **Interface** | port2 |

**To define destination addresses - CLI**

```
config firewall address
  edit OfficeLAN
    set type ipmask
    set subnet 10.11.101.0/24
    set associated-interface port2
  end
```

### Creating the tunnel client range address

In this example, all SSL-VPN users are assigned a single range of IP addresses. The tunnel client addresses must not conflict with each other or with other addresses in your network. The best way to accomplish this is to assign addresses from a subnet that is not used elsewhere in your network.

**To define tunnel client addresses - web-based manager**

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

| | |
|---|---|
| **Address Name** | SSL_tunnel_users |
| **Type** | Subnet / IP Range |
| **Subnet / IP Range** | 10.11.254.0/24 |
| **Interface** | Any |

**To define destination addresses - CLI**

```
config firewall address
  edit SSL_tunnel_users
    set type ipmask
    set subnet 10.11.254.0/24
  end
```

## Enabling SSL VPN and setting the tunnel user IP address range

By default, SSL VPN is not enabled. At the same time as you enable SSL VPN, you can define the IP address range from which SSL VPN tunnel-mode clients are assigned their virtual IP addresses.

**To enable SSL VPN and set tunnel address range - CLI**

```
config vpn ssl settings
  set sslvpn-enable enable
  set tunnel-ip-pools SSL_tunnel_users
end
```

**To set tunnel address range - web-based manager**

1. Go to *VPN* > *SSL* > *Config*.
2. In *IP Pools*, select *Edit*.
3. In the *Available* list, select *SSL_tunnel_users* and then select the down arrow button to move the address to the *Selected* list.
4. Select *OK*.
5. Select *Apply*.

## Creating the web portal

You need to create one web portal, portal1, for example.

**To create the portal1 web portal**

1. Go to *VPN* > *SSL* > *Portal* and select *Create New*.
2. In the *Name* field, enter `portal1`.
3. In *Applications*, select the application types to permit.

4 Select *OK,* then select *OK* again.

**To create the web portals - CLI**

```
config vpn ssl web portal
  edit portal1
    config widget
      edit 0
        set type tunnel
        set tunnel-status enable
      end
    end
```

## Creating the user account and user group

After enabling SSL VPN and creating the web portal, you need to create the user account and then the user group for the SSL VPN users. In the user group configuration, you select the web portal to which the users are directed.

**To create the user account - web-based manager**

1 Go to *User* > *User* and select *Create New*.

2 In *User Name*, enter `user1`.

3 Select *Password* and enter the password in the field on the right.

4 Select *OK*.

**To create the user account - CLI**

```
config user local
  edit user1
    set type password
    set password user1_pass
  end
```

**To create the user group - web-based manager**

1 Go to *User* > *User Group* > *User Group*.

2 Select *Create New* and enter the following information:

| | |
|---|---|
| **Name** | group1 |
| **Type** | SSL VPN |
| **Portal** | portal1 |

3 From the *Available* list, select *user1* and move it to the *Members* list by selecting the right arrow button.

4 Select *OK*.

**To create the user group - CLI**

```
config user group
  edit group1
    set group-type sslvpn
    set member user1
    set sslvpn-portal portal1
  end
```

## 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 network 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 72.

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.The authentication, ensures that only authorized users 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. A tunnel-mode policy is required if you want to provide a tunnel-mode connection for your clients.

### To create the SSL VPN security policy - web-based manager

1 Go to *Policy* > *Policy* > *Policy*.

2 Select *Create New* and enter the following information:

| | |
|---|---|
| **Source Interface/Zone** | port1 |
| **Source Address** | All |
| **Destination Interface/Zone** | port2 |
| **Destination Address** | OfficeLAN |
| **Action** | SSL-VPN |
| **User Authentication Method** | Local |

3 Select *Add* and enter the following information:

| | |
|---|---|
| **User Group** | group1 |
| **Service** | Any |
| **Schedule** | always |

4 Select *OK*, and then select *OK* again.

### To create the SSL VPN security policy - CLI

```
config firewall policy
  edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr all
    set dstaddr OfficeLAN
    set action ssl-vpn
    config identity-based-policy
      edit 1
        set groups group1
        set schedule always
        set service ANY
      end
    end
```

**To create the tunnel-mode security policy - web-based manager**

1 Go to *Policy* > *Policy* > *Policy.*

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

| | |
|---|---|
| **Source Interface/Zone** | sslvpn tunnel interface (ssl.root) |
| **Source Address** | SSL_tunnel_users |
| **Destination Interface/Zone** | port2 |
| **Destination Address** | OfficeLAN |
| **Schedule** | always |
| **Service** | ANY |
| **Action** | ACCEPT |
| **NAT** | Enable |

**To create the tunnel-mode security policy - CLI**

```
config firewall policy
  edit 0
    set srcintf ssl.root
    set dstintf port2
    set srcaddr SSL_tunnel_users
    set dstaddr OfficeLAN
    set action accept
    set schedule always
    set service ANY
    set nat enable
  end
```

## Add routing 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 accomplish this.

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

1 Go to *Router* > *Static* > *Static Route* and select *Create New*.

2 Enter the following information and select *OK*.

| | |
|---|---|
| **Destination IP/Mask** | `10.11.254.0/24`<br>This is the IP address range that you assigned to users of the web portal. See “Creating the tunnel client range address” on page 73. |
| **Device** | Select the SSL VPN virtual interface, *ssl.root* for example. |

Leave other settings at their default values.

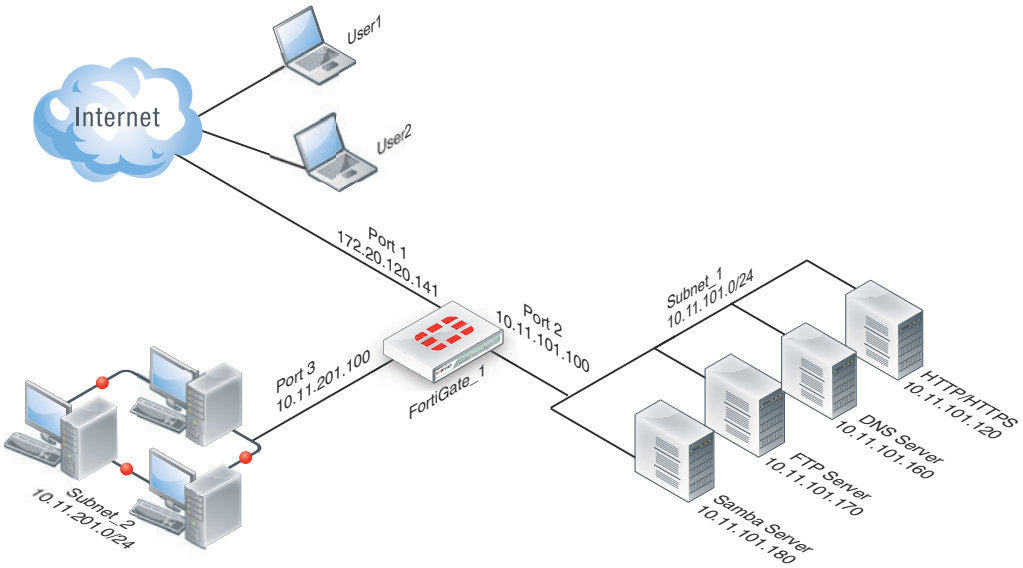
**To add a route to SSL VPN tunnel mode clients - CLI**

```
config router static
  edit 0
    set device ssl.root
    set dst 10.11.254.0/24
  end
```

# Multiple user groups with different access permissions example

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.

**Figure 10: SSL VPN configuration for different access permissions by user group**




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.
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 *Firewall Objectes* > *Address* > *Address.*

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

| | |
|---|---|
| **Address Name** | Subnet_1 |
| **Type** | Subnet / IP Range |
| **Subnet / IP Range** | 10.11.101.0/24 |
| **Interface** | port2 |

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

| | |
|---|---|
| **Address Name** | Subnet_2 |
| **Type** | Subnet / IP Range |
| **Subnet / IP Range** | 10.11.201.0/24 |
| **Interface** | port3 |

**To define destination addresses - CLI**

```
config firewall address
  edit Subnet_1
    set type ipmask
    set subnet 10.11.101.0/24
    set associated-interface port2
  next
  edit Subnet_2
    set type ipmask
    set subnet 10.11.201.0/24
    set associated-interface port3
  end
```

### 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 in your network.

**To define tunnel client addresses - web-based manager**

1 Go to *Firewall Objects* > *Address* > *Address.*

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

| | |
|---|---|
| **Address Name** | Tunnel_group1 |
| **Type** | Subnet / IP Range |
| **Subnet / IP Range** | 10.11.254.[1-50] |
| **Interface** | Any |

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

| | |
|---|---|
| **Address Name** | Tunnel_group2 |
| **Type** | Subnet / IP Range |
| **Subnet / IP Range** | 10.11.254.[51-100] |
| **Interface** | Any |

**To define tunnel client addresses - CLI**

```
config firewall address
  edit Tunnel_group1
    set type iprange
    set end-ip 10.11.254.50
    set start-ip 10.11.254.1
  next
  edit Tunnel_group2
    set type iprange
    set end-ip 10.11.254.100
    set start-ip 10.11.254.51
  end
```

## 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* > *Portal* and select *Create New*.
2 Enter `portal1` in the *Name* field and select *OK*.
3 In *Applications*, select all of the application types that the users can access.
4 Select the *Edit* icon on the *Tunnel Mode* widget.
5 In *IP Pools*, select *Edit*.
6 In the *Available* list, select *Tunnel_ group1* and then select the down arrow button. Select *OK*.
7 Select *OK* in the *Tunnel Mode* widget.
8 Select *OK*.

**To create the portal2 web portal**

1 Go to *VPN* > *SSL* > *Portal* and select *Create New*.
2 Enter `portal2` in the *Name* field and select *OK*.
3 In *Applications*, select all of the application types that the users can access.
4 Select the *Edit* icon on the *Tunnel Mode* widget.
5 In *IP Pools*, select *Edit*.
6 In the *Available* list, select *Tunnel_ group2* and then select the down arrow button. Select *OK*.
7 Select *OK* in the *Tunnel Mode* widget.
8 Select *OK*.

**To create the web portals - CLI**

```
config vpn ssl web portal
  edit portal1
    set allow-access ftp ping rdp smb ssh telnet vnc web
    config widget
      edit 0
        set type tunnel
        set tunnel-status enable
        set ip-pools "Tunnel_group1"
      end
    next
  edit portal2
    set allow-access ftp ping rdp smb ssh telnet vnc web
    config widget
      edit 0
        set type tunnel
        set tunnel-status enable
        set ip-pools "Tunnel_group2"
      end
    end
  end
```

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* > *User* 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* > *User Group* > *User Group*.
2. Select *Create New* and enter the following information:

| | |
|---|---|
| **Name** | group1 |
| **Type** | SSL VPN |
| **Portal** | portal1 |

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.

**To create the user groups - CLI**

```
config user group
  edit group1
    set group-type sslvpn
    set member user1
    set sslvpn-portal portal1
  next
```

```
edit group2
  set group-type sslvpn
  set member user2
  set sslvpn-portal portal2
end
```

## 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 78.

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 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* > *Policy* > *Policy.*

2 Select *Create New and* enter the following information:

| | |
|---|---|
| **Source Interface/Zone** | port1 |
| **Source Address** | All |
| **Destination Interface/Zone** | port2 |
| **Destination Address** | Subnet_1 |
| **Action** | SSL-VPN |

3 Select *Add* and enter the following information:

| | |
|---|---|
| **User Group** | group1 |
| **Service** | Any |

4 Select *OK*, and then select *OK* again.

5 Select *Create New and* enter the following information:

| | |
|---|---|
| **Source Interface/Zone** | port1 |
| **Source Address** | All |
| **Destination Interface/Zone** | port3 |
| **Destination Address** | Subnet_2 |
| **Action** | SSL-VPN |

6 Select *Add* and enter the following information:

| | |
|---|---|
| **User Group** | group2 |
| **Service** | Any |

**7** Select *OK*, and then select *OK* again.

**To create the SSL VPN security policies - CLI**

```
config firewall policy
  edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr all
    set dstaddr Subnet_1
    set action ssl-vpn
    set nat enable
    config identity-based-policy
      edit 1
        set groups group1
        set schedule always
        set service ANY
      end
    next
  edit 0
    set srcintf port1
    set dstintf port3
    set srcaddr all
    set dstaddr Subnet_2
    set action ssl-vpn
    set nat enable
    config identity-based-policy
      edit 1
        set groups group2
        set schedule always
        set service ANY
      end
    end
```

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

**1** Go to *Policy* > *Policy* > *Policy*.

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

| | |
|---|---|
| **Source Interface/Zone** | sslvpn tunnel interface (ssl.root) |
| **Source Address** | Tunnel_group1 |
| **Destination Interface/Zone** | port2 |
| **Destination Address** | Subnet_1 |
| **Action** | ACCEPT |
| **NAT** | Enable |

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

| | |
|---|---|
| **Source Interface/Zone** | sslvpn tunnel interface (ssl.root) |
| **Source Address** | Tunnel_group2 |
| **Destination Interface/Zone** | port3 |
| **Destination Address** | Subnet_2 |

| | |
|---|---|
| **Action** | ACCEPT |
| **NAT** | Enable |

**To create the tunnel-mode security policies - CLI**

```
config firewall policy
  edit 0
    set srcintf ssl.root
    set dstintf port2
    set srcaddr Tunnel_group1
    set dstaddr Subnet_1
    set action accept
    set schedule always
    set service ANY
    set nat enable
  next
  edit 0
    set srcintf ssl.root
    set dstintf port3
    set srcaddr Tunnel_group2
    set dstaddr Subnet_2
    set action accept
    set schedule always
    set service ANY
    set nat enable
  end
end
```

## 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 accomplish this.

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

1 Go to *Router* > *Static* > *Static Route* and select *Create New*.

2 Enter the following information and select *OK*.

| | |
|---|---|
| **Destination IP/Mask** | `10.11.254.0/24`<br>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 78. |
| **Device** | Select the SSL VPN virtual interface, *ssl.root* for example. |

Leave other settings at their default values.

**To add a route to SSL VPN tunnel mode clients - CLI**

```
config router static
  edit 0
    set device ssl.root
    set dst 10.11.254.0/24
  end
```

## Enabling SSL VPN operation

By default, SSL VPN is not enabled. SSL VPN is configured in the CLI only.

**To enable SSL VPN and set tunnel address range - CLI**

```
config vpn ssl settings
  set sslvpn-enable enable
  set tunnel-ip-pools SSL_tunnel_users
end
```

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

# Index