SSL VPN

FortiOS™ Handbook v3
for FortiOS 4.0 MR3
FortiOS™ Handbook SSL VPN
v3
30 April 2012
01-434-112804-20120430

© Copyright 2012 Fortinet, Inc. All rights reserved. Contents and terms are subject to change by Fortinet without prior notice. Reproduction or transmission of this publication is encouraged.

Trademarks

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Visit these links for more information and documentation for your Fortinet products:
Fortinet Knowledge Base - http://kb.fortinet.com
Technical Documentation - http://docs.fortinet.com
Training Services - http://campus.training.fortinet.com
Technical Support - http://support.fortinet.com
You can report errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.
# Contents

## Introduction
- Audience ........................................... 7

## Introduction to SSL VPN
- SSL VPN modes of operation .......................... 9
  - Web-only mode ................................... 10
  - Tunnel mode ..................................... 10
  - Port forwarding mode ............................... 11
  - Application support ............................... 12
- SSL VPN and IPv6 ................................... 12
- Traveling and security ............................... 12
  - Host check ...................................... 12
  - Cache cleaning .................................. 12

## Basic Configuration
- User accounts and groups ............................. 13
- Authentication ...................................... 14
- IP addresses for users .............................. 14
- Authentication of remote users ...................... 15
  - Setting the client authentication timeout ....... 15
  - Strong authentication with security certificates .... 15
- Configuring SSL VPN web portals .................... 16
- SSL connection configuration ....................... 17
- Portal configuration ................................ 17
  - Portal settings .................................. 18
  - Portal widgets ................................... 19
- Tunnel mode settings ................................ 21
  - Port forward tunnel ................................ 23
  - The Session Information widget ................. 24
  - The Bookmarks widget ............................ 24
  - The Connection Tool widget ...................... 26
- Configuring security policies ....................... 27
  - Firewall addresses ................................ 27
  - Create an SSL VPN security policy ............... 27
  - Create a tunnel mode security policy ............ 29
  - Routing for tunnel mode ......................... 30
  - Split tunnel Internet browsing policy ........... 30
  - Enabling a connection to an IPsec VPN ........... 31
SSL VPN for FortiOS 4.0 MR3

Contents

Additional configuration options .................................................. 33
Routing in tunnel mode .................................................................. 33
Changing the port number for web portal connections ...................... 33
SSL offloading ............................................................................. 34
Customizing the web portal login page ........................................... 34
Host Check. .................................................................................. 35
  Creating a custom host check list .................................................. 37
Windows OS check ....................................................................... 38
Configuring cache cleaning ............................................................ 39
Configuring virtual desktop ............................................................ 39
  Configuring virtual desktop application control .............................. 40
Configuring client OS Check .......................................................... 41
Adding WINS and DNS services for clients ...................................... 42
Setting the idle timeout setting ...................................................... 42
SSL VPN logs .............................................................................. 43
  Viewing log data .......................................................................... 43
Monitoring active SSL VPN sessions ............................................... 43
Troubleshooting ......................................................................... 44

The SSL VPN client ...................................................................... 45
FortiClient. ................................................................................... 45
Downloading the SSL VPN tunnel mode client. ............................... 46
Tunnel mode client configuration. ................................................... 47
Uninstalling the tunnel mode client. ............................................... 47

Setup examples .......................................................................... 49
Secure internet browsing ............................................................... 49
  Creating an SSL VPN IP pool and SSL VPN web portal ................. 49
  Creating the SSL VPN user and user group ................................ 50
Creating a static route for the remote SSL VPN user ...................... 50
Creating security policies ............................................................. 50
Results ......................................................................................... 51

Split Tunnel ................................................................................ 51
  Creating a firewall address for the head office server ...................... 52
    Creating an SSL VPN IP pool and SSL VPN web portal ............... 52
    Creating the SSL VPN user and user group ................................. 53
  Creating a static route for the remote SSL VPN user ...................... 53
  Creating security policies ........................................................... 53
Results ......................................................................................... 54

Multiple user groups with different access permissions example ........ 54
  General configuration steps ........................................................ 55
Creating the firewall addresses ....................................................... 55
Creating the destination addresses ............................................... 55
Contents

Creating the tunnel client range addresses ............................................. 56
Creating the web portals ........................................................................... 57
Creating the user accounts and user groups ............................................. 58
Creating the security policies ................................................................. 59
Create the static route to tunnel mode clients ........................................ 61
Enabling SSL VPN operation. ................................................................. 62

Index 63
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.
- **Basic Configuration** explains how to configure the FortiGate unit and the web portal. Along with these configuration details, this chapter also explains how to grant unique access permissions, 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.
- **The SSL VPN client** provides an overview of the FortiClient software required for tunnel mode, where to obtain the software, install it and the configuration information required for remote users to connect to the internal network.
- **Setup examples** explores several configuration scenarios with step-by-step instructions. While the information provided is enough to set up the described SSL VPN configurations, these scenarios are not the only possible SSL VPN setups.

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. Employees travelling across the country or around the world require timely and comprehensive access to network resources. As a result of the growing need for providing remote/mobile clients with easy, cost-effective and secure access to a multitude of resources, the concept of a Virtual Private Network was developed.

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 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.

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

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

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 or tunnel mode.
Web-only mode

Web-only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Sun Java runtime environment.

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 VP 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 and portal functionality is provided through small applets called widgets. Widget windows can be moved or minimized. The controls within each widget depend on its function. There are predefined web portals and the administrator can create additional portals.

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

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

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

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.

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.

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

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 “Tunnel mode settings” on page 21.

**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 forward mode, or proxy mode, provides this middle ground between web mode and tunnel mode.

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

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

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

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

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

For information on configuring a port forward tunnel, see “Port forward tunnel” on page 23.
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.

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)

Traveling and security

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

When setting up the portal, you can include two options to ensure corporate data is safe; a host check for antivirus software, and a cache cleaner.

Host check

You can enable a host integrity checker to scan the remote client. The integrity checker probes the remote client computer to verify that it is safe before access is granted. Security attributes recorded on the client computer (for example, in the Windows registry, in specific files, or held in memory due to running processes) are examined and uploaded to the FortiGate unit.

For more information, see “Host Check” on page 35.

Cache cleaning

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.

For more information, see “Cache cleaning” on page 12.
Basic Configuration

Configuring SSL VPN involves a number of configurations within FortiOS that you need to complete to make it all come together. This chapter describes the components required, and how and where to configure them to set up the FortiGate unit as an SSL VPN server. The configurations and steps are high level, to show you the procedures needed, and where in FortiOS they are located. For real-world examples, see the chapter, “Setup examples” on page 49.

There are three or four key steps to configuring an SSL VPN tunnel. The first three in the points below are mandatory, while the other is optional. This chapter will outline these four key steps, as well as additional configuration you can do for tighter security and monitoring.

The key steps are:

• Create user accounts and user groups for the remote clients.  
  (“User accounts and groups” on page 13)
• Create a web portal to define user access to network resources.  
  (“Configuring SSL VPN web portals” on page 16)
• Configure the security policies.  
  (“Configuring security policies” on page 27)
• For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.  
  (“Routing in tunnel mode” on page 33)
• Setup logging of SSL VPN activities.  
  (“SSL VPN logs” on page 43)

User accounts and groups

The first step for an SSL VPN tunnel is to add the users and user groups that will access the tunnel. You may already have users defined for other authentication-based security policies. These users and groups are identified when creating the security policy when defining the authentication rules.

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.

To create a user account

• in the web-based manager, go to User > User, and select Create New.
• in the CLI, use the commands in config user local.

All users accessing the SSL tunnel must be in a firewall user group. As part of configuring the user group, you select the SSL VPN web portal that the members of the group access after authentication.
To create user groups

- in the web-based manager, go to User > User Group > User Group and select Create New.
- in the CLI, use the commands in config user group.

Authentication

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

To authenticate users, you can use a plain text password on the 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.

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.

IP addresses for users

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

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

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

1. Go to 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.
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
```

You can select the 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 “Tunnel mode settings” on page 21.

Authentication of remote users

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

The web portal can include bookmarks to connect to internal network resources. A web (HTTP/HTTPS) bookmark can include login credentials so that the FortiGate unit automatically logs the user into the 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 67.

Setting the client authentication timeout

The client authentication timeout controls how long an authenticated user will remain connected. When this time expires, the system forces the remote client to authenticate again. As with the idle timeout, a shorter period of time is more secure. The default value is 28800 seconds (8 hours). You can only modify this timeout value in the CLI.

For example, to change the authentication timeout to 18000 seconds, enter the following commands:

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

Strong authentication with security certificates

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

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

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

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

1. Go to VPN > SSL > Config.
2. Select Require Client Certificate.
3. Select Apply.

To require client authentication by security certificates - CLI

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

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

In the FortiGate unit SSL VPN settings, you can select which certificate the FortiGate offers to authenticate itself. By default, the FortiGate unit offers its factory installed (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

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

**Configuring SSL VPN web portals**

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

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

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Pools</td>
<td>Select Edit to select the range or subnet firewall addresses that represent IP address ranges reserved for tunnel-mode SSL VPN clients. The IP Pool that you select will be the one created in the previous steps.</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>Select the signed server certificate to use for authentication. If you leave the default setting (Self-Signed), the FortiGate unit offers its factory installed certificate from Fortinet, to remote clients when they connect.</td>
</tr>
<tr>
<td>Require Client Certificate</td>
<td>Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process. For information on using PKI to provide client certificate authentication, see the User Authentication Guide.</td>
</tr>
<tr>
<td>Encryption Key Algorithm</td>
<td>Select the algorithm for creating a secure SSL connection between the remote client web browser and the FortiGate unit. This will depend on what the web browser of the client can support. 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 is transmitted over the SSL link.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Type the period of time (in seconds) that the connection can remain idle before the user must log in again. The range is from 10 to 28800 seconds. Setting the value to 0 will disable the idle connection timeout. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.</td>
</tr>
<tr>
<td>Login Port</td>
<td>Enter the port number for HTTPS access.</td>
</tr>
<tr>
<td>Advanced (DNS and WINS Servers)</td>
<td>Enter up to two DNS servers and/or two WINS servers to be provided for the use of clients.</td>
</tr>
</tbody>
</table>

Portal configuration

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

There are three pre-defined default web portal configurations available:
- full-access
- tunnel-access
- web-access
To view the portals settings page, go to VPN > SSL > Portal.

<table>
<thead>
<tr>
<th>Portal Settings page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit Settings window</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Add Widget</strong></td>
</tr>
<tr>
<td><strong>Widgets</strong></td>
</tr>
</tbody>
</table>

**Portal settings**

The portal settings determine what SSL VPN users see when they log in to the FortiGate unit. Both the FortiGate administrator and the SSL VPN user have the ability to customize the web portal settings.

Portal settings are configured by going to VPN > SSL > Portal and select Settings.

**General settings**

The general settings tab enables you to set up the portal container - what the remote user sees when they log in. It also is the location where you define what applications the remote user can use when connecting. The applications selected affect how you configure the widgets later on. For example, if you do not select the HTTP/HTTPS option, you cannot add bookmarks in the bookmark widget.

**Virtual Desktop settings**

The virtual desktop options, available for Windows XP and Windows Vista client PCs, are configured to completely isolate 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 unexpectedly, any files that may remain will be encrypted.

With the virtual desktop, you can define what the remote user can do when connected, including:

- switching between the virtual and remote desktop
- share contents of the clipboard between both desktops
- use removable media over the tunnel
- allow network share access and printing
- define what applications can be used.

Virtual desktop requires the Fortinet host check plug in. If the plug in is not present, it is automatically downloaded to the client computer.
Security Control settings

Security control options provide cache cleaning and host checking to the clients of your web portal. Cache cleaning clears information from the client browser cache just before the SSL VPN session ends. The cache cleaner is effective only if the session terminates normally. The cache is not cleaned if the session ends unexpectedly.

Host checking enforces the client’s use of antivirus or firewall software. Each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for specific security software selected from the Host Check list located at VPN > SSL > Host Check. See “Host Check” on page 35.

Portal widgets

Portal widgets are sections of information that the user will view when they log in to the portal. By default, all widgets are shown. You can modify or remove widgets as required.

Session Information

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.

Bookmarks

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

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

Connection Tool

Use the Connection Tool widget to connect to a internal network resource without adding a bookmark to the bookmark list. You select the type of resource and specify the URL or IP address of the host computer.

Tunnel Mode

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.

Configuring the web portal page layout

You can determine which widgets are displayed on the web portal page and adjust the layout.
To configure the web portal page - web-based manager

On the web portal page itself, you 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:
  - “Tunnel mode settings” on page 21
  - “The Session Information widget” on page 24
  - “The Connection Tool widget” on page 26
- 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 26
  - “Configuring cache cleaning” on page 39
  - “Configuring virtual desktop” on page 39
  - “Configuring client OS Check” on page 41 (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, although due its complexity, is not recommended. 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 1 on page 20, 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
```

**Tunnel mode settings**

If your web portal provides tunnel mode access, the *Tunnel Mode* widget is included automatically when creating a new portal, with the *Split Tunneling* option enabled so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user’s other traffic follows its normal route. 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.

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

---

*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`.***
To configure tunnel mode settings - web-based manager

1. Go to VPN > SSL > Portal and select Create New.
2. Select the Edit icon in the Tunnel Mode widget title bar.

Figure 2: Tunnel Mode widget - edit mode

3. Enter the following information:

| Name | Enter a name for the widget. |
| IP Mode | Select the mode by which the IP address is assigned to the user. |
| Range | Use 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 | 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 | Split tunneling is enabled by default. 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.

4. Select OK in the Tunnel Mode widget.
5. 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:

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

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

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:

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

**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 16. To configure the application, create a bookmark with the Type of `PortForward`. 
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.

Ensure that HTTP/HTTPS is enabled in the Applications list of the General settings, by selecting the Settings button in the portal configuration window.

To configure the Bookmarks widget

1. Go to VPN > SSL > Portal, and select Create New.
2. Select the Edit icon in the Bookmarks widget title bar.
3. Select the Applications check boxes for the types of bookmarks that you want to support.
4. To add a bookmark, select Add.
5 Enter or edit the following information:

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

**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. If you are an administrator configuring a bookmark for users: Enter %username% to represent the user’s SSL VPN user name. Enter %passwd% to represent the user’s SSL VPN password. |
| Add | Enter another Field Name / Value pair, for the password for example. A new set of Field Name / Value fields is added. |

6 Select OK.

7 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:

```bash
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
```

The Connection Tool widget

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

Ensure that what you want remote users to connect to is enabled in the Applications list of the General settings, by selecting the Settings button in the portal configuration window.

To configure the Connection Tool widget

1. Go to VPN > SSL > Portal, and select Create New.
2. Select the Edit icon in the Connection Tool widget title bar.
3. Enter a new Name for the widget.
4. Select the types of Applications that the Connection Tool is enabled to access.
5. 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
```
Configuring security policies

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

This section contains the procedures needed to configure security policies for web-only mode operation and tunnel-mode operation. These procedures assume that you have already completed the procedures outlined in “User accounts and groups” on page 13.

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

Firewall addresses

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

For tunnel mode, you will already have defined firewall addresses for the IP address ranges that the FortiGate unit will assign to SSL VPN clients. See “Windows OS check” on page 38.

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

To create a firewall address, in the web-based manager, go to Firewall Objects > Address > Address, and select Create New. Using the CLI, use the commands in config firewall address.

Create an SSL VPN security policy

At minimum, you need one SSL VPN security policy to authenticate users and provide access to the protected networks. You will need additional security policies only if you have multiple web portals that provide access to different resources.

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.
- 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.

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

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

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

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Select the name of the FortiGate network interface to that connects to the Internet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Select all.</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the FortiGate network interface that connects to the protected network.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the firewall address you created that represents the networks and servers to which the SSL VPN clients will connect. If you want to associate multiple firewall addresses or address groups with the Destination Interface/Zone, from Destination Address, select the plus symbol. In the dialog box, move the firewall addresses or address groups from the Available Addresses section to the Members section, then select OK.</td>
</tr>
<tr>
<td>Action</td>
<td>Select SSL-VPN.</td>
</tr>
<tr>
<td>SSL Client Certificate Restrictive</td>
<td>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 “Strong authentication with security certificates” on page 15.</td>
</tr>
<tr>
<td>Cipher Strength</td>
<td>Select the bit level of SSL encryption. The web browser on the remote client must be capable of matching the level that you select.</td>
</tr>
<tr>
<td>Configure SSL-VPN Users</td>
<td>A security policy for an SSL VPN is automatically an identity-based policy.</td>
</tr>
<tr>
<td>Add</td>
<td>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.</td>
</tr>
<tr>
<td>User Group</td>
<td>Select user groups in the left list and use the right arrow button to move them to the right list.</td>
</tr>
<tr>
<td>Service</td>
<td>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.</td>
</tr>
</tbody>
</table>
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
```

**Create a tunnel mode security policy**

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

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

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

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

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Select the virtual SSL VPN interface, such as <code>ssl.root</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Select the firewall address you created that represents the IP address range assigned to SSL VPN clients, such as <code>SSL_VPN_tunnel_users</code>.</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the interface that connects to the protected network.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the firewall address that represents the networks and servers the SSL VPN clients will connect to. To select multiple firewall addresses or address groups, select the plus sign next to the drop-down list.</td>
</tr>
</tbody>
</table>
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.

Routing for tunnel mode

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

To add the tunnel mode route - web-based manager

1. Go to **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
```

Split tunnel Internet browsing policy

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

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

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Select the virtual SSL VPN interface, ssl.root, for example.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Select the firewall address you created that represents the IP address range assigned to SSL VPN clients.</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the FortiGate network interface that connects to the Internet.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select all.</td>
</tr>
<tr>
<td>Action</td>
<td>Select Accept.</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable.</td>
</tr>
<tr>
<td></td>
<td>Leave other settings at their default values.</td>
</tr>
</tbody>
</table>

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 a connection to an IPsec VPN

You might want to provide your SSL VPN clients access to another network, such as a branch office, that is connected by an IPsec VPN. To do this, you need only to add the appropriate security policy. For information about route-based and policy-based IPsec VPNs, see the IPsec VPN Guide.

Route-based Connection

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.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Select the virtual SSL VPN interface, ssl.root, for example.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Select the firewall address that represents the IP address range assigned to SSL VPN clients.</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the virtual IPsec interface for your IPsec VPN.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the address of the IPsec VPN remote protected subnet.</td>
</tr>
</tbody>
</table>
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
```

Policy-based connection

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

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

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Select the virtual SSL VPN interface, ssl.root, for example.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Select the firewall address that represents the IP address range assigned to SSL VPN clients.</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the FortiGate network interface that connects to the Internet.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the address of the IPsec VPN remote protected subnet.</td>
</tr>
<tr>
<td>Action</td>
<td>Select IPSEC.</td>
</tr>
<tr>
<td>VPN tunnel</td>
<td>Select the Phase 1 configuration name of your IPsec VPN.</td>
</tr>
<tr>
<td>Allow inbound</td>
<td>Enable</td>
</tr>
<tr>
<td>Allow outbound</td>
<td>Enable</td>
</tr>
<tr>
<td>NAT inbound</td>
<td>Enable</td>
</tr>
</tbody>
</table>

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.

**Additional configuration options**

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

**Routing in tunnel mode**

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

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

1. Go to 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
```

**Changing the port number for web portal connections**

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

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
```

SSL offloading

Configuring SSL offloading that allows or denies client renegotiation, is configured in the CLI. This feature helps to resolve the issues that affect all SSL and TLS servers that support renegotiation, identified by the Common Vulnerabilities and Exposures system in CVE-2009-3555. The IETF is currently working on a TLS protocol change that will permanently resolve the issue. The SSL offloading renegotiation feature is considered a workaround until the IETF permanently resolves the issue.

The CLI command is `ssl-client-renegotiation` and is found in config firewall vip command.

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 form of replacement message, in HTML format. You can modify the content to display a customized message. Note that there are specific fields that must remain in the code to ensure the page appears correctly in the user’s browser.

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.

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.
4. Edit the HTML text. Note the following content that must remain on the page:
   - The login page must contain 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-eq
viv="cache-control" content="no-cache"> <meta http-eq
viv="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.openner && window.openner.top) {
window.openner.top.location = window.openner.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>
<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.

**Host Check**

When you enable AV, FW, or AV-FW host checking in the web portal Security Control settings, each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for security software selected from the Host Check list. For more information, see “Portal settings” on page 18.

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

To configure host checking, go to **VPN > SSL > Host Check**. To add to the list, select **Create New**.
Host integrity checking is only possible with client computers running Microsoft Windows platforms.

### Host Check Software page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the host check list.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of host checking, either AV or FW.</td>
</tr>
<tr>
<td>GUID</td>
<td>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.</td>
</tr>
<tr>
<td>Version</td>
<td>Enter the software’s version.</td>
</tr>
<tr>
<td>Create New</td>
<td>Creates a new check item to add to the list below.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies the settings within the software.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the check software item from the list on the Host Check Software page. To remove multiple check software items from the list, select the check box for each row to remove, and select Delete.</td>
</tr>
<tr>
<td>#</td>
<td>The order in which each item is listed.</td>
</tr>
<tr>
<td>Target</td>
<td>The type of target that you chose.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of check that you chose.</td>
</tr>
<tr>
<td>Action</td>
<td>The type of action that you chose.</td>
</tr>
</tbody>
</table>

### Host Check Software window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select how the FortiGate unit checks for the correct version of the application.</td>
</tr>
<tr>
<td>Action</td>
<td>Select one of the following: Require – If the item is found, the client meets the check item condition. 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.</td>
</tr>
<tr>
<td>File/Path</td>
<td>Enter the file name and path. This field appears when you select the Type of File.</td>
</tr>
<tr>
<td>Process</td>
<td>Enter the application’s executable file name. This field appears when you select the Type of Process.</td>
</tr>
<tr>
<td>Registry</td>
<td>Enter the registry number of the application. This field appears when you select the Type of Registry.</td>
</tr>
</tbody>
</table>
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:

```bash
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:

```bash
config vpn ssl web portal
  edit full-access
    set host-check custom
    set host-check-policy FortiClient-AV FortiClient-FW
  end
```

Creating a custom host check list

If you configure a custom host check for your web portal (see “Host Check” on page 35), 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.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name of the application. The name does not need to match the actual application name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the type of security application. Can be AV for antivirus or FW for firewall.</td>
</tr>
<tr>
<td>GUID</td>
<td>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.</td>
</tr>
<tr>
<td>Version</td>
<td>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.</td>
</tr>
</tbody>
</table>
Additional configuration options

<table>
<thead>
<tr>
<th>Create New</th>
<th>If you do not know the GUID, add alternative checks for the application. The security software is considered found only if all checks succeed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select how to check for the application:</td>
</tr>
<tr>
<td></td>
<td>- 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</td>
</tr>
<tr>
<td></td>
<td>- Process — Look for the application as a running process. In Process, enter the application’s executable file name.</td>
</tr>
<tr>
<td></td>
<td>- Registry — Search for a Windows Registry entry. In Registry, enter a registry item, for example HKLM\SOFTWARE\Fortinet\FortiClient\Misc</td>
</tr>
<tr>
<td>Action</td>
<td>Select one of</td>
</tr>
<tr>
<td></td>
<td>- Require — If the item is found, the client meets the check item condition.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>MD5 Signatures</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

```plaintext
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
```

SSL VPN for FortiOS 4.0 MR3

01-434-112804-20120430

http://docs.fortinet.com/
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.

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 and then select the Security Control tab.
3. Select Clean Cache.
4. 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 plug in. If the plug in 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 and then select the Virtual Desktop tab.
3. Select Enable Virtual Desktop.
4. Enable the other options as needed.
5 Optionally, select an Application Control List.
   See "Configuring virtual desktop application control".
6 Select OK, then 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.

Configuration is located in VPN > SSL > Virtual Desktop Application Control and select Create New.

<table>
<thead>
<tr>
<th>Virtual Desktop Application Control List page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Enter a name for the virtual desktop application list.</td>
</tr>
<tr>
<td>Allow the applications on the list and block all others</td>
</tr>
<tr>
<td>Select to allow the applications on this list.</td>
</tr>
<tr>
<td>Block the applications on the list and allow all others</td>
</tr>
<tr>
<td>Select to block the applications on the list.</td>
</tr>
<tr>
<td>Create New</td>
</tr>
<tr>
<td>Creates a new application signature.</td>
</tr>
<tr>
<td>Edit</td>
</tr>
<tr>
<td>Modifies the settings within the application signature.</td>
</tr>
<tr>
<td>Delete</td>
</tr>
<tr>
<td>Removes an application signature from the list on the Virtual Desktop Application Control List page.</td>
</tr>
<tr>
<td>To remove multiple signatures from the list, on the Virtual Desktop Application Control List page, select the check box for the applications and select Delete.</td>
</tr>
<tr>
<td>Applications</td>
</tr>
<tr>
<td>The name of the application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Signatures (window)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Enter the name of the application.</td>
</tr>
<tr>
<td>MD5 Signatures (one per line)</td>
</tr>
<tr>
<td>Enter the MD5 signature for application executable file. You can enter more than one but each one requires to be on a separate line. Entering multiple MD5 signatures helps to match multiple versions of the application.</td>
</tr>
</tbody>
</table>
There are two types of application control list:

- allow the listed applications and block all others
- 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.

```plaintext
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
```

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
```plaintext
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

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

SSL VPN logs

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

For more information on configuring logs on the FortiGate unit, see the Logging and Reporting Guide.

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

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

```bash
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
```

Logging of SSL VPN traffic is configured when you create the security policy, by selecting the Log Allowed Traffic option in the web-based manager or using the CLI command set logtraffic enable under config firewall policy.

Viewing log data

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

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.

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 SSL VPN port assignment (default 10443). Verify the SSL VPN security policy. |
| Error: “The web page cannot be found.” | Check URL: 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 “Routing for tunnel mode” on page 30. |
| 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 to the latest firmware then use the following CLI command: config vpn ssl settings set route-source-interface enable 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 the error message “Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12)” appears. 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 FortiClient. Access to the web portal or tunnel will fail if Internet Explorer has the privacy Internet Options set to High. If set to High, Internet Explorer will: Block cookies that do not have a compact privacy policy. Block cookies that use personally identifiable information without your explicit consent. |
The SSL VPN client

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

- **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** establishes a connection to the remote protected network that any application can use. This requires FortiClient SSL VPN application that sends and receives data through the SSL VPN tunnel.

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

  If the client computer runs Linux or Mac OS X, the user needs to download the tunnel mode client application from the Fortinet Support web site. See the Release Notes for your FortiOS firmware for the specific operating system versions that are supported.

  On Linux and Mac OS X platforms, tunnel mode operation cannot be initiated from the web portal Tunnel Mode widget. The remote user must use the standalone tunnel client 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.

**FortiClient**

Remote users can use FortiClient software to initiate an SSL VPN tunnel to connect to the internal network. FortiClient uses local port TCP 1024 to initiate an SSL encrypted connection to the FortiGate unit, on port TCP 10443. When connection using FortiClient, the FortiGate unit authenticates the FortiClient SSL VPN request based on the user group options. The FortiGate unit establishes a tunnel with the client and assigns a virtual IP address to the client PC. Once the tunnel has been established, the user can access the network behind the FortiGate unit.
There are three FortiClient application options available, depending on your requirements:

- FortiClient/FortiClient Premium
- FortiClient Lite (free) - http://download.cnet.com/FortiClient-Lite/3000-2239_4-75532356.html
- Standalone client (free)
- iPhone and iPad app available for free from the iTunes App Store.

For details on configuring FortiClient for SSL VPN, see the FortiClient documentation.

**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.

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**

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

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.
Tunnel mode client configuration

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

<table>
<thead>
<tr>
<th>Connection Name</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with your user account.</td>
</tr>
<tr>
<td>Client Certificate</td>
<td>Use this field if the SSL VPN requires a certificate for authentication. Select the required certificate from the drop-down list. The certificate must be installed in the Internet Explorer certificate store.</td>
</tr>
<tr>
<td>Settings...</td>
<td>Select to open the Settings dialog and select the Keep connection alive until manually stopped check box to prevent tunnel connections from closing due to inactivity.</td>
</tr>
</tbody>
</table>

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.
Setup examples

The examples in this chapter demonstrate the basic configurations needed for common connections to the SSL VPN tunnel and portals, applying the steps outlined in the chapter “Basic Configuration” on page 13.

The example included are:

- Secure internet browsing
- Split Tunnel
- Multiple user groups with different access permissions example

Secure internet browsing

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

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

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to VPN > SSL > Config and for IP Pools select Edit and add SSLVPN_TUNNEL_ADDR1 to the Selected table.
2. Create the SSL VPN portal to by going to VPN > SSL > Portal and selecting tunnel-access.
3. Select the Edit pencil icon for the Tunnel Mode widget and enter the following:
Creating the SSL VPN user and user group

Create the SSL VPN user and add the user to a user group configured for SSL VPN use.

1. Go to User > User > User and select Create New to add the user:

   - **User Name**: twhite
   - **Password**: password

2. Select OK.

3. Go to User > User Group > User Group and select Create New to add twhite to the SSL VPN user group:

   - **Name**: Tunnel
   - **Type**: Firewall
   - **Allow SSL-VPN Access**: tunnel-access

Make sure you select the Allow SSL VPN Access option. If not selected, the Tunnel user group will not appear in the group list when configuring the authentication security policy.

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

Creating a static route for the remote SSL VPN user

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

1. Go to Router > Static > Static and select Create New to add the static route:

   - **Destination IP/Mask**: 10.212.134.0/255.255.255.0
   - **Device**: ssl.root

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

2. Select OK.

Creating security policies

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

1. Go to Policy > Policy > Policy and select Create New to add the SSL VPN security policy:

   - **Name**: Browsing
   - **IP Mode**: User Group
   - **IP Pools**: SSLVPN_TUNNEL_ADDR1

4. Select OK.
2. Select Configure SSL-VPN Users and select Add to add an authentication rule for the remote user:

<table>
<thead>
<tr>
<th>Selected User Groups</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Services</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
</tbody>
</table>

If the Tunnel user group does not appear in the User Group list, ensure you select the SSL VPN Access option when creating the user group. If that option is not selected, the Tunnel user group will not appear in the user group list when configuring the authentication security policy.

3. Select OK.

4. Select Create New to add a security policy that allows remote SSL VPN users to connect to the Internet:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>ssl.root</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

5. Select OK.

Results

Using FortiClient SSLVPN application, log into the VPN using the address https://172.20.120.136:10443/ and log in as twhite. Once connected, you can browse the Internet.

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

Split Tunnel

For this example, the remote users are configured to be able to securely access head office internal network servers, and browse the Internet through the head office firewall. This will enable the remote user to use the FortiGate security to connect to the internal network and the web.
This solution describes how to configure FortiGate SSL VPN split tunnelling using the FortiClient SSL VPN software, available from the Fortinet Support site.

Using split tunneling, all communication from remote SSL VPN users to the head office internal network and to the Internet uses an SSL VPN tunnel between the user’s PC and the head office FortiGate unit. Connections to the Internet are routed back out the head office FortiGate unit to the Internet. Replies come back into the head office FortiGate unit before being routed back through the SSL VPN tunnel to the remote user.

Creating a firewall address for the head office server

1. Go to Firewall Objects > Address > Address and select Create New and add the head office server address:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Head office server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>192.168.1.12</td>
</tr>
<tr>
<td>Interface</td>
<td>Internal</td>
</tr>
</tbody>
</table>

2. Select OK.

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to VPN > SSL > Config and for IP Pools select Edit and add SSLVPN_TUNNEL_ADDR1 to the Selected table.

2. Create the SSL VPN portal to by going to VPN > SSL > Portal and selecting tunnel-access.

3. Select the Edit pencil icon for the Tunnel Mode widget and enter the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Connect to head office server</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Mode</td>
<td>User Group</td>
</tr>
<tr>
<td>IP Pools</td>
<td>SSLVPN_TUNNEL_ADDR1</td>
</tr>
<tr>
<td>Split Tunneling</td>
<td>Enable</td>
</tr>
</tbody>
</table>

4. Select OK.
Creating the SSL VPN user and user group

Create the SSL VPN user and add the user to a user group configured for SSL VPN use.

1. Go to User > User > User, select Create New and add the user:

<table>
<thead>
<tr>
<th>User Name</th>
<th>twhite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>password</td>
</tr>
</tbody>
</table>

2. Select OK.

3. Go to User > User Group > User Group and select Create New to add twhite to the SSL VPN user group:

<table>
<thead>
<tr>
<th>Name</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
<tr>
<td>Allow SSL-VPN Access</td>
<td>tunnel-access</td>
</tr>
</tbody>
</table>

Make sure you select the Allow SSL-VPN Access option. If not selected, the Tunnel user group will not appear in the group list when configuring the authentication security policy.

4. Move twhite to the Members list.

5. Select OK.

Creating a static route for the remote SSL VPN user

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

1. Go to Router > Static > Static and select Create New to add the static route:

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>10.212.134.0/255.255.255.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>ssl.root</td>
</tr>
</tbody>
</table>

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

2. Select OK.

Creating security policies

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

1. Go to Policy > Policy > Policy and select Create New to add the SSL VPN security policy:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>wan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>internal</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Head office server</td>
</tr>
<tr>
<td>Action</td>
<td>SSL-VPN</td>
</tr>
</tbody>
</table>
2 Select Configure SSL-VPN Users and select Add to add an authentication rule for the remote user:

<table>
<thead>
<tr>
<th>Selected User Groups</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Services</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
</tbody>
</table>

If the Tunnel user group does not appear in the User Group list, ensure you select the SSL VPN Access option when creating the user group. If that option is not selected, the Tunnel user group will not appear in the user group list when configuring the authentication security policy.

3 Select OK.

4 Select Create New to add a security policy that allows remote SSL VPN users to connect to the Internet:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>ssl.root</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

5 Select OK.

Results

Using the FortiClient SSL VPN application on the remote PC, connect to the VPN using the address https://172.20.120.136:10443/ and log in with the twhite user account. Once connected, you can connect to the head office server or browse to web sites on the Internet.

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

Multiple user groups with different access permissions 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 3: 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 Objects > Address > Address.

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

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Subnet_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.101.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>port2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Subnet_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.201.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>port3</td>
</tr>
</tbody>
</table>

To define destination addresses - CLI

```plaintext
config firewall address
diff Subnet_1
    set type ipmask
    set subnet 10.11.101.0/24
    set associated-interface port2
next
diff 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:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Tunnel_group1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.254.[1-50]</td>
</tr>
<tr>
<td>Interface</td>
<td>Any</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Tunnel_group2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
</tbody>
</table>
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
```

**Table:**

<table>
<thead>
<tr>
<th>Subnet / IP Range</th>
<th>10.11.254.[51-100]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Any</td>
</tr>
</tbody>
</table>
Multiple user groups with different access permissions example

Setup examples

SSL VPN for FortiOS 4.0 MR3

http://docs.fortinet.com/

Multiple user groups with different access permissions example

SSL VPN for FortiOS 4.0 MR3

http://docs.fortinet.com/

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>group1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>SSL VPN</td>
</tr>
<tr>
<td>Portal</td>
<td>portal1</td>
</tr>
</tbody>
</table>

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
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 55.

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:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>All</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Subnet_1</td>
</tr>
<tr>
<td>Action</td>
<td>SSL-VPN</td>
</tr>
</tbody>
</table>

3. Select Add and enter the following information:

<table>
<thead>
<tr>
<th>User Group</th>
<th>group1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Any</td>
</tr>
</tbody>
</table>

4. Select OK, and then select OK again.
5. Select Create New and enter the following information:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>All</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port3</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Subnet_2</td>
</tr>
<tr>
<td>Action</td>
<td>SSL-VPN</td>
</tr>
</tbody>
</table>

6. Select Add and enter the following information:

<table>
<thead>
<tr>
<th>User Group</th>
<th>group2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Any</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>sslvpn tunnel interface (ssl.root)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Tunnel_group1</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Subnet_1</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>sslvpn tunnel interface (ssl.root)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Tunnel_group2</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port3</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Subnet_2</td>
</tr>
</tbody>
</table>
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
```

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`.

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>10.11.254.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 56.</td>
<td></td>
</tr>
</tbody>
</table>

Device | Select the SSL VPN virtual interface, `ssl.root` for example. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave other settings at their default values.</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

A
authentication
  client certificates, 17
  server certificate and SSL VPN, 17
  authentication timeout setting, 15

C
cache cleaner, 12
certificate, server, 17
checking windows version, 38
certificates
  downloading, 46
  client certificates, 17

D
downloading
tunnel client, 46

F
FortiClient, 49, 52

H
host check, 35
  custom, 37
  introduction, 12
  OS, 41
host OS, patch check, 41

I
idle timeout setting, 42
installation on Vista, 11
IP address
tunnel mode range, 14

L
logging
  enabling SSL VPN events, 43
  setting event-logging parameters, 43

M
modes of operation
  overview, 9
  port forwarding, 11
  tunnel mode, 10
  web-only mode, 10

O
OS
  host patch check, 41
  OS patch check, 38

P
patch check
  host OS, 41
  port
    forwarding, 11
    number, web-portal connections, 33

R
remote Internet access, 49
replacement message, to customize web portal login page, 34
routing, 33

S
security policy
  web-only mode access, 27
server certificate, 17
Single Sign On (SSO), 15
split tunnel, 51
split tunneling, 52
SSL VPN
  allow/deny client renegotiation, 34
  checking client certificates, 17
  downloading client, 46
  enabling, 62
  event logging, 43
  FortiClient, 52
  host check, 35
  host OS patch check, 41
  portal widgets, 19
    bookmarks, 19
    connection tool, 19
    session information, 19
  tunnel mode, 19
  specifying server certificate, 17
  specifying timeout values, 17
  split tunneling, 52
  Subsession, 51
  Virtual Desktop, 45
  web portal, 16
ssl.root, 50, 53
SSO (Single Sign On), 15

T
timeout values, 17
Index

Tunnel Mode, 49
  tunnel mode, 10
  configuring FortiGate server, 29
  IP address range, 14
  routing, 33

U
  user accounts, 13
  user groups, 13
  different access permissions, 54

V
  Virtual Desktop, 45

W
  web portal
    customizing login page, 34
    setting login page port number, 33
  SSL VPN, SSL VPN web portal
    customize, 16
  web-only mode, 10
    security policy for, 27
  windows version check, 38

X
  X.509 security certificates, 15