FortiOS™ Handbook

SSL VPN for FortiOS 5.0

SSL VPN for FortiOS 5.0

May 22, 2014

01-504-112804-20140522

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Contents

Change Log

Date	Change Description
2014-05-22	Update to configuring web-based and tunnel mode policies.
2013-10-30	Minor edit - setting web portal tunnel-mode IP pools.
2013-09-16	Added RFCs 2246, 4346, 5246, 6101, and 6176 for SSL and TLS support.
2012-11-02	New FortiOS 5.0 release.

Chapter 1 SSL VPN for FortiOS 5.0

- 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.

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.

FortiOS supports the SSL and TLS versions defined below.

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

Table 1. SSL and TLS version support table.

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 VPN security in the FortiGate unit and the SSL security in the web browser. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

FortiGate SSL VPN web portals have a 1- or 2-column page layout 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, Firefox, Chrome, 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 authentication 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 and split tunneling” 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 21.

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 30.

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 "Configuring cache cleaning" on page 32.

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 39.

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 17)
- Configure the security policies.
  ("Configuring security policies" on page 22)
- For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.
  ("Routing in tunnel mode" on page 29)
- Setup logging of SSL VPN activities.
  ("SSL VPN logs" on page 34)

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. You can use one policy for multiple groups, or multiple policies to handle differences between the groups such as access to different services, or different schedules.

To create a user account

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

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

To create user groups

- in the web-based manager, go to *User & Device* > *User* > *User Groups* 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 *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 *Authentication Guide*.

MAC host check

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

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

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

IP addresses for users

After the FortiGate unit authenticates a request for a tunnel-mode connection, the FortiGate unit assigns the SSL VPN client an IP address for the session. The address is assigned from an 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* > *Addresses* and select *Create New*.
2. Enter an *Name*, for example, `SSL_VPN_tunnel_range`.
3. Select a *Type* of *IP Range*.
4. In the *Subnet/IP Range* field, enter the starting and ending IP addresses that you want to assign to SSL VPN clients, for example `10.254.254.[80-100]`.
5. In *Interface*, select *Any*.
6. Select *OK*.

To set tunnel-mode client IP address range - CLI

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

```
config firewall address
  edit SSL_tunnel_users
    set type iprange
    set end-ip 10.254.254.100
    set start-ip 10.254.254.80
  end
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 and split tunneling" 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 20.

Setting the client authentication timeout

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

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

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

You can also set the idle timeout for the client, to define how long the user does not access the remote resources before they are logged out. For information see "SSL connection configuration" on page 18.

Allow one time login per user

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

To do this, go to *VPN* > *SSL* > *Portal* and select to disable *Allow Multiple Concurrent Sessions for Each User*. It is enabled by default.

To configure in the CLI, enter the commands:

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

Once set, once the user has logged in, no other user can use the same login credentials.

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 *Authentication Guide*.

You can select the *Require Client Certificate* option in *SSL VPN config* 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

```
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

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

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

NSA Suite B cryptography support

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

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

```
exec vpn certificate local generate ec
```

Configuring SSL VPN web portals

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 *Authentication Guide*.

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, and 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 log in options, go to *VPN* > *SSL* > *Config.*

IP Pools	Select *Edit* to select the range or subnet firewall addresses that represent IP address ranges reserved for tunnel-mode SSL VPN clients.
Server Certificate	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.
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process. For information on using PKI to provide client certificate authentication, see the *Authentication Guide*.
Encryption Key Algorithm	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.
Idle Timeout	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. You can also set the authentication timeout for the client, to define how long the user can remain connected to the network. For information see "Setting the client authentication timeout" on page 15.
Login Port	Enter the port number for HTTPS access.
Enable Endpoint Registration	Select so that FortiClient registers with the FortiGate unit when connecting. If you configured a registration key by going to *System* > *Config* > *Advanced*, the remote user is prompted to enter the key. This only occurs on the first connection to the FortiGate unit.
Advanced (DNS and WINS Servers)	Enter up to two DNS servers and/or two WINS servers to be provided for the use of clients.

Portal configuration

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

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

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

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

Each web portal type include similar configuration options. Select between the different portals by selecting one from the drop-down list in the upper right corner of the window. You can also create a custom portal by selecting the plus sign next to the portal drop-down list.

Name	The name for the portal
Portal Message	This is a text header that appears on the top of the web portal.
Theme	A color styling for the web portal.
Page Layout	Select one or two column layouts for the widgets that appear on the web portal page.
Enable 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.
Enable Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route.
IP Pools	Select an IP Pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. **Save Password** - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. **Auto Connect** - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. **Always Up (Keep Alive)** - When enabled, if the user selects this option, the FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.
Enable Web Mode	Select to enable web mode access.
Applications	Select the applications the user can access when connected over the VPN portal.
Include Session Info	Select to display the Session Information widget on the portal page. 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.

Include Connection Tool	Select to display the Connection Tool widget on the portal page. 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.
Include Bookmarks	Select to include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window appears with the web page. Telnet, VNC, and RDP require a browser plug-in. FTP and Samba replace the bookmarks page with an HTML file-browser.
Prompt Mobile Users to Download FortiClient App	If a remote user is using web browser to connects to the SSL VPN in web mode they are prompted to download the FortiClient Application. The remote user can accept or reject the notification. If the user accepts, they are redirected to the FortiClient web site.
Allow Multiple Concurrent Sessions for Each User	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same credentials again. To prevent multiple logins, clear the check box.

Adding bookmarks

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.

To add a bookmark

1. On the *VPN* > *SSL* > *Portal* page, ensure *Include Bookmarks* is enabled.
2. Select *Create New* and enter the following information:

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

Select *OK*.

For more configuration options, see “Additional configuration options” on page 28.

Personal bookmarks

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

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

On mid-range and high end FortiGate units, this feature is enabled by default. On low-end FortiGate units, it must be enabled.

To enable personal bookmarks

1. Go to *System* > *Admin* > *Settings*.
2. In the *Display Options on GUI* section, select *SSPVPN Personal Bookmark Management*.
3. Select *Apply*.

Custom login screen

You can create a custom log in for your remote SSL VPN users. When configured with a security policy, when the user connects to the SSL VPN portal, a custom log in screen appears. With this screen, you can define the address, customize the look and define how many users are can connect at any one time to the portal.

To configure the login screen, go to V*PN* > *SSL* > *Custom*, and selecting *Create New*.

When adding the URL Path, you only need to enter the subdirectory or site. The FortiGate unit will complete the remainder of the address. For example, if the sub site is corpusers, only enter `corpusers`. The final URL that appears is http://172.20.120.230/corpusers. The login port is separately configured by going to *VPN* > *SSL* > *Config*.

When configuring with the security policy, when you create *SSL VPN Authentication Rules*, you can select the specific portal login screen.

Tunnel mode and split tunneling

If you want your web portal to have tunnel mode access, select *Tunnel Mode* when creating a new portal. Enable *Split Tunneling* so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user’s other traffic follows its normal route.

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

Ensure that *Port Forward* is enabled in the *Applications* list.

The Connection tool widget

The *Connection Tool* widget enables a user to connect to resources when isn’t a bookmark. 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 - CLI

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

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

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.

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.*

Create an SSL VPN security policy

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

The SSL VPN security policy specifies:

- the remote address that corresponds to the IP address of the remote user.
- the local protected subnet address that corresponds to the IP address or addresses that remote clients need to access.

  The local protected subnet 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. Select the *Policy Type* as *VPN* and the *Policy Subtype* as *SSL-VPN*.
3. Enter the following information:

Incoming Interface	Select the name of the FortiGate network interface to that connects to the Internet.
Remote Address	Select *all*.
Local Interface	Select the FortiGate network interface that connects to the protected network.
Local Protected Subnet	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*.
SSL Client Certificate Restrictive	Select to allow access only to holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field. See “Strong authentication with security certificates” on page 16.
Cipher Strength	Select the bit level of SSL encryption. The web browser on the remote client must be capable of matching the level that you select.

4. Under *Configure SSL-VPN Authentication Rules*, select *Create New*.

Add a user group to the policy. The New SSL VPN 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.

Group(s)	Select user groups that can connect to the SSL VPN tunnel.
User(s)	Select individual users that can connect to the SSL VPN tunnel.
Schedule	Select always.
SSL-VPN Portal	Select the portal the users connect to.
Custom Login	Select to choose a configured login screen. For more information, see "Custom login screen" on page 21.

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 ALL
        set sslvpn-poprtal <portal_name>
      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. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.

3. Enter the following information and select *OK*.

Incoming Interface	Select the virtual SSL VPN interface, such as *ssl.root.*
Source Address	Select the firewall address you created that represents the IP address range assigned to SSL VPN clients, such as SSL_VPN_tunnel_users.
Outgoing Interface	Select the interface that connects to the protected network.
Destination Address	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.
Service	Select service in the left list and use the right arrow button to move them to the right list. Select the ALL service to allow the user group access to all services.
Action	Select *Accept*.
Enable NAT	Select *Enable NAT.* (Optional)

To configure the tunnel mode security policy - CLI

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

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

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

Routing for tunnel mode

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

To add the tunnel mode route - web-based manager

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

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

To add the tunnel mode route - CLI

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

```
config router static
  edit <id>
    set device ssl.root
    set dst 10.11.254.0/24
    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. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information and select *OK*.

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

To configure the Internet browsing security policy - CLI

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

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

Enabling a connection to an IPsec VPN

You might want to provide your SSL VPN clients access to another network, such as a branch office, that is connected by an IPsec VPN. To do this, you need only to add the appropriate security policy. 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. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information and select *OK*.

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

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

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

```
config firewall policy
  edit 0
    set srcintf ssl.root
    set dstintf toOfficeA
    set srcaddr SSL_tunnel_users
    set dstaddr OfficeAnet
    set action accept
    set nat enable
    set schedule always
    set service ALL
end
```

Policy-based connection

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

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.

3. Enter the following information and select *OK*.

Local Interface	Select the virtual SSL VPN interface, *ssl.root*, for example.
Local Protected Subnet	Select the firewall address that represents the IP address range assigned to SSL VPN clients.
Outgoing VPN Interface	Select the FortiGate network interface that connects to the Internet.
Remote Protected Subnet	Select the address of the IPsec VPN remote protected subnet.
VPN tunnel	Select the Phase 1 configuration name of your IPsec VPN.
Allow traffic to be initiated from the remote site	Enable
NAT inbound	Enable

4. Configure inbound NAT from the CLI:

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

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

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

```
config firewall policy
  edit 0
    set srcintf ssl.root
    set dstintf port1
    set srcaddr SSL_tunnel_users
    set dstaddr OfficeAnet
    set action ipsec
    set schedule always
    set service ALL
    set inbound enable
    set outbound enable
    set natinbound enable
    set vpntunnel 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 Routes* and select *Create New*.

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

To add the tunnel mode route - CLI

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

```
config router static
  edit <id>
    set device ssl.root
    set dst 10.11.254.0/24
    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 443 and users can access the web portal login page using the following default URL:

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

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

To change the SSL VPN port - web-based manager

1. If *Current VDOM* appears at the bottom left of the screen, select *Global* from the list of VDOMs.
2. Go to *VPN* > *SSL* > *Config*.
3. Type an unused port number in *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 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 *SSL VPN login page*.
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.

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 configuration" on page 18.

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

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

To configure host checking - CLI

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

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

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

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

Creating a custom host check list

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

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

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.

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

Windows OS check

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

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

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

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

Configuring cache cleaning

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

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

To enable cache cleaning

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

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. Configure the application control list in the CLI.

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

OS Check is configurable only in the CLI.

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

Adding WINS and DNS services for clients

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

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

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

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

1. Go to *VPN* > *SSL* > *Config*.
2. Select the *Expand Arrow* to display the *Advanced* section.
3. Enter the IP addresses of DNS servers in the *DNS Server* fields as needed.
4. Enter the IP addresses of WINS servers in the *WINS Server* fields as needed.
5. Select *Apply*.

To specify WINS and DNS services for clients - CLI

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

Setting the idle timeout setting

The idle timeout setting controls how long the connection can remain idle before the system forces the remote user to log in again. For security, keep the default value of 300 seconds (5 minutes) or less.

To set the idle timeout - web-based manager

1. Go to *VPN* > *SSL* > *Config*.
2. In the *Idle Timeout* field, enter the timeout value.

   The valid range is from 10 to 28800 seconds.
3. Select *Apply*.

To set the idle timeout - CLI

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

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

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

2. Select *Enable*, and select *VPN activity event*.
3. Select *Apply*.

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”.

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

Monitoring active SSL VPN sessions

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

To monitor SSL VPNs - web-based manager

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

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

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

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 25.

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, 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 443. 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.

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

Tunnel mode client configuration

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

Connection Name	If you have pre-configured the connection settings, select the connection from the list and then select *Connect*. Otherwise, enter the settings in the fields below.
Remote Gateway	Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN.
Username	Enter your user name.
Client Certificate	Use this field if the SSL VPN requires a certificate for authentication. Select the required certificate from the drop-down list. The certificate must be installed in the Internet Explorer certificate store.

Setup examples

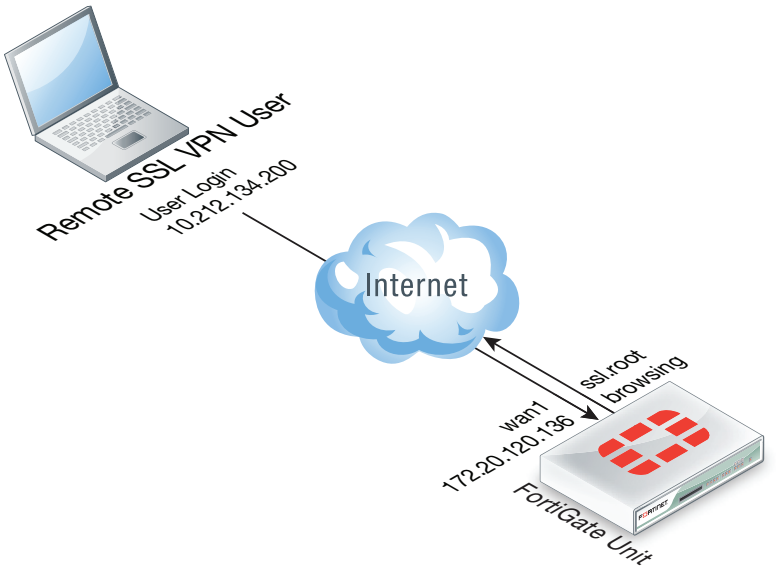
The examples in this chapter demonstrate the basic configurations needed for common connections to the SSL VPN tunnel and portals, applying the steps outlined in the chapter “Basic Configuration” on page 13.

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 *SSLVPN_TUNNEL_ADDR1*.
2. Create the SSL VPN portal to by going to *VPN* > *SSL* > *Portal* and selecting *tunnel-access* in the upper right-hand corner drop-down list box.
3. 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 & Device* > *User* > *User Definition* and select *Create New* to add the user:

User Name	twhite
Password	password

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

Name	SSL Group
Type	Firewall

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

Creating a static route for the remote SSL VPN user

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

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

   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.

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*.
2. Select the *Policy Type* as *VPN* and the *Policy Subtype* as *SSL-VPN*.
3. to add the SSL VPN security policy:

Incoming Interface	wan1
Remote Address	all
Local Interface	ssl.root
Local Protected Subnet	all

4. Select *Create New* for Configure SSL-VPN Authentication Rules and add an authentication rule for the remote user:

Selected User Groups	Tunnel
Selected Services	All
Schedule	always
SSL-VPN Portal	tunnel-access

5. Select *OK*.
6. Select *Create New* to add a security policy that allows remote SSL VPN users to connect to the Internet
7. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.:

Incoming Interface	ssl.root
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

8. Select *OK*.

Results

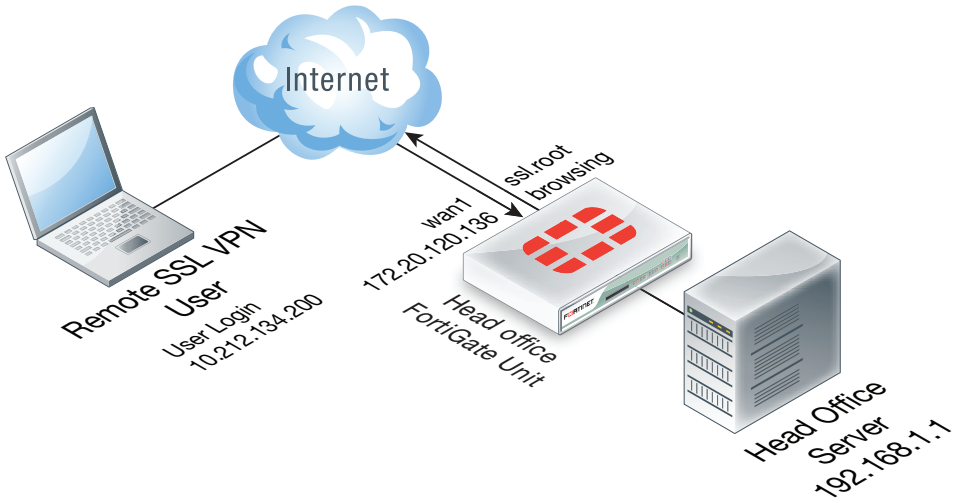
Using FortiClient SSLVPN application, log into the VPN using the address `https://172.20.120.136:443/` and log in as `twhite`. Once connected, you can browse the Internet.

From the FortiGate web-based manager go to *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* > *Addresses* and select *Create New* and add the head office server address:

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

2. Select *OK*.

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to *VPN* > *SSL* > *Config*.
2. *For IP Pools* select *SSLVPN_TUNNEL_ADDR1*.
3. Create the SSL VPN portal to by going to *VPN* > *SSL* > *Portal* and select the plus sign in the upper right of the window.
4. Enter the following:

Name	Connect to head office server
IP Pools	SSLVPN_TUNNEL_ADDR1
Enable Tunnel Mode	Enable
Split Tunneling	Enable

5. Select *OK*.

Creating the SSL VPN user and user group

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

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

User Name	twhite
Password	password

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

Name	Tunnel
Type	Firewall

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

Creating a static route for the remote SSL VPN user

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

1. Go to *Router* > *Static* > *Static* and select *Create New*
2. For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*:

Destination IP/Mask	10.212.134.0/255.255.255.0
Device	ssl.root

3. 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*.
2. Select the *Policy Type* of VPN and the *Policy Subtype* as SSL-VPN.
3. Complete the following:

Incoming Interface	wan1
Remote Address	all
Local Interface	internal
Local Protected Subnet	Head office server

4. Under *Configure SSL-VPN Authentication Rules* select *Create New* to add an authentication rule for the remote user:

Groups(s)	Tunnel
Service	ALL
Schedule	always

5. Select *OK*.

   Add a security policy that allows remote SSL VPN users to connect to the Internet.
6. Select *Create New*.
7. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
8. Complete the following and select *OK*:

Incoming Interface	ssl.root
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Results

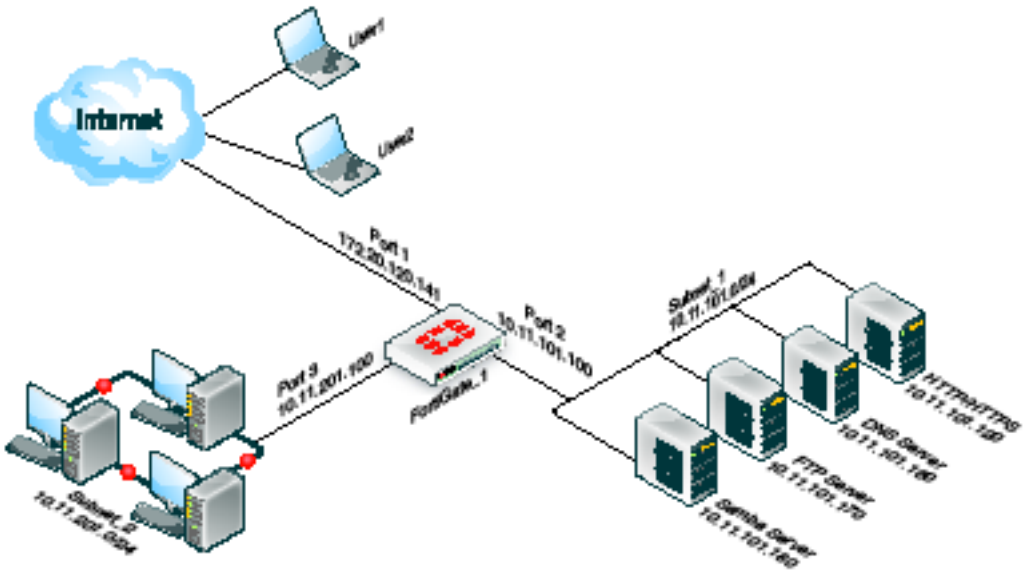
Using the FortiClient SSL VPN application on the remote PC, connect to the VPN using the address `https://172.20.120.136:443/` and log in with the `twhite` user account. Once connected, you can connect to the head office server or browse to web sites on the Internet.

From the web-based manager go to *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 1: 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* > *Addresses.*
2. Select *Create New*, enter the following information, and select *OK*:

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

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

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

Creating the tunnel client range addresses

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

To define tunnel client addresses - web-based manager

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

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

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

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

Creating the web portals

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

To create the portal1 web portal

1. Go to *VPN* > *SSL* > *Portal* and select the plus icon in the upper right corner.
2. Enter `portal1` in the *Name* field.
3. In *Applications*, select all of the application types that the users can access.
4. In *IP Pools*, select *Tunnel_ group1*.
5. Select *OK*.

To create the portal2 web portal

1. Go to *VPN* > *SSL* > *Portal* and select the plus icon in the upper right corner.
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. In *IP Pools*, select *Tunnel_ group2*
5. Select *OK*.

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

Creating the user accounts and user groups

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

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

To create the user groups - web-based manager

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

Name	group1
Type	Firewall

3. From the *Available* list, select *user1* and move it to the *Members* list by selecting the right arrow button.
4. Select *OK*.
5. Repeat steps 2 through 4 to create group2, assigned to portal2, with user2 as its only member.

Creating the security policies

You need to define security policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected networks behind the FortiGate unit. Before you create the security policies, you must define the source and destination addresses to include in the policy. See “Creating the firewall addresses” on page 45.

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* and select *Create New.*
2. Select the *Policy Type* of *VPN* and the *Policy Subtype* as *SSL-VPN*.
3. Enter the following information:

Incoming Interface	port1
Remote Address	All
Local Interface	port2
Local Protected Interface	Subnet_1

4. Under Configure *SSL-VPN Authentication Rules*, select *Create New* and enter the following information:

Group(s)	group1
Schedule	always
Service	ALL
SSL-VPN Portal	portal1

5. Select *OK*, and then select *OK* again.
6. Select *Create New.*
7. Select the *Policy Type* of *VPN* and the *Policy Subtype* as *SSL-VPN*.
8. Enter the following information:

Incoming Interface	port1
Remote Address	All
Local Interface	port3
Local Protected Interface	Subnet_2

9. Under Configure *SSL-VPN Authentication Rules*, select *Create New* and enter the following information:

Group(s)	group2
Schedule	always
Service	ALL
SSL-VPN Portal	portal1

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

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

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

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

4. Select *Create New.*
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

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

Create the static route to tunnel mode clients

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

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

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

   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.

2. Enter the following information and select *OK*.

Destination IP/Mask	`10.11.254.0/24` This IP address range covers both ranges that you assigned to SSL VPN tunnel-mode users. See “Creating the tunnel client range addresses” on page 46.
Device	Select the SSL VPN virtual interface, *ssl.root* for example.

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

U

V

W

X