
# FortiGate
# SSL VPN User Guide
# Version 3.0 MR5

FORTINET

www.fortinet.com

*FortiGate SSL VPN User Guide*
11 September 2007
01-30005-0348-20070911

# Contents

# Introduction

This section introduces you to FortiGate™ Secure Sockets Layer (SSL) VPN technology and provides supplementary information about Fortinet™ publications.

The following topics are included in this section:



## About FortiGate SSL VPN

FortiGate SSL VPN technology makes it safe to do business over the Internet. In addition to encrypting and securing information sent from a web browser to a web server, FortiGate SSL VPN can be used to encrypt most Internet-based traffic.

With the FortiGate unit's built-in SSL VPN capabilities, small home offices, medium-sized businesses, enterprises, and service providers can ensure the confidentiality and integrity of data transmitted over the Internet. The FortiGate unit provides enhanced authentication and restricted access to company network resources and services.

The two modes of SSL VPN operation, supported in NAT/Route mode only, are:

- web-only mode, for thin remote clients equipped with a web browser only
- tunnel mode, for remote computers that run a variety of client and server applications

When the FortiGate unit provides services in web-only mode, a secure web connection between the remote client and the FortiGate unit is established using 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.

Where users have complete administrative rights over their computers and use a variety of applications, tunnel mode allows remote clients to access the local internal network as if they were connected to the network directly. In tunnel mode, a secure SSL connection is established initially for the FortiGate unit to download SSL VPN client software (an ActiveX plugin) to the web browser. After the user installs the SSL VPN client software, they can initiate a VPN tunnel with the FortiGate unit whenever the SSL connection is open.

When the SSL VPN feature is used, all client traffic is encrypted and sent to the SSL VPN. This includes both traffic intended for the private network and Internet traffic that is normally sent unencrypted. Split tunneling 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 bandwith and alleviates bottlenecks.

The mode of operation needed depends on the number and type of applications installed on the remote computer. Access to any application not supported through web-only mode can be supported through tunnel mode. For more information about these modes of operation, see “Configuring a FortiGate SSL VPN” on page 13.

# About this document

This document explains how to configure SSL VPN operation using the web-based manager and contains the following chapters:

- Configuring a FortiGate SSL VPN describes the two modes of operation, recommends a deployment topology, and provides an overview of the associated infrastructure dependencies. The high-level steps for configuring each mode of operation are also included with cross-references to underlying procedures. This chapter also details the basic administrative tasks needed to support the two modes of operation, and describes the additional step-by-step procedures needed to configure each mode.
- Working with the web portal introduces the web portal applications and explains how to work with them. The chapter also explains how to install the ActiveX plugin and initiate a VPN tunnel when tunnel mode is enabled.

## Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:

**Note:** Highlights useful additional information.

**Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

### Typographic conventions

FortiGate documentation uses the following typographical conventions:

| Convention | Example |
|---|---|
| **Keyboard input** | In the Name field, type `admin`. |
| **Code examples** | `config sys global`<br>`  set ips-open enable`<br>`end` |
| **CLI command syntax** | `config firewall policy`<br>`  edit id_integer`<br>`  set http_retry_count <retry_integer>`<br>`  set natip <address_ipv4mask>`<br>`end` |
| **Document names** | *FortiGate SSL VPN User Guide* |
| **File content** | `<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>` |
| **Menu commands** | Go to **VPN > SSL > Config**. |
| **Program output** | `Welcome!` |
| **Variables** | `<group_name>` |

## FortiGate documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*

  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*

  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*

  Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

- *FortiGate CLI Reference*

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*

  Available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*

  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*

  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*

  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*

  Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*

  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*

  Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

# Related documentation

Additional information about Fortinet products is available from the following related documentation.

## FortiManager documentation

- *FortiManager QuickStart Guide*

  Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*

  Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

## FortiClient documentation

- *FortiClient Host Security User Guide*

  Describes how to use FortiClient Host Security software to set up a VPN connection from your computer to remote networks, scan your computer for viruses, and restrict access to your computer and applications by setting up firewall policies.
- *FortiClient Host Security online help*

  Provides information and procedures for using and configuring the FortiClient software.

## FortiMail documentation

- *FortiMail Administration Guide*

  Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Web Mail Online Help*

  Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

## FortiAnalyzer documentation

- *FortiAnalyzer Administration Guide*

  Describes how to install and configure a FortiAnalyzer unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiAnalyzer unit as a NAS server.
- *FortiAnalyzer online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

## Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at http://docs.forticare.com.

## Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

### Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

## Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

# Configuring a FortiGate SSL VPN

This section provides a comparison of SSL and IPSec VPN technology, in addition to an overview of the two modes of SSL VPN operation. The high-level steps for configuring each mode are also included with cross-references to underlying procedures.

The following topics are included in this section:



## Comparison of SSL and IPSec VPN technology

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

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

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

### Legacy versus web-enabled applications

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

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

### Authentication differences

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

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

### Connectivity considerations

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

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

### Relative ease of use

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

### Client software requirements

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

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

### Access control

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

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

### Session failover support

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

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

## SSL VPN modes of operation

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on user name, password, and authentication domain. A successful login determines the access rights of remote users according to user group. The user group settings specify whether the connection will operate in web-only mode (see “Web-only mode” on page 15) or tunnel mode (see “Tunnel mode” on page 16).

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

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

### Web-only mode

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

Support for SSL VPN web-only mode is built into the FortiOS operating system. The feature comprises 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, and RDP.

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.

Configuring the FortiGate unit involves selecting web-only-mode access in the user group settings and enabling the feature through SSL VPN configuration settings. The user group settings determine which server applications can be accessed. SSL encryption is used to ensure traffic confidentiality.

### Web-only mode client requirements

The remote client computer must be equipped with the following software:

- Microsoft Windows 2000/XP/2003/Vista, Linux, or UNIX operating system
- Microsoft Internet Explorer 6.0 (or later), Netscape Navigator 7.0 (or later), or Mozilla Foundation/Firefox 1.2 (or later)
- If Telnet/VNC or RDP are used, Sun Java runtime environment 1.4 (or later), with Java applet access, JavaScript access, and enabled cookie acceptance

**Note:** Web browsers offer different SSL security capabilities. The FortiGate unit offers an SSL version 2 option through the CLI if required to support older browsers. In addition, the FortiGate unit supports a range of cipher suites for negotiating SSL communications with a variety of web browsers. The web browser must at least support a 64-bit cipher length.

## Tunnel mode

Tunnel mode offers remote users the freedom to connect to the internal network using the traditional means of web-based access from laptop computers, as well as from airport kiosks, hotel business centers, and Internet cafés. If the applications on the client computers used by your user community vary greatly, you can deploy a dedicated SSL VPN client to any remote client through its web browser. The SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate unit through an SSL VPN tunnel over the HTTPS link between the web browser and the FortiGate unit. Also available is split tunneling, which ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. This conserves bandwith and alleviates bottlenecks.

In tunnel mode, remote clients connect to FortiGate unit and the web portal login page using Microsoft Internet Explorer or Mozilla Foundation/Firefox. 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. The user can then download the SSL VPN client (an ActiveX or Java plugin) and install it using controls provided through the web portal.

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 selecting tunnel-mode access in the user group settings and enabling the feature through SSL VPN configuration settings. The firewall policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

### Tunnel-mode client requirements

The remote computer must be equipped with the following software:

- Microsoft Windows 2000/XP/2003 (32-bit only)
- Microsoft Internet Explorer 6.0 (or later) with ActiveX enabled, or Mozilla Foundation/Firefox (1.2 or later) with Java Platform enabled

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

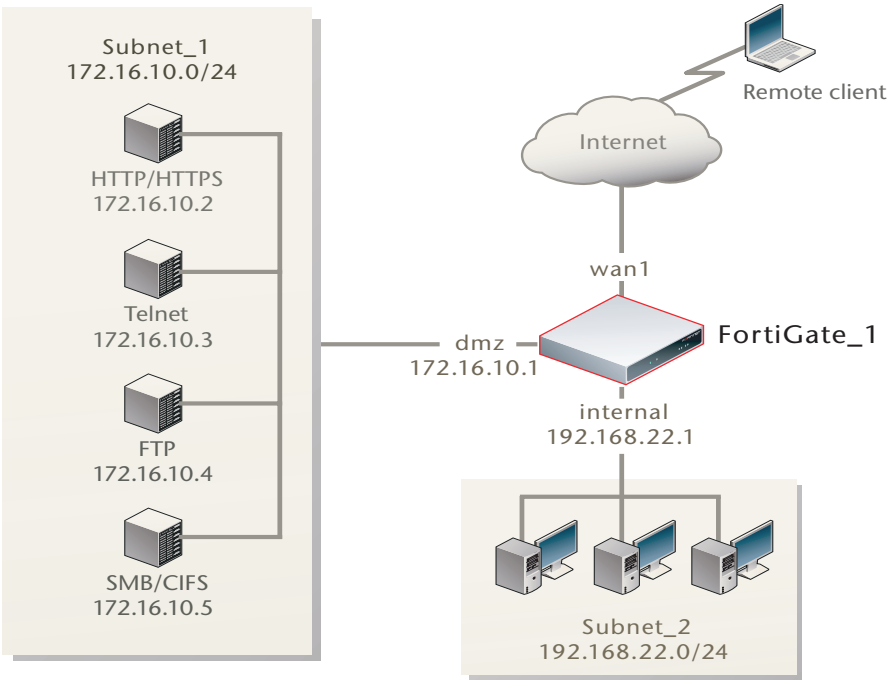
## Topology

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

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

For example, Figure 1 shows a FortiGate gateway (FortiGate_1) to two private networks, Subnet_1 and Subnet_2.

**Figure 1: Example SSL VPN configuration**




To provide remote clients with access to all of the servers on Subnet_1 from the Internet, you would configure FortiGate_1 as follows:

- Create an SSL VPN user group and include the remote users in the user group. When you create the user group, you also specify whether the users may access the web portal in web-only mode or tunnel mode.

- For tunnel-mode users, define the virtual IP addresses that the FortiGate unit is to assign to remote clients when they connect.
- Create a firewall destination IP address of `172.16.10.0/24`.
- Bind the user group to the firewall destination address when you define the firewall policy. The firewall policy identifies which IP packets to encrypt and send through the secure SSL link.

If your user community needs access to Subnet_2, you would create a second firewall destination IP address of `192.168.22.0/24` and create a second firewall policy that binds the associated remote clients to the Subnet_2 destination address.

### Infrastructure requirements

- The FortiGate unit must be operating in NAT/Route mode and have a static public IP address.
- The ISP assigns IP addresses to remote clients before they connect to the FortiGate unit.
- If the remote clients need web-only mode access, see “Web-only mode client requirements” on page 16.
- If the remote clients need tunnel-mode access, see “Tunnel-mode client requirements” on page 17.

## Configuration overview

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

To configure FortiGate SSL VPN technology, you should follow these general steps:

1. Enable SSL VPN connections and set the basic options needed to support SSL VPN configurations. See “Configuring SSL VPN settings” on page 19.
2. To use X.509 security certificates for authentication purposes, load the signed server certificate, CA root certificate, and Certificate Revocation List (CRL) onto the FortiGate unit, and load the personal/group certificates onto the remote clients. For more information, see the *FortiGate Certificate Management User Guide*.
3. Create one FortiGate user account for each remote client, and assign the users to SSL VPN type user groups. See “Configuring user accounts and SSL VPN user groups” on page 25.
4. Configure the firewall policy and the remaining parameters needed to support the required mode of operation:
   - For web-only mode operation, see “Configuring Web-only firewall policies” on page 29.
   - For tunnel-mode operation, see “Configuring tunnel-mode firewall policies” on page 30.

5 Define SSL VPN event-logging parameters. See “Configuring SSL VPN event-logging” on page 33.

6 You can also monitor active SSL VPN sessions. See “Monitoring active SSL VPN sessions” on page 34.

# Configuring SSL VPN settings

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

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

Refer to the *FortiGate Installation Guide* and *FortiGate Administration Guide* to change the password, configure the interfaces of the FortiGate unit, and assign basic operating parameters, including a default gateway.

There are basic administrative tasks common to all modes of operation that must be completed first, regardless of the connection mode you select.

The **VPN > SSL > Config** page contains basic SSL VPN settings including idle-timeout values and SSL encryption preferences for compatibility with various web browsers. You may also optionally enable authentication through X.509 security certificates (for more information about security certificates, see the *FortiGate Certificate Management User Guide*).

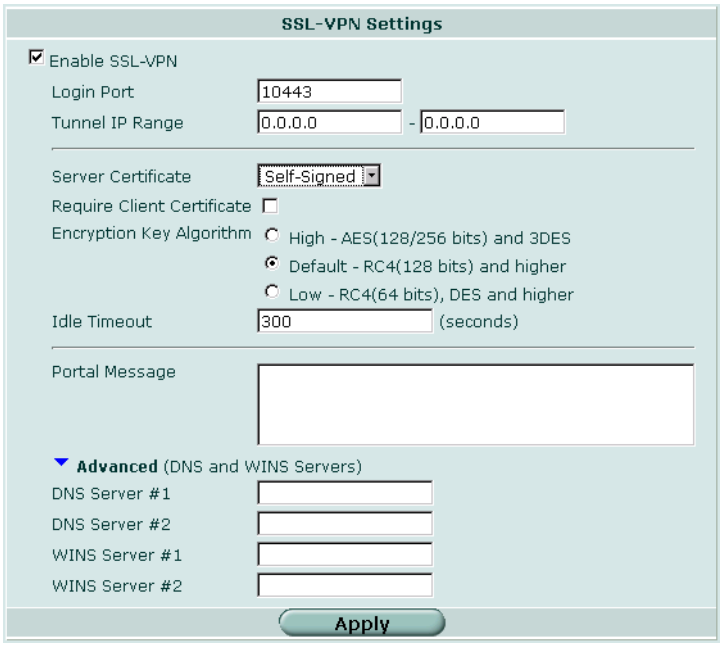
In addition to setting these preferences on the **VPN > SSL > Config** page, you may choose to modify the following system settings:

- The FortiGate unit redirects web browsers to the web portal home page after the remote client has been authenticated and the user has logged in successfully. As an option, you can display a second HTML page in a popup window for all members of a user group. For more information, see “Redirecting a user group to a popup window” on page 23.
- You can customize the look of the web portal login page through replacement messages. For more information, see “Customizing the web portal login page” on page 24.

## Enabling SSL VPN connections and editing SSL VPN settings

To enable SSL VPN connections and configure or edit SSL VPN settings, go to **VPN > SSL > Config** and select Enable SSL-VPN. The FortiGate unit does not accept web-only mode or tunnel-mode connections while SSL VPN operation is disabled.

**Figure 2: Edit SSL VPN settings**




**Enable SSL VPN** — Select to enable SSL VPN connections.

**Login Port** — Enter a different HTTPS port number for remote client web browsers to connect to the FortiGate unit, if required. The default port number is 10443. See Specifying a port number for web portal connections.

**Tunnel IP Range** — Specify the range of IP addresses reserved for tunnel-mode SSL VPN clients. Type the starting and ending address that defines the range of reserved IP addresses. See Specifying an IP address range for tunnel-mode clients.

**Server Certificate** — Select the signed server certificate to use for authentication purposes. If you leave the default setting (Self-Signed), the FortiGate unit offers its factory installed (self-signed) certificate from Fortinet to remote clients when they connect. See Enabling strong authentication through security certificates.

**Require Client Certificate** — If you want to enable the use of group certificates for authenticating remote clients, select the option. Afterward, when the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process.

**Encryption Key Algorithm** — Select the algorithm for creating a secure SSL connection between the remote client web browser and the FortiGate unit.
See Specifying the cipher suite for SSL negotiations.

- **Default - RC4(128 bits) and higher** — If the web browser on the remote client is capable of matching a 128-bit or greater cipher suite, select this option.
- **High - AES(128/256 bits) and 3DES** — If the web browser on the remote client is capable of matching a high level of SSL encryption, select this option to enable cipher suites that use more than 128 bits to encrypt data.
- **Low - RC4(64 bits), DES and higher** — If you are not sure which level of SSL encryption the remote client web browser supports, select this option to enable a 64-bit or greater cipher suite.

| | |
|---|---|
| **Idle Timeout** | Type the period of time (in seconds) to control how long the connection can remain idle before the system forces the user to log in again. The range is from 10 to 28800 seconds. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up. See Setting the idle timeout setting. |
| **Portal Message** | If you want to display a custom caption at the top of the web portal home page, type the message. See Adding a custom caption to the web portal home page. |

**Advanced (DNS and WINS Servers)** See Adding WINS and DNS services for clients.

| | |
|---|---|
| **DNS Server #1**<br>**DNS Server #2** | Enter up to two DNS Servers to be provided for the use of clients. |
| **WINS Server #1**<br>**WINS Server #2** | Enter up to two WINS Servers to be provided for the use of clients. |

When you finish making your selections, select Apply.

**Note:** The Tunnel IP Range fields are used to configure tunnel-mode access only. If you are configuring web-only mode operation, leave `0.0.0.0` values in the Tunnel IP Range fields. If you are configuring tunnel-mode operation, see "Specifying an IP address range for tunnel-mode clients" on page 21. For information about enabling certificate-based authentication through the Server Certificate and Require Client Certificate options, refer to the *FortiGate Certificate Management User Guide*.

## Specifying a port number for web portal connections

You can optionally specify a different TCP port number for users to access the web portal login page through the HTTPS link. By default, the port number is 10443 and users can access the web portal login page using the following default URL:

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

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

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

1. Go to **VPN > SSL > Config**.
2. In the Login Port field, type an unused port number.
3. Select Apply.

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

The Tunnel IP Range fields on the **VPN > SSL > Config** page enable you to reserve a range of IP addresses for remote SSL VPN clients. After the FortiGate unit authenticates a request for a tunnel-mode connection, the SSL VPN client connects to the FortiGate unit and is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the SSL VPN client.

**Note:** Use the Tunnel IP Range fields on the `VPN > SSL > Config` page to reserve a range of global IP addresses. If you configure a user group and define Restrict tunnel IP range for this group, the group range is used in the SSL VPN configuration. If you do not define a range of global IP addresses, you must define a group range. If you define both IP address ranges, the group level range is applied to the configuration. See To create a user group for more information about the group IP address range configuration.

**Caution:** Take care to prevent overlapping IP addresses. Do not assign 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 reserve a range of IP addresses for tunnel-mode clients**

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

2 In the Tunnel IP Range fields, type the starting and ending IP addresses (for example, `10.254.254.80` to `10.254.254.100`).

3 Make a note of this address range for future reference. You will need this information when you define the firewall source IP address for tunnel-mode connections.

4 Select Apply.

## Enabling strong authentication through security certificates

The FortiGate unit supports strong (two-factor) authentication through X.509 security certificates (version 1 or 3). Strong authentication can be configured for SSL VPN user groups by selecting the Server Certificate and Require Client Certificate options on the **VPN > SSL > Config** page. However, you must first ensure that the required certificates have been installed.

To generate certificate requests, install signed certificates, import CA root certificates and certificate revocation lists, and back up and/or restore installed certificates and private keys, refer to the *FortiGate Certificate Management User Guide*.

## Specifying the cipher suite for SSL negotiations

The FortiGate unit supports a range of cryptographic cipher suites to match the capabilities of various web browsers. The web browser and the FortiGate unit negotiate a cipher suite before any information (for example, a user name and password) is transmitted over the SSL link.

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

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

- If the web browser on the remote client is capable of matching a 128-bit or greater cipher suite, select Default - RC4(128 bits) and higher.
- If the web browser on the remote client is capable of matching a high level of SSL encryption, select High - AES(128/256 bits) and 3DES. This option enables cipher suites that use more than 128 bits to encrypt data.
- If you are not sure which level of SSL encryption the remote client web browser supports, select Low - RC4(64 bits), DES and higher. The web browser must at least support a 64-bit cipher length.

3 Select Apply.

## 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. To improve security, keep the default value of 300 seconds.

1. Go to **VPN > SSL > Config**.
2. In the Idle Timeout field, type an integer value. The valid range is from 10 to 28800 seconds.
3. Select Apply.

## Setting the client authentication timeout setting

The client authentication timeout setting controls how long an authenticated connection will remain connected. When this time expires, the system forces the remote client to authenticate again.

**Note:** The default value is 1500 seconds. You can only modify this timeout value in the CLI.

For example, to change the authentication timeout to 1800 seconds, enter the following commands:

```
config vpn ssl settings
  set auth-timeout 1800
  end
```

## Adding a custom caption to the web portal home page

You can add a custom caption (maximum 31 characters) to the top of the web portal home page.

**To add a custom caption**

1. Go to **VPN > SSL > Config**.
2. In the Portal Message field, type the caption.
3. Select Apply.

## Adding WINS and DNS services for clients

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

1. Go to **VPN > SSL > Config**.
2. Select the blue triangle to open the Advanced section.
3. Enter the IP addresses of one or two DNS Servers to be provided for the use of clients.
4. Enter the IP addresses of one or two WINS Servers to be provided for the use of clients.

## Redirecting a user group to a popup window

The FortiGate unit redirects web browsers to the web portal home page after the remote client has been authenticated and the user has logged in successfully.

As an option, you can have the FortiGate unit display a second HTML page in a popup window when the client web browser is redirected to the web portal home page. To support this feature, the level of security settings associated with the Internet zone in the web browser must be set to permit popup windows.

The following procedure assumes that SSL VPN user groups have been defined (see "Configuring user accounts and SSL VPN user groups" on page 25). A different popup window can be specified per user group.

**To display a custom popup window for a user group**

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

2 Select the Edit icon in the row that corresponds to the SSL VPN user group.

3 Expand SSL-VPN User Group Options.

4 In the Redirect URL field, type the URL of the web page that you want to display in the popup window.

5 Select OK.

## Customizing the web portal login page

The HTML code making up the web portal login page can be edited. Before you begin, copy the default text to a separate text file for safe-keeping. Afterward, if editing produces unexpected results, you can restore the text to the original version.

**To edit the HTML code**

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

2 Expand the SSL VPN row and select the Edit icon that corresponds to the SSL VPN login message.


3 Edit the HTML text, subject to the restrictions given in the *FortiGate Administration Guide* (see "Changing the authentication login page" in the "System Config" chapter).

Select OK.

# Configuring user accounts and SSL VPN user groups

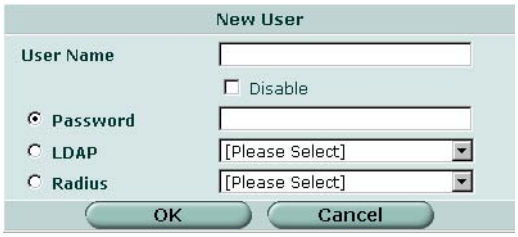
Remote users must be authenticated before they can request services and/or access network resources through the web portal. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS and LDAP to authenticate remote clients.

You can choose to use a plain text password for authentication through the FortiGate unit (Local domain), forward authentication requests to an external RADIUS or LDAP server, or utilize PKI certificate authentication. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the RADIUS or LDAP server. In the case of certificate authentication, you must install the required certificates.

The following procedures explain how to create a user account and user group in the Local domain. For information about how to create RADIUS, LDAP or PKI user accounts, refer to the "User" chapter of the *FortiGate Administration Guide*. For information about certificate authentication, see the *FortiGate Certificate Management User Guide.*

### To create a user account in the Local domain

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



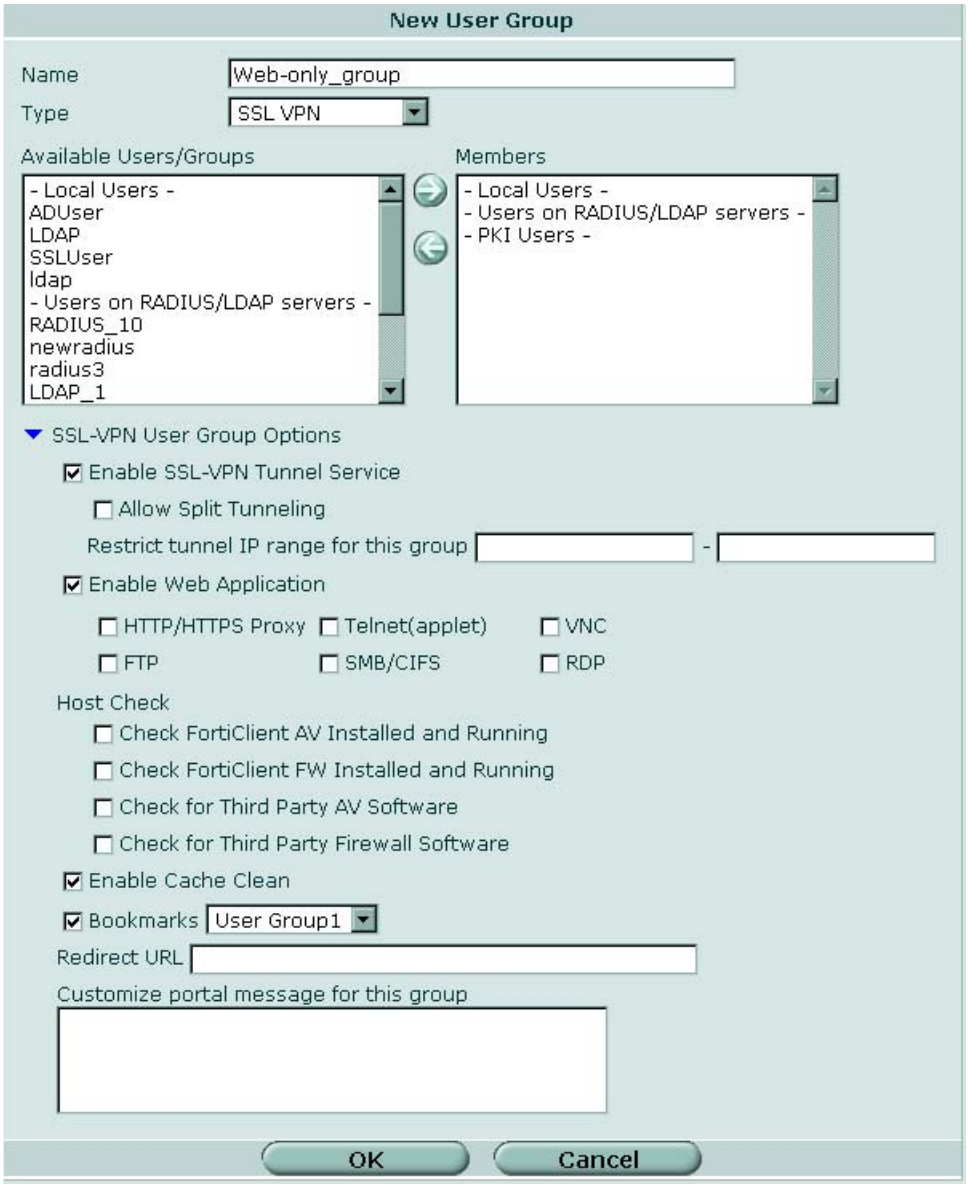

| | |
|---|---|
| **User Name** | Type or edit the remote user name (for example, `User_1`). |
| **Disable** | Select Disable to prevent this user from authenticating. |
| **Password** | Select Password to authenticate this user using a password stored on the FortiGate unit.<br>Type or edit the password to be associated with the user account. The password should be at least six characters long. |
| **LDAP** | Select LDAP to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the drop-down list. |
| **RADIUS** | Select RADIUS to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the drop-down list. |

2 Select OK.

3 Repeat this procedure for each remote user.

**To create a user group**

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




2 In the Name field, type a name for the group (for example, `Web-only_group`).

3 From the Type drop-down list, select SSL VPN.

4 One at a time, select user names from the Available Users/Groups list, and select the right-pointing arrow to move them to the Members list.

5 Select the blue triangle to expand the SSL-VPN User Group Options.

6 Select Enable SSL-VPN Tunnel Service If the remote clients associated with the user group need to establish an SSL VPN tunnel with the FortiGate unit.

**Note:** If a user has been configured to use tunnel-mode only, when they log in, the tunnel is brought up automatically.

7 To activate the split tunnel feature, select Enable Split Tunneling. Split tunneling 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.

8 To override the Tunnel IP range defined in **VPN > SSL > Config,** enter the starting and ending IP address range for this group in the Restrict tunnel IP range for this group fields.

**Note:** If you configure a user group and define Restrict tunnel IP range for this group, the group range is used in the SSL VPN configuration. If you do not define a range of global IP addresses, you must define a group range. If you define both IP address ranges, the group level range is applied to the configuration. See To reserve a range of IP addresses for tunnel-mode clients for more information about the global IP address range configuration.

9 If the user group requires web-only-mode access, select Enable Web Application and then select the web applications and/or network file services that the user group needs. The corresponding server applications can be running on the network behind the FortiGate unit or accessed remotely through the Internet.

10 To enable client-integrity checking options, select from the following:

- Check FortiClient AV Installed and Running
- Check FortiClient FW Installed and Running
- Check for Third Party AV Software
- Check for Third Party Firewall Software

The client-integrity checking options determine whether the FortiClient™ Host Security application or other antivirus/firewall applications are running on the client computer before a tunnel is established. If there are no applications installed and enabled on the client computer, the connection is refused. Table 1 lists the products supported for clients who have Windows XP SP2. All other systems must have Norton (Symantec) AntiVirus or McAfee VirusScan software installed and enabled.

**Table 1: AV/Firewall supported product detection**

| Product | AV | Firewall |
|---|---|---|
| **Norton Internet Security 2006** | Y | Y |
| **Trend Micro PC-cillin** | Y | Y |
| **McAfee** | Y | Y |
| **Sophos Anti-Virus** | Y | N |
| **Panda Platinum 2006 Internet Security** | Y | Y |
| **F-Secure** | Y | Y |
| **Secure Resolutions** | Y | Y |
| **Cat Computer Services** | Y | Y |
| **AhnLab** | Y | Y |
| **Kaspersky** | Y | Y |
| **ZoneAlarm** | Y | Y |

11 To enable the FortiGate unit to remove residual information from the remote client computer (for example, from the web browser cache) just before the SSL VPN session ends, select Enable Cache Clean. When this feature is enabled, if the client's browser cannot install and run the cache cleaner, the user is not allowed to access the SSL-VPN portal.

12 To allow the SSL VPN user group to use a pre-configured bookmark group, enable Bookmarks and select the bookmark group from the drop-down list.

13 To have the FortiGate unit display a second HTML page in a popup window when the web portal home page is displayed, type the URL of the web page into the Redirect URL field.

14 To display a custom web portal home page caption for this group, enter the message in the Customize portal message for this group field.

**Note**: This custom message overrides the portal message configured in **VPN > SSL > Config**.

15 Select OK.

# Configuring firewall policies

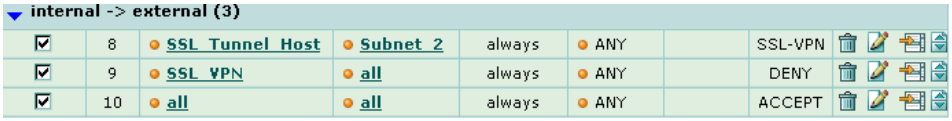
This section contains the procedures needed to configure firewall policies for web-only mode operation and tunnel-mode operation. These procedures assume that you have already completed the procedures outlined in "Configuring user accounts and SSL VPN user groups" on page 25.

A firewall policy specifies the originating (source) IP address of a packet and the destination address defines the IP address of the intended recipient or network.

In general, configuring a firewall policy involves:

- specifying the IP source and destination addresses
- specifying the level of SSL encryption to use and the authentication method
- binding the user group to the firewall policy

**Note:** In tunnel mode, it is necessary to create a DENY firewall policy that immediately follows the SSL VPN policy. If this policy is not created, SSL VPN tunnels will use other ACCEPT firewall policies. See the configuration below:




The following topics are included in this section:

- Configuring firewall addresses
- Configuring tunnel-mode firewall policies
- Configuring SSL VPN event-logging
- Monitoring active SSL VPN sessions

## Configuring firewall addresses

Configuring the firewall addresses for web-only and tunnel mode connections involves specifying the IP source/host and destination addresses:

Web-only mode:

- For the source address, select the predefined address “all” in the firewall encryption policy to refer to web-only mode clients.
- The destination address corresponds to the IP address or addresses that remote clients need to access. The destination address may correspond to an entire private network (behind the FortiGate unit), a range of private IP addresses, or the private IP address of a server or host.

Tunnel mode:

- The source address corresponds to the range of IP addresses that can be connected to the FortiGate unit. This address is used to restrict who can access the FortiGate unit.
- The destination address corresponds to the IP address or addresses that remote clients need to access. The destination address may correspond to an entire private network (behind the FortiGate unit), a range of private IP addresses, or the private IP address of a server or host.

## Configuring Web-only firewall policies

### To specify the destination IP address

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

2 In the Address Name field, type a name that represents the local network, server(s), or host(s) to which IP packets may be delivered (for example, `Subnet_1`).

3 From the Type list, select Subnet/IP Range.

4 In the Subnet/IP Range field, type the corresponding IP address and subnet mask (for example, `172.16.10.0/24`).

**Note:** To provide access to a single host or server, you would type an IP address like `172.16.10.2/32`. To provide access to two servers having contiguous IP addresses, you would type an IP address range like `172.16.10.[4-5]`.

5 Select OK.

### To define the firewall policy for web-only mode connections

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

2 Enter these settings in particular:

| | |
|---|---|
| **Source** | Interface/Zone<br>Select the FortiGate interface that accepts connections from remote users.<br>Address Name<br>Select `all`. |
| **Destination** | Interface/Zone<br>Select the FortiGate interface to the local private network (for example, `dmz`).<br>Address Name<br>Select the IP destination address that you defined previously (for example, `Subnet_1`). |
| **Service** | Select ANY. |
| **Action** | Select SSL-VPN. |

| | |
|---|---|
| **SSL Client Certificate Restrictive** | Select to allow traffic generated by holders of a (shared) group certificate, for example, a user group containing PKI peers/users. 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 list. |
| **Cipher Strength** | Select one of the following options to determine the level of SSL encryption to use. The web browser on the remote client must be capable of matching the level that you select:<br>• To use any cipher suite, select Any.<br>• To use a 164-bit or greater cipher suite, select High >= 164.<br>• To use a 128-bit or greater cipher suite, select Medium >= 128. |
| **User Authentication Method** | Select one of the following options to bind user groups to authentication methods:<br>• If the user group contains only local users, select Local.<br>• If the remote clients will be authenticated by an external RADIUS server, select Radius.<br>• If the remote clients will be authenticated by an external LDAP server, select LDAP.<br>• If the user group contains Local, RADIUS, and LDAP users, select Any to enable all of the authentication methods. Local is attempted first, then RADIUS, then LDAP. |
| **Available Groups** | Select the name of the user group requiring SSL VPN access, and then select the right-pointing arrow. Do not select more than one user group unless all members of the selected user groups have identical access requirements. |

3 Select OK.

4 If the user group requires access to another server or network, create the IP destination address (see “To specify the destination IP address” on page 29) and repeat this procedure to create the required firewall policy.

5 Create additional IP destination addresses and firewall policies if required for each additional user group.

## Configuring tunnel-mode firewall policies

Follow the procedures in this section to complete a tunnel-mode configuration. These procedures assume that you have already completed the procedures found in “Configuring user accounts and SSL VPN user groups” on page 25.

When a remote client initiates a connection to the FortiGate unit, the FortiGate unit authenticates the client and determines which mode of operation is in effect for the user. When tunnel mode is enabled, the user can access the server applications and network services on the internal network if required and/or download and install an ActiveX plugin from the web portal. The ActiveX control provides SSL VPN client software.

**Note:** On the web browser, ensure that the security settings associated with the Internet zone permit ActiveX controls to be downloaded and run.

After the user adds the ActiveX plugin to the web browser on the remote client, the user can start the SSL VPN client software to initiate an SSL VPN tunnel with the FortiGate unit. The FortiGate unit establishes the tunnel with the SSL client and assigns the client a virtual IP address. Afterward, the SSL client uses the assigned virtual IP address as its source address for the duration of the session.

To configure the FortiGate unit to support tunnel-mode access, you perform the following configuration tasks on the FortiGate unit:

- Specify the range of IP addresses that can be assigned to SSL VPN clients when they establish tunnels with the FortiGate unit. See "Specifying an IP address range for tunnel-mode clients" on page 21.
- Define a firewall policy to support tunnel-mode operations.

A firewall policy specifies the originating (source) IP address of a packet and the destination address defines the IP address of the intended recipient or network. In this case, the source address corresponds to the range of IP addresses permitted to connect to the FortiGate unit, and the destination address corresponds to the IP address(es) of the host(s), server(s), or network behind the FortiGate unit.

Configuring the firewall policy involves:

- specifying the source and destination IP addresses:
  - The source address corresponds to the range of IP addresses that can be connected to the FortiGate unit.
  - The destination address 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.
- specifying the level of SSL encryption to use and the authentication method
- binding the user group to the firewall policy

**Note:** If your destination address, SSL encryption, and user group are the same as for your web-only mode connection, you do not need to create a firewall policy for tunnel mode. The FortiGate unit uses the web-only mode policy settings except for the source address range, which it obtains from the tunnel IP range settings.

### To specify the source IP address

1. Go to **Firewall > Address** and select Create New.
2. In the Address Name field, type a name that represents the IP addresses permitted to set up SSL VPN connection (for example, `SSL_Tunnel_Host`).
3. From the Type list, select Subnet/IP Range.
4. In the Subnet/IP Range field, type the corresponding IP address and subnet mask (for example, `172.16.10.0/24`). Enter 0.0.0.0/0.0.0.0 to indicate 'all'.

**Note:** To provide access to a single host or server, you would type an IP address like `172.16.10.2/32`. To provide access to two servers having contiguous IP addresses, you would type an IP address range like `172.16.10.[4-5]`.

5. In the Interface field, select the interface to the internal (private) network.
6. Select OK.

### To specify the destination IP address

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

2 In the Address Name field, type a name that represents the local network, server(s), or host(s) to which IP packets may be delivered (for example, `Subnet_2`).

3 In the Subnet/IP Range field, type the corresponding IP address (for example, `192.168.22.0/24` for a subnet, or `192.168.22.2/32` for a server or host), or IP address range (`192.168.22.[10-25]`).

4 In the Interface field, select the interface to the external (public) network.

5 Select OK.

### To define the firewall policy for tunnel-mode operations

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

2 Enter these settings:

| | |
|---|---|
| **Source** | Interface/Zone<br>Select the FortiGate interface that accepts connections from remote users (for example, `external`).<br>Address Name<br>Select the name that corresponds to the range of IP addresses that you reserved for SSL VPN clients (for example, `SSL_Tunnel_clients`). |
| **Destination** | Interface/Zone<br>Select the FortiGate interface to the local private network (for example, `internal`).<br>Address Name<br>Select the IP destination address that you defined previously for the host(s), server(s), or network behind the FortiGate unit (for example, `Subnet_2`). |
| **Service** | Select ANY. |
| **Action** | Select SSL-VPN. |
| **SSL Client Certificate Restrictive** | Select to allow traffic generated by holders of a (shared) group certificate, for example, a user group containing PKI peers/users. 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. |
| **Cipher Strength** | Select one of the following options to determine the level of SSL encryption to use. The web browser on the remote client must be capable of matching the level that you select:<br>• To use any cipher suite, select Any.<br>• To use a 164-bit or greater cipher suite, select High >= 164.<br>• To use a 128-bit or greater cipher suite, select Medium >= 128. |
| **User Authentication Method** | Select one of the following options to bind user groups to authentication methods:<br>• If the user group contains only local users, select Local.<br>• If the remote clients will be authenticated by an external RADIUS server, select Radius.<br>• If the remote clients will be authenticated by an external LDAP server, select LDAP.<br>• If the user group contains Local, RADIUS, and LDAP users, select Any to enable all of the authentication methods. Local is attempted first, then RADIUS, then LDAP. |
| **Available Groups** | Select the name of the user group requiring SSL VPN access, and then select the right-pointing arrow. Do not select more than one user group unless all members of the selected user groups have identical access requirements. |

3 Select OK.

**Note:** If you apply a protection profile in a SSL VPN firewall policy, it will only apply to tunnel-mode operations.

4 If the user group requires access to another server or network, create the IP destination address (see "To specify the destination IP address" on page 29) and repeat this procedure to create the required firewall policy.

5 Create additional IP destination addresses and firewall policies if required for each additional user group.

# Configuring SSL VPN event-logging

You can configure the FortiGate unit to log SSL VPN events. For information about how to interpret log messages, see the *FortiGate Log Message Reference*.

**To log SSL VPN events**

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

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

- a FortiAnalyzer unit
- the FortiGate system memory
- a remote computer running a syslog server

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

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

4 If logs will be written to system memory, from the Log Level list, select Information. For more information, see the "Log & Report" chapter of the *FortiGate Administration Guide*.

5 Select Apply.

**To filter SSL VPN events**

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

2 Select Enable, and then select one or more of the following options:

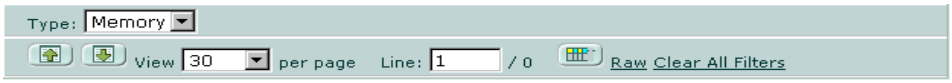
- SSL VPN user authentication event
- SSL VPN administration event
- SSL VPN session event

3 Select Apply.

**To view SSL VPN event logs**

1 Go to **Log&Report > Log Access**.

2 If the option is available from the Type list, select the log file from disk or memory.



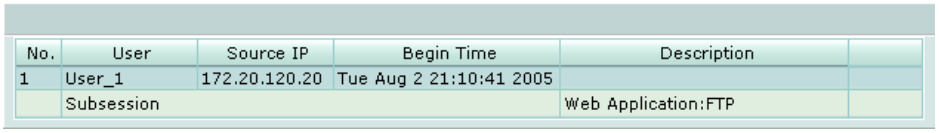

You can modify the settings in the top row to meet your requirements. Log messages are displayed beneath the top row.

# Monitoring active SSL VPN sessions

You can display a list of all active SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time that the connection was made. The list also identifies which services are being provided (see Figure 3 on page 34).

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

**Figure 3: Monitor list: Web-only mode connections**



| No. | User | Source IP | Begin Time | Description |
|---|---|---|---|---|
| 1 | User_1 | 172.20.120.20 | Tue Aug 2 21:10:41 2005 | |
| | Subsession | | | Web Application:FTP |

**No.** The identifier of the connection.

**User** The user names of all connected remote users.

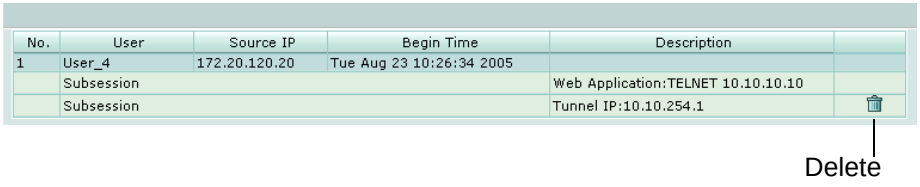
**Source IP** The IP addresses of the host devices connected to the FortiGate unit.

**Begin Time** The starting time of each connection.

**Description** Information about which services are being provided.

When a tunnel-mode user is connected, the Description field displays the IP address that the FortiGate unit assigned to the remote host (see Figure 4 on page 34).

**Figure 4: Monitor list: Tunnel-mode connection**




| No. | User | Source IP | Begin Time | Description |
|---|---|---|---|---|
| 1 | User_4 | 172.20.120.20 | Tue Aug 23 10:26:34 2005 | |
| | Subsession | | | Web Application:TELNET 10.10.10.10 |
| | Subsession | | | Tunnel IP:10.10.254.1 |

If required, you can end a session/connection by selecting the Delete button in the row that corresponds to the connection.

# Configuring SSL VPN bookmarks and bookmark groups

If you create a user account that permits web-only mode access, you can create hyperlinks to frequently accessed server applications that the user can use to start any session from the home page through the hyperlinks. The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the Bookmarks list. The bookmarks are available when the user starts an active SSL VPN session.

## Viewing the SSL VPN bookmark list

You can display a list of all existing SSL VPN bookmarks created using the FortiGate unit. The list details the name of the bookmark, type of bookmark, and the link details.

To view the list of predefined SSL VPN bookmarks, go to **VPN > SSL > Bookmark**.

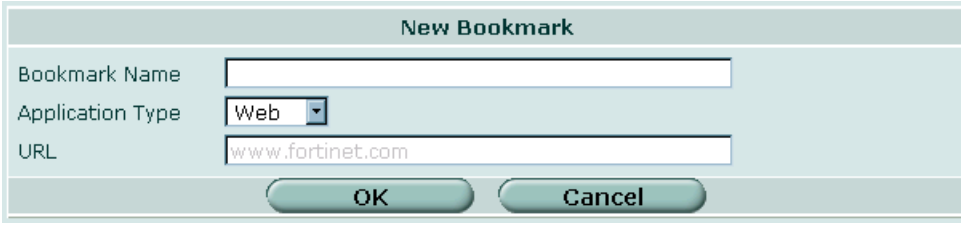
**Figure 5: Bookmark list**


| | |
|---|---|
| **Bookmark Name** | The type/names of links to remote server applications and network services. |
| **Link** | The URL, host, or folder of the bookmark link. |
| **Delete and Edit icons** | Delete or edit an entry in the list. |

## Configuring SSL VPN bookmarks

Go to **VPN > SSL > Bookmark** and select Create New to create hyperlinks to frequently accessed server applications.

**Figure 6: Create New Bookmark**



**Bookmark Name** Type the text to display in the hyperlink. The name is displayed in the Bookmarks list.

**Application Type** Select the abbreviated name of the server application or network service from the drop-down list:

- Web
- Telnet
- FTP
- SMB/CIFS
- VNC
- RDP

**URL/Host/Folder** Type the information that the FortiGate unit needs to forward client requests to the correct server application or network service:

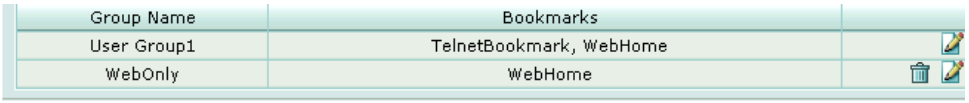
- If the application type is Web, type the URL of the web server (for example, `www.fortinet.com`).
- If the application type is Telnet, type the IP address of the telnet host (for example, `10.10.10.10`).
- If the application type is FTP, type the IP address of the FTP host as a root directory/folder (for example, `//server/folder/`).
- If the application type is SMB/CIFS, type the IP address of the SMB host and the root directory/folder associated with your account (for example, `//server/folder/`).
- If the application type is VNC, type the IP address of the VNC host (for example, `10.10.10.10`).
- If the application type is RDP, type the IP address of the RDP host (for example, `10.10.10.10`).

## Viewing the SSL VPN Bookmark Groups list

You can create a group of specific bookmarks that can be included in the configuration of an SSL VPN user group.

To view a list of bookmark groups, go to **VPN > SSL > Bookmark Group**.

**Figure 7: Bookmark Group list**




**Group Name** Name of bookmark group

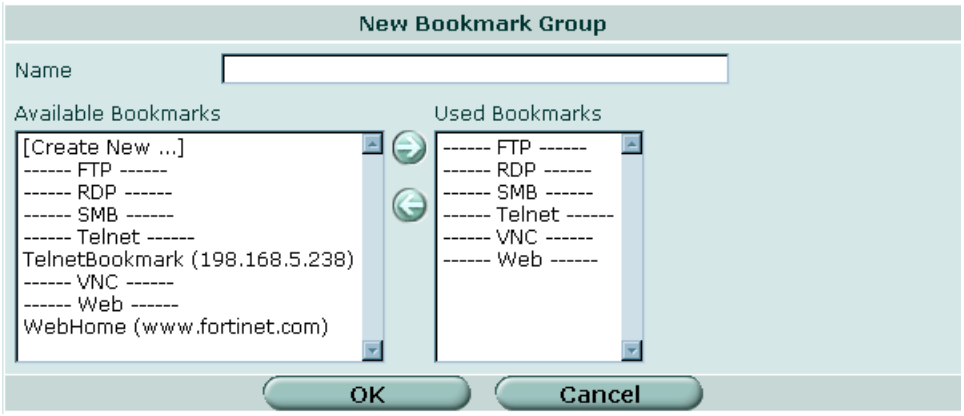
**Bookmarks** List of bookmarks that are components of the bookmark group in Group Name.

**Delete and Edit icons** Delete or edit an entry in the list.

## Configuring SSL VPN bookmark groups

Go to **VPN > SSL > Bookmark Group** and select Create New to create a group of selected bookmarks.

**Figure 8: Create New Bookmark Group**




| | |
|---|---|
| **Name** | Type the name of the bookmark group. The name is displayed in the Bookmark Group list, and is a selection in the Bookmarks list in an SSL VPN user group. |
| **Available Bookmarks** | The list of bookmarks available for inclusion in the bookmark group. Lists bookmarks under appropriate category (FTP, RDP, SMB, Telnet, VNC, or Web). |
| **Used Bookmarks** | The list of bookmarks that belong to the bookmark group. |
| **Right arrow button** | Add a bookmark to the Used Bookmarks list.<br>Select a bookmark name in the Available Bookmarks list and select the right arrow button to move it to the Used Bookmarks list. |
| **Left arrow button** | Remove a bookmark from the Used Bookmarks list.<br>Select a bookmark in the Used Bookmarks list and select the left arrow button to move it to the Available Bookmarks list. |
| **Create New...** | Select to create a new bookmark for inclusion in the Available Bookmarks list. |

## Assigning SSL VPN bookmark groups to SSL VPN users

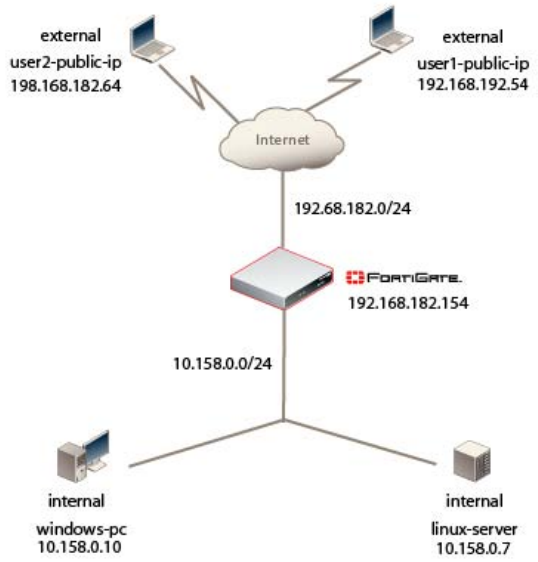
To assign a bookmark group to a user group, go to **User > User Group**, and select/create a SSL VPN user group to assign the bookmark group to. Expand the SSL-VPN User Group Options, enable Bookmarks and select a bookmark group from the drop-down list. When you assign a bookmark group to a SSL VPN user group, all the bookmarks included in the group are available to the SSL VPN users in the selected SSL VPN user group.

**Figure 9: Assigning a bookmark group to a user**

# Granting unique access permissions for SSL VPN tunnel user groups

For situations where there is a requirement for more than one user to be permitted tunnel mode access, the key is to split the tunnel IP range into sub-IP ranges, where each user group (with the user as a member) is assigned a dedicated IP range (with no overlap) and therefore can have different access permissions.

**Figure 10: SSL VPN configuration for unique access permissions**




## Sample configuration for unique access permissions with tunnel mode user groups

In this sample configuration, there are two user groups, each one with a dedicated IP address range.

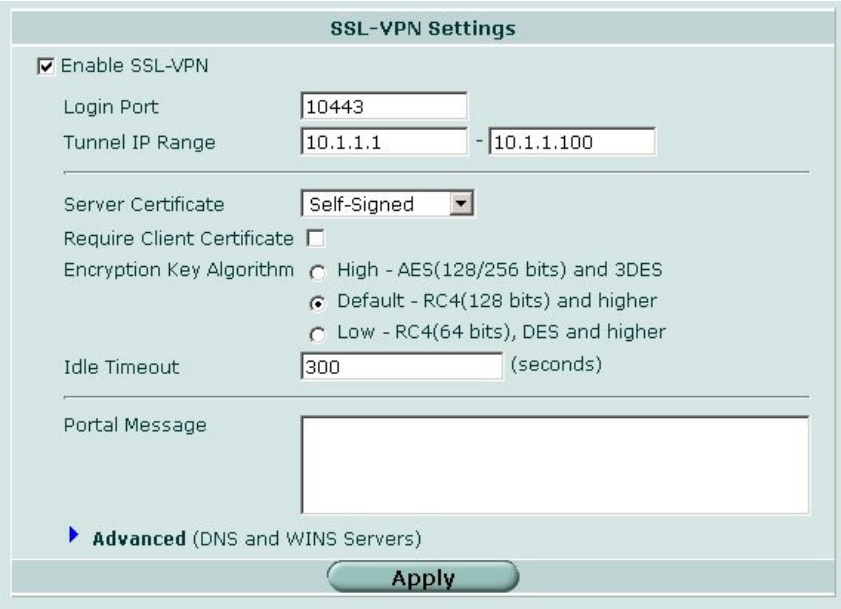
**Note:** The source address for both SSL VPN firewall policies can be left as ‘all’ when the users do not have static public IPs.

First, you establish the tunnel IP range.

Go to **VPN > SSL,** and enable SSL-VPN.

Enter the Tunnel IP Range corresponding to the range of IP addresses available for the users/user groups, in this case 10.1.1.1 - 10.1.1.100.

**Figure 11: Enable SSL-VPN Settings**




After enabling SSL VPN, you must create the users and then the user groups that require SSL VPN tunnel mode access.

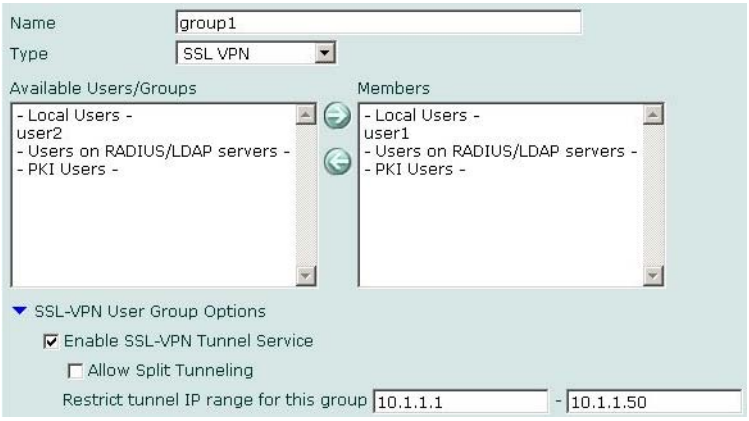
Go to **User > Local** and create user1 and user2 with password authentication.

**Note:** user1 only has permission to access the Linux server, while user2 only has permission to access the Windows PC.

After you create the users, you must create the SSL VPN user groups. In order to configure each user with different access permissions, you must create separate user groups and designate specific IP ranges for each group.

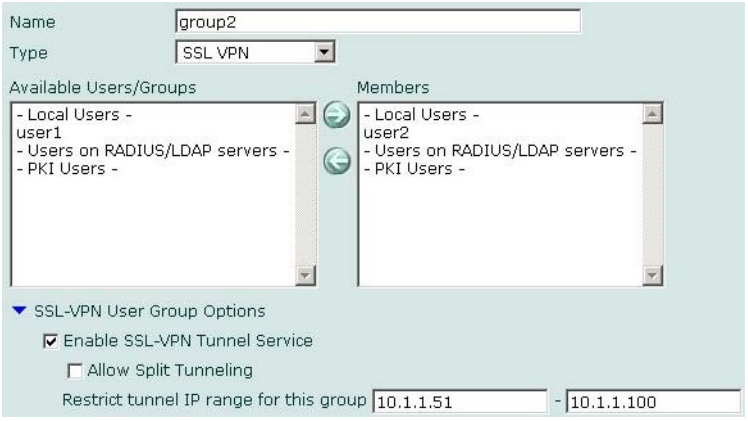
Go to **User > User Group**. Create group1 as an SSL VPN user group with user1 as the member and 10.1.1.1 - 10.1.1.50 as the values in 'Restrict tunnel IP range for this group'.

**Figure 12: group1 user group attributes**




Create group2 as an SSL VPN user group with user2 as the member and 10.1.1.51 - 10.1.1.100 as the values in 'Restrict tunnel IP range for this group'.

**Figure 13: group2 user group attributes**




After you create the user groups, you need to define the firewall policies to support tunnel-mode operations.

The firewall policy specifies the originating (source) IP address of a packet and the destination address that defines the IP address of the intended recipient or network. In this configuration, the source address corresponds to the public IP address that can connect to the FortiGate unit, and the destination address corresponds to the IP address of the Linux server/Windows PC behind the FortiGate unit.

Before you create the firewall policy, you must define the source and destination addresses to include in the policy.

Go to **Firewall > Address** to create the source and destination addresses to specify in the firewall policies.

**Figure 14: Source/destination firewall addresses - Public IP**

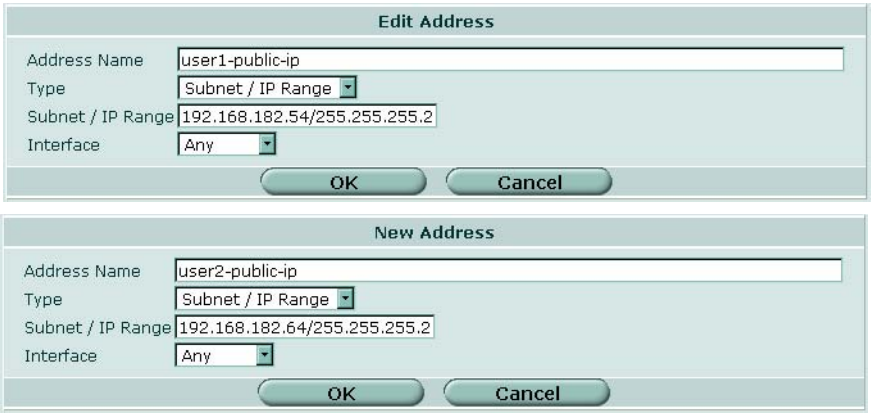
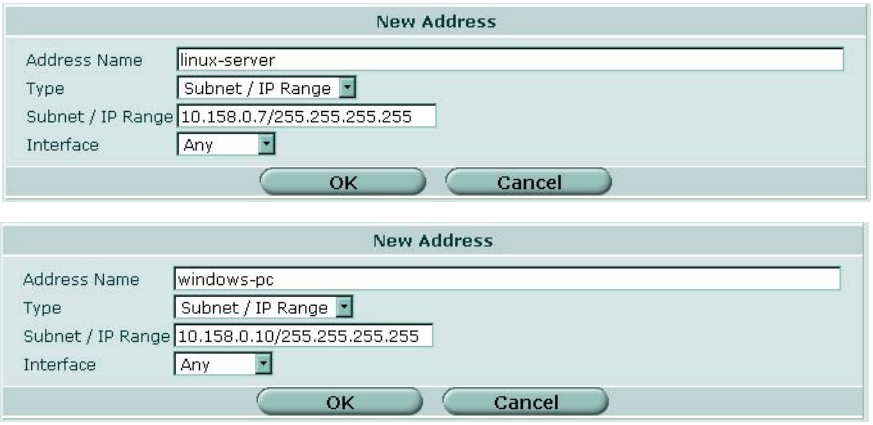


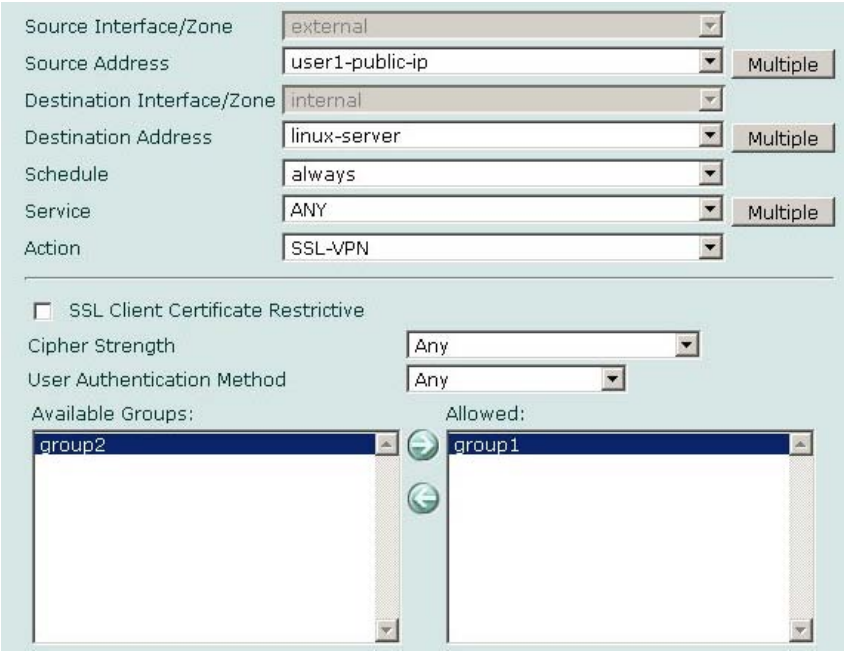
**Figure 15: Source/destination firewall addresses - Linux/Windows PC**




After creating the source and destination addresses, go to **Firewall > Policy** to create the firewall policies.

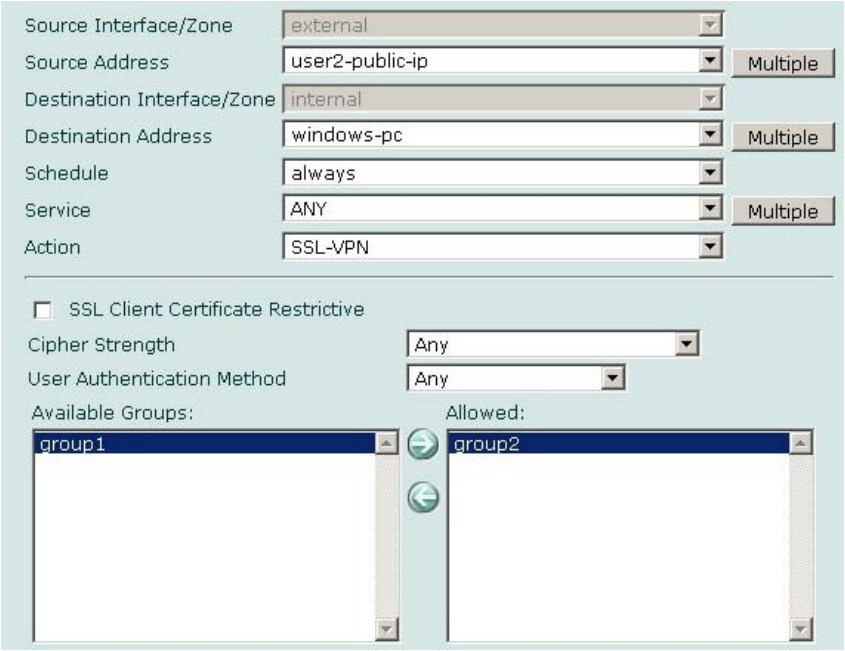
The policy for user1 is an SSL-VPN firewall policy that includes the applicable source and destination addresses, and has group1 as the user group attached to the policy.

**Figure 16: user1 firewall policy**



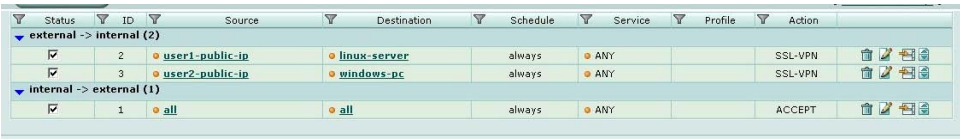

The user2 policy is also an SSL-VPN firewall policy that includes the applicable source and destination addresses, and has group2 as the user group attached to the policy.

**Figure 17: user2 firewall policy**

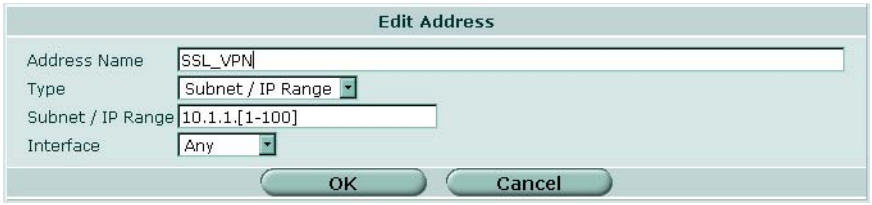



To view the SSL VPN policies, go to **Firewall > Policy**.

**Figure 18: Firewall policy list**




To avoid overlap with other firewall policies, add a DENY policy below the SSL VPN policies (the source is the SSL VPN tunnel IP range). See Configuring firewall policies for more information.




# Working with the web portal

This section introduces the web portal features and explains how to configure them.

The following topics are included in this section:



## Connecting to the FortiGate unit

You can connect to the FortiGate unit using a web browser. The URL of the FortiGate interface may vary from one installation to the next. If required, ask your FortiGate administrator for the URL of the FortiGate unit, and obtain a user name and password.

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

**To log in to the FortiGate secure HTTP gateway**

1. Using the web browser on your computer, browse to the URL of the FortiGate unit (for example, `https://`<FortiGate_IP_address>`:10443/remote`).
2. The FortiGate unit may offer you a self-signed security certificate. If you are prompted to proceed, select Yes.
3. A second message may be displayed to inform you that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. You can ignore the message.
4. When you are prompted for your user name and password:
   - In the Name field, type your user name.
   - In the Password field, type your password.

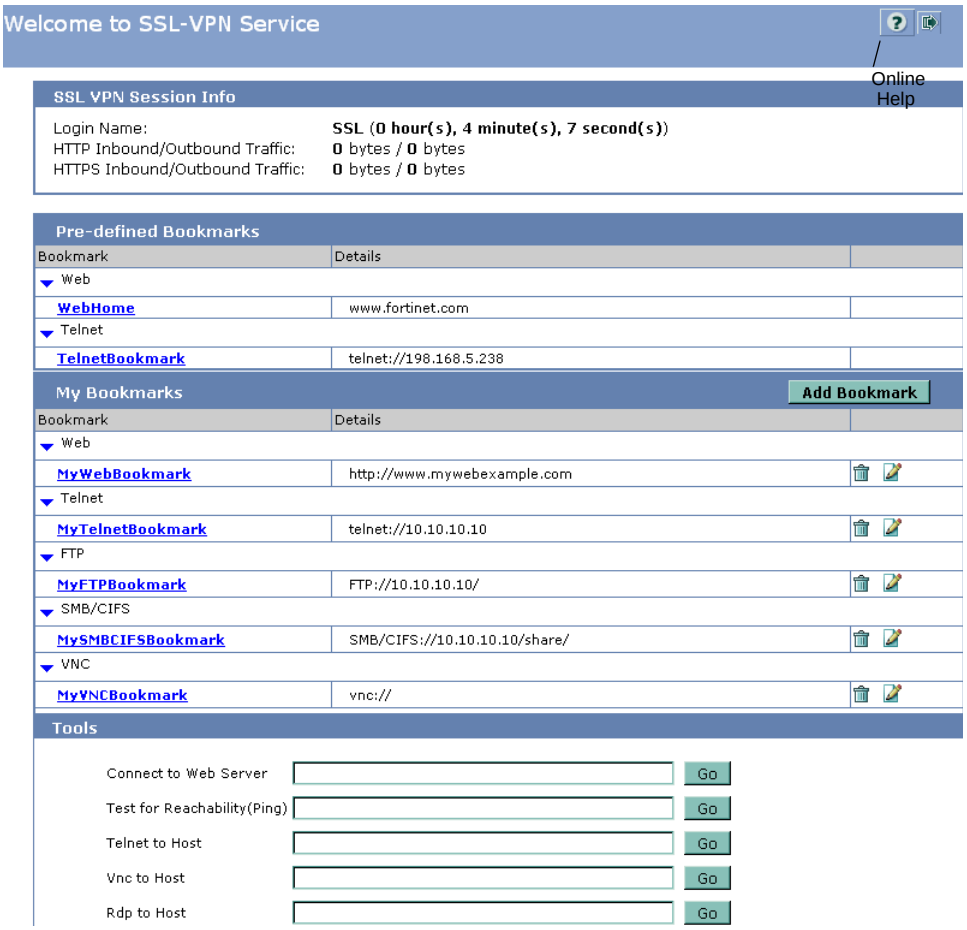
5 Select Login.

The FortiGate unit will redirect your web browser to the FortiGate SSL VPN Remote Access Web Portal home page automatically.

# Web portal home page features

The FortiGate SSL VPN Remote Access Web Portal home page (see Figure 19) is displayed after you log in. If you need help as you work, select the Online Help button in the top right corner of the page.

**Figure 19: FortiGate SSL VPN Remote Access Web Portal page**




If your user account permits web-only mode access, and your administrator has set up pre-defined bookmarks for you, they will appear in a list under Pre-defined Bookmarks. You can start any session from these hyperlinks, but you cannot change them. Also, you can create your own hyperlinks to frequently accessed server applications and start any session from the home page through these hyperlinks. See “Launching web portal applications” on page 45 and “Adding a bookmark to the My Bookmarks list” on page 46. In Figure 19, hyperlinks to all of the supported web portal applications are present in the My Bookmarks list.

If your user account permits tunnel-mode connections, you can install/uninstall Fortinet SSL VPN client software and/or initiate an SSL VPN tunnel with the FortiGate unit. Selecting the Activate SSL-VPN Tunnel Mode link at the top of the home page displays the Fortinet SSL VPN Client area. See “Tunnel-mode features” on page 55.

At the bottom of the page in the Tools area (see Figure 19 on page 44), you can connect to a web server or start a telnet session. You can also check connectivity to a host or server on the network behind the FortiGate unit. For more information, see “Starting a session from the Tools area” on page 55.

## Launching web portal applications

The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the My Bookmarks list (see “Adding a bookmark to the My Bookmarks list” on page 46).

**Note:** If you want to access a web server or telnet server without first adding a bookmark to the My Bookmarks list, type the URL or IP address of the server into the appropriate field under Tools instead (see “Starting a session from the Tools area” on page 55).

One or more of the following server applications may be available to you, depending on whether they were installed by the server administrator:

- Web servers (HTTP/HTTPS) download HTML pages in response to web browser requests.
- Telnet servers (TCP/IP Terminal Emulation Protocol) enable you to use your computer as a virtual terminal to log in to a remote host.
- FTP (File Transfer Protocol) servers enable you to transfer files between your computer and a remote host.
- SMB/CIFS servers implement the Server Message Block (SMB) protocol to support file sharing between your computer and a remote server host.
- VNC (Virtual Network Computing) servers enable you to remotely control another computer, for example, accessing work from your home computer.
- RDP (Remote Desktop Protocol) servers have a multi-channel protocol that allows users to connect to computers running Microsoft Terminal Services.

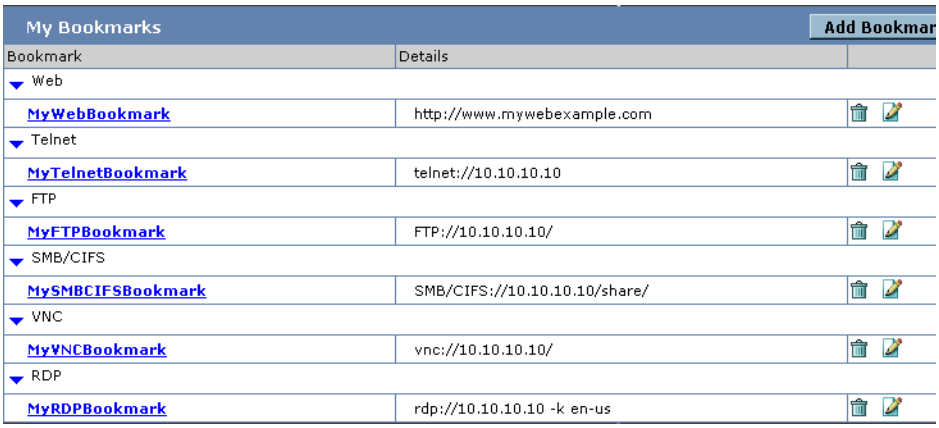
**Note:** Windows file sharing through SMB/CIFS is supported through shared directories.

When you access any of these server applications, the server may prompt you for a user name and password. To log in, you must have a user account created by the server administrator.

## Adding a bookmark to the My Bookmarks list

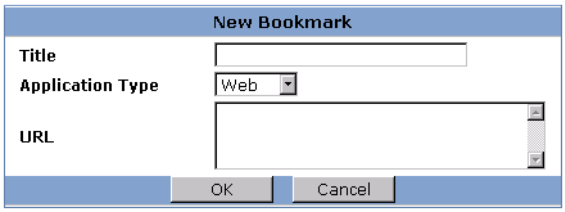
You can add a list of frequently used connections to the web portal home page. Afterward, select any hyperlink from the My Bookmarks list to initiate a session.

**Figure 20: Frequently used connections in the My Bookmarks list**




| | |
|---|---|
| **Add Bookmark** | Create a hyperlink. |
| **Bookmark** | The names of links to remote server applications and network services. |
| **Details** | The information that the FortiGate unit needs to forward client requests to servers on the Internet or a private network behind the FortiGate unit. |
| **Delete and Edit icons** | Delete or edit an entry in the list. |

**Figure 21: New Bookmark dialog box**

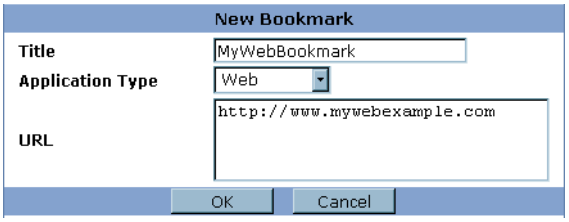



| | |
|---|---|
| **Title** | Type the text to display in the hyperlink. The name is displayed in the My Bookmarks list. |

| | |
|---|---|
| **Application Type** | Select the abbreviated name of the server application or network service from the drop-down list:<br>• Web<br>• Telnet<br>• FTP<br>• SMB/CIFS<br>• VNC<br>• RDP |
| **URL**, **Host Name/IP**, or **Shared File Folder** | Type the information that the FortiGate unit needs to forward client requests to the correct server application or network service:<br>• If the application type is Web, type the URL of the web server (for example, `http://www.google.com` or `https://172.20.120.101`).<br>• If the application type is Telnet, type the IP address of the telnet host (for example, `10.10.10.10`).<br>• If the application type is FTP, type the IP address of the FTP host as a root directory (for example, `//10.10.10.10/share/`).<br>• If the application type is SMB/CIFS, type the IP address of the SMB host and the root directory associated with your account (for example, `//10.10.10.10/share/`).<br>• If the application type is VNC, type the IP address of the VNC host (for example, `10.10.10.10`).<br>• If the application type is RDP, type the IP address of the RDP host (for example, `10.10.10.10`). |

### To add an HTTP or HTTPS connection and access the web server

1. Select Add Bookmark.
2. In the Title field, type a name to represent the connection.
3. From the Application Type list, select Web.
4. In the URL field, type the URL of the web server (for example, `http://www.mywebexample.com` or `https://172.20.120.101`).




5. Select OK.
6. To connect to the web server, select the hyperlink that you created.

   The FortiGate unit replaces the URL with `https://`<FG_IP_address>:<port_no>`/proxy/http/`<specified_URL> and the requested page is displayed.
7. To end the session, close the browser window.

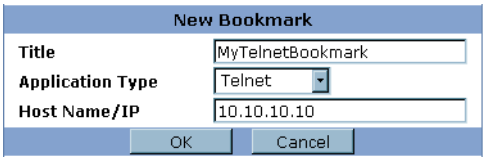
### To add a telnet connection and start a telnet session

1. Select Add Bookmark.

2 In the Title field, type a name to represent the connection.

3 From the Application Type list, select Telnet.

4 In the Host Name/IP field, type the IP address of the telnet host (for example, `10.10.10.10`).



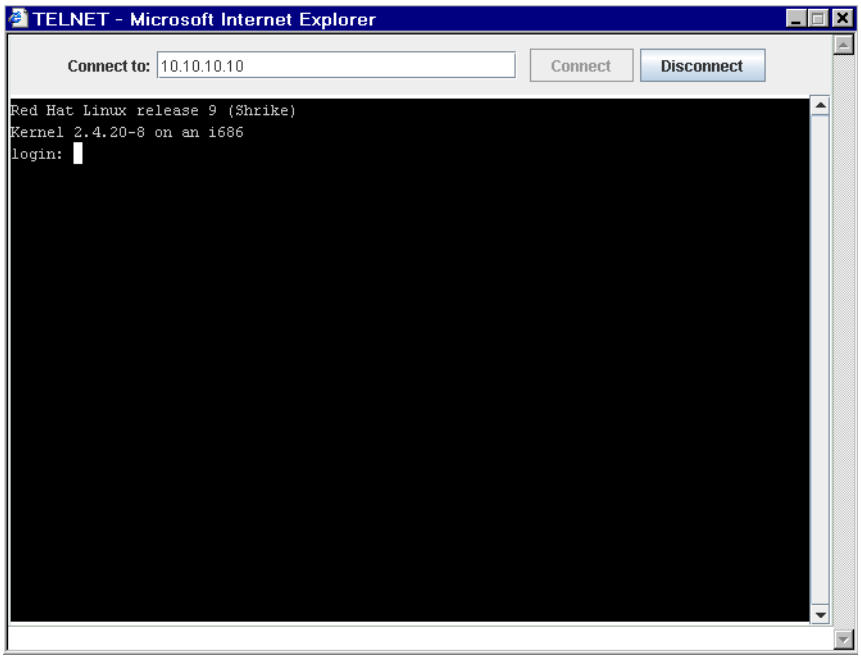

5 Select OK.

6 To start a telnet session, select the hyperlink that you created.

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

7 Select Connect.

8 A telnet session starts and you are prompted to log in to the remote host. You must have a user account to log in. After you log in, you may enter any series of valid telnet commands at the system prompt.




9 To end the session, select Disconnect (or type `exit`) and then close the TELNET connection window.

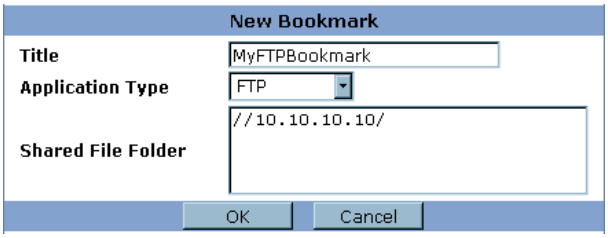
**To add an FTP connection and start an FTP session**

1 Select Add Bookmark.

2 In the Title field, type a name to represent the connection.

3 From the Application Type list, select FTP.

4 In the Shared File Folder field, type the IP address of the FTP host as a root directory (for example, `//10.10.10.10/`).



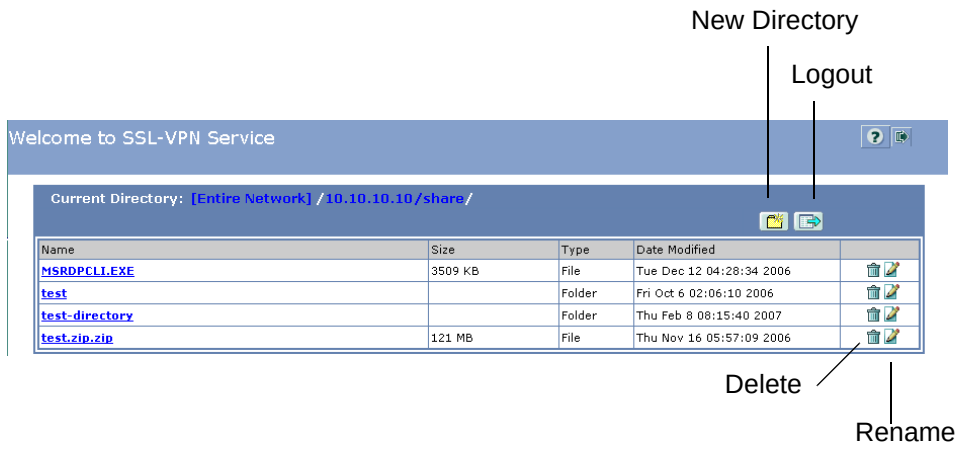

5 Select OK.

6 To start the ftp session, select the hyperlink that you created.

7 When you are prompted to log in to the remote host, type your user name and password. You must have a user account on the remote host to log in.


8 Select Login.

After you log in, the files and subdirectories in the root directory are displayed. You can switch to a subdirectory from the root directory. For example, the following image shows the contents of a subdirectory named `share`.



The view enables you to navigate through the file system and manipulate files in the following ways:

- To download a file from the current directory, select the file link in the Name column.
- To create a subdirectory in the current directory, select New directory.
- To delete a file or subdirectory from the current directory, select Delete.
- To rename a file in the current directory, select Rename.
- To upload a file from the remote directory to the current directory on your client computer, select the file link in the Name column.
- To access a subdirectory, select the file link in the Name column.
- When the current directory is a subdirectory, you can select Up to switch to the parent directory.

9 To end the FTP session, select Logout.

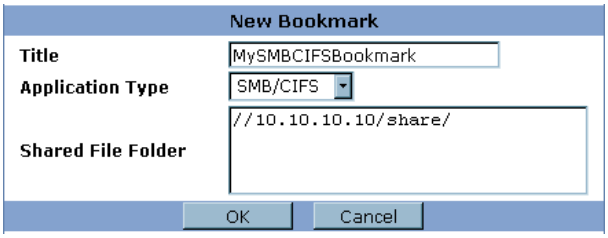
**To add a SMB/CIFS connection and start a SMB session**

1 Select Add Bookmark.

2 In the Title field, type a name to represent the connection.

3 From the Application Type list, select **SMB/CIFS**.

4 In the Shared File Folder field, type the IP address of the SMB host and the root directory associated with your account (for example, `//10.10.10.10/share/`).



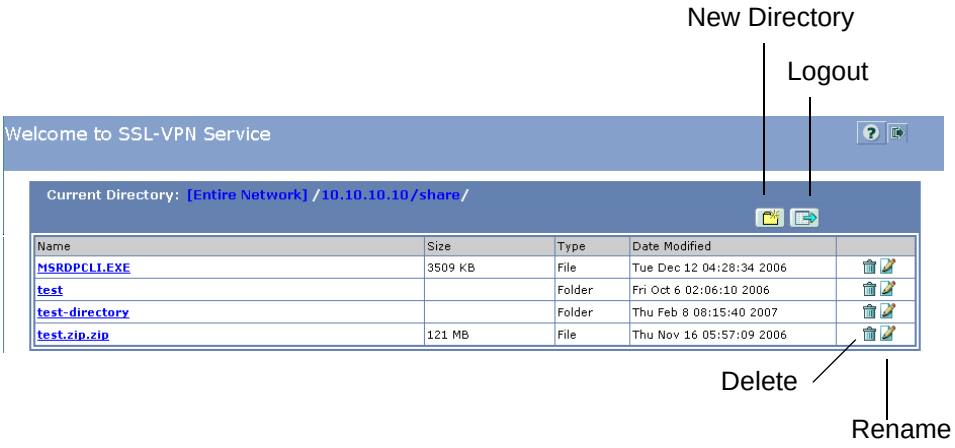

5 Select OK.

6 To start a SMB/CIFS session, select the hyperlink that you created.

7 When you are prompted to log in to the remote host, type your user name and password. You must have a user account on the remote host to log in.


8 Select Login.

After you log in, the root directory associated with your user or group account is displayed. For example, in the figure below, the files and subdirectories in the root directory `share` are displayed.




The view enables you to navigate through the file system and manipulate files in the following ways:

- To download a file from the current directory, select the file link in the Name column.
- To create a subdirectory in the current directory, select New directory.
- To delete a file or subdirectory from the current directory, select Delete.
- To rename a file in the current directory, select Rename.
- To upload a file from the remote directory to the current directory on your client computer, select the file link in the Name column.
- To access a subdirectory, select the file link in the Name column.
- When the current directory is a subdirectory, you can select Up to switch to the parent directory.

**9** To end the SMB/CIFS session, select Logout.

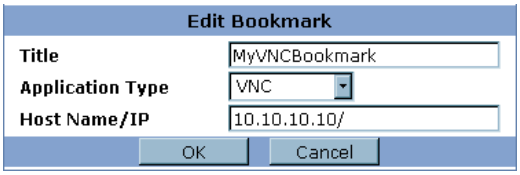
**To add a VNC connection and start a VNC session**

1 Select Add Bookmark.

2 In the Title field, type a name to represent the connection.

3 From the Application Type list, select **VNC**.

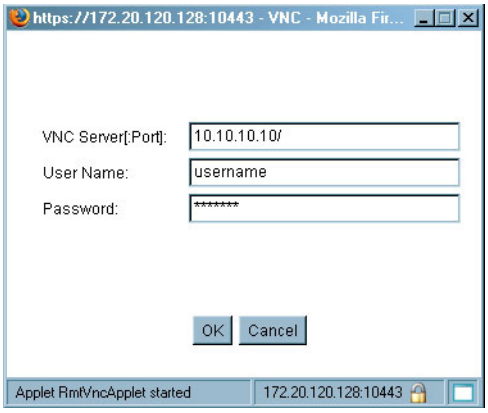
4 In the Host Name/IP field, type the IP address of the VNC host (for example, `10.10.10.10/`).




5 Select OK.

6 To start a VNC session, select the hyperlink that you created.

7 When you are prompted to log in to the remote host, type your user name and password. You must have a user account on the remote host to log in.




8 Select OK.

9 To end the VNC session, select Disconnect.

### To add a RDP connection and start a RDP session

**Note:** You can specify a keyboard layout setting as a parameter when setting up the RDP connection. The format to enter the setting in "**RDP to Host**" is:

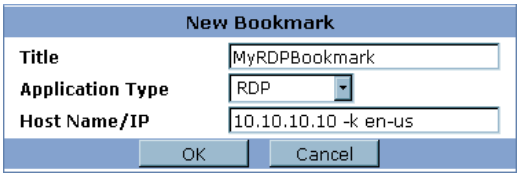
- "`yourserver.com -m fr`"

where '`fr`' selects French as the Windows environment. Select the code that matches your local installation of Windows - for example, if your local machine has the Turkish version of Windows installed, select '`tr`', regardless of the version of Windows installed on the server you connect to.

The codes are as follows:

- ar: Arabic
- da: Danish
- de: German
- en-bg: English, Great Britain
- en-us: English, US
- es: Spanish
- fi: Finnish
- fr: French
- fr-be: French, Belgian
- hr: Croatian
- it: Italian
- ja: Japanese
- lt: Lithuanian
- lv: Latvian
- mk: Macedonian
- no: Norwegian
- pl: Polish
- pt: Portuguese
- pt-br: Brazilian Portuguese
- ru: Russian
- sl: Slovenian
- sv: Sedanese
- tk: Turkmen
- tr: Turkish

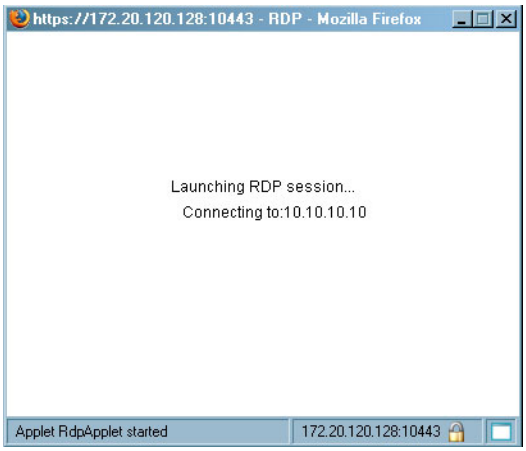
1. Select Add Bookmark.
2. In the Title field, type a name to represent the connection.
3. From the Application Type list, select **RDP**.
4. In the Shared File Folder field, type the IP address of the RDP host (for example, `10.10.10.10`).




5. Select OK.

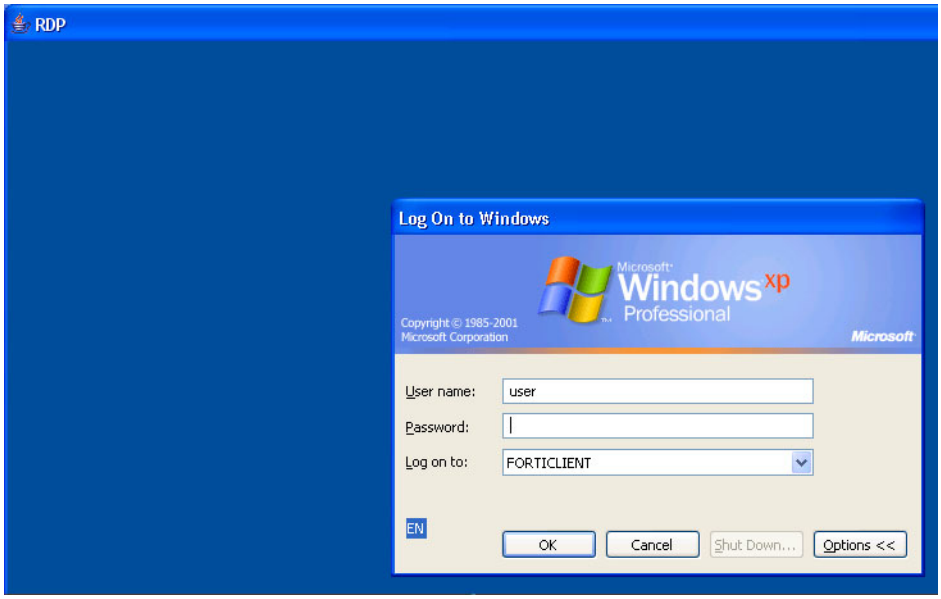
6 To start a RDP session, select the hyperlink that you created.

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




7 When you see a screen configuration dialog, click OK.


8 When you are prompted to log in to the remote host, type your user name and password. You must have a user account on the remote host to log in.




9 Select Login.

10 To end the RDP session, select Logout.

# Starting a session from the Tools area

You can connect to any web server or telnet server without adding a bookmark to the My Bookmarks list. The fields in the Tools area enable you to specify the URL or IP address of the host computer. If required, you can ping a host computer behind the FortiGate unit to verify connectivity to that host.

**To connect to a web server from the Tools area**

1. In the Connect to Web Server field, type the URL of the web server (for example, `http://www.mywebexample.com` or `https://172.20.120.101`).
2. Select Go.

   The FortiGate unit replaces the URL with `https://`<FG_IP_address>:<port_no>`/proxy/http/`<specified_URL> and the requested page is displayed.
3. To end the session, close the browser window.

**To ping a host or server behind the FortiGate unit**

1. In the Test for Reachability (Ping) field, type the IP address of the host or server that you want to reach (for example, `192.168.12.22`).
2. Select Go.

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

**To start a telnet session from the Tools area**

1. In the Telnet to Host field, type the IP address of the telnet host (for example, `192.168.5.238`).
2. Select Go.

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

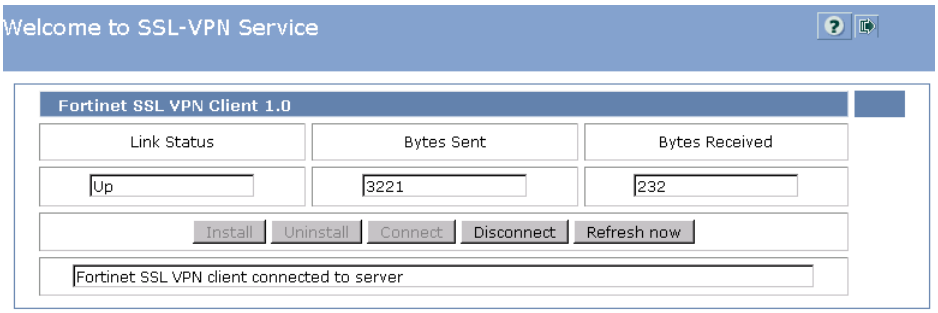
3. Select Connect.
4. A telnet session starts and you are prompted to log in to the remote host. You must have a user account to log in. After you log in, you may enter any series of valid telnet commands at the system prompt.
5. To end the session, select Disconnect (or type `exit`) and then close the TELNET connection window.

# Tunnel-mode features

The FortiGate SSL VPN Remote Access Web Portal page is displayed after you log in. Selecting the Activate SSL-VPN Tunnel Mode link at the top of the home page displays the Fortinet SSL VPN Client area.

If your user account permits tunnel-mode connections, you can install/uninstall SSL VPN client software and/or initiate an SSL VPN tunnel with the FortiGate unit (see Figure 22). For more information, see “Working with the ActiveX plugin” on page 56.

**Figure 22: Fortinet SSL VPN Client 1.0 page (tunnel mode)**




| | |
|---|---|
| **Link Status** | The state of the SSL VPN tunnel:<br>• Up is displayed when an SSL VPN tunnel with the FortiGate unit has been established.<br>• Down is displayed when a tunnel connection has not been initiated. |
| **Bytes Sent** | The number of bytes of data transmitted from the client to the FortiGate unit since the tunnel was established. |
| **Bytes Received** | The number of bytes of data received by the client from the FortiGate unit since the tunnel was established. |
| **Install** | Download the SSL VPN client software from the FortiGate unit and add the ActiveX plugin to the local web browser. |
| **Uninstall** | Uninstall the ActiveX plugin. |
| **Connect** | Initiate a session and establish an SSL VPN tunnel with the FortiGate unit. |
| **Disconnect** | End the session and close the tunnel to the FortiGate unit. |
| **Refresh Now** | Refresh the Fortinet SSL VPN Client page. |

## Working with the ActiveX plugin

The ActiveX plugin provides the software that your client computer needs to establish an SSL VPN tunnel with the FortiGate unit. You have to download the ActiveX plugin from the FortiGate unit and install the plugin on your client computer before your computer can establish a VPN tunnel with the FortiGate unit. Controls for downloading and installing the ActiveX plugin are displayed in the Fortinet SSL VPN Client area of the web portal.

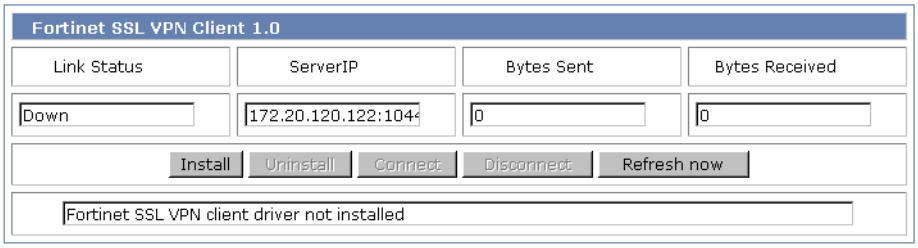
You only have to install the ActiveX plugin once. Afterward, you can use the SSL VPN client software to initiate a VPN tunnel with the FortiGate unit whenever you access the web portal.

**Note:** On your web browser, ensure that the security settings associated with the Internet zone permit you to download and run ActiveX controls. You must also have administrator rights on your computer to install the ActiveX control.

### To download and install the ActiveX plugin

1. At the top of the web portal home page, select the Activate SSL-VPN Tunnel Mode link.
2. The FortiGate unit may prompt you to install and run sslvpn.cab. Select Yes to proceed.

The Fortinet SSL VPN Client 1.0 page is displayed.




3 Select Install.

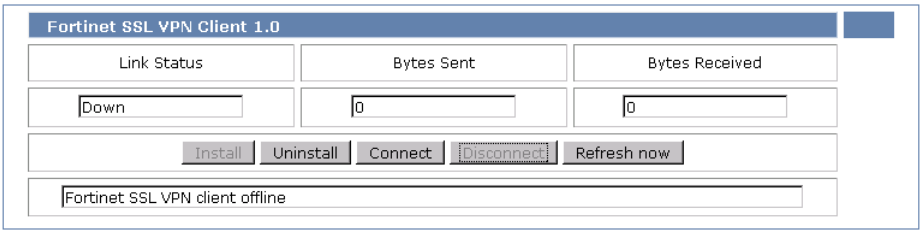
### To initiate a VPN tunnel with the FortiGate unit

The IP address of the public FortiGate interface and the TCP port number through which SSL VPN connections are made are displayed in the Server IP field of the Fortinet SSL VPN Client page.

1 At the top of the web portal home page, select the Activate SSL-VPN Tunnel Mode link.

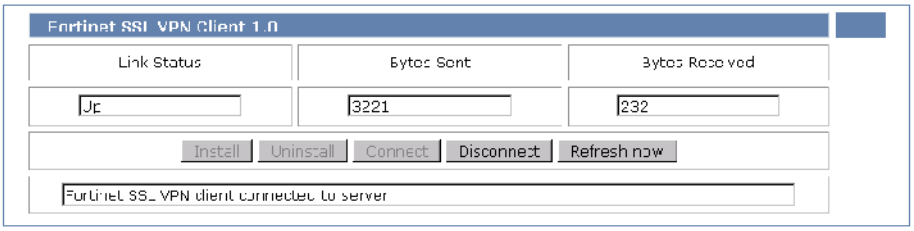
The Fortinet SSL VPN Client page opens.

**Note:** If client security checks are configured for your account, they must complete successfully before the Connect button is enabled.




2 Select Connect.

**Figure 23: Tunnel established**




After the “Fortinet SSL VPN client connected to server” message is displayed and the Disconnect button is enabled (see Figure 23) you have direct access to the network behind the FortiGate unit, subject to the conditions of the FortiGate firewall policy. For example, using a client application on your computer, you could connect to a server application on the network behind the FortiGate unit and download information.

To stop the SSL VPN session and disconnect from the FortiGate unit, select Disconnect. You must log out from the web portal to disconnect from the FortiGate unit (see “Logging out” on page 58). You can use the Connect button to re-establish the tunnel.

### Uninstalling the ActiveX plugin

**To uninstall the ActiveX plugin**

**Note:** You do not have to uninstall the SSL VPN client software if you wish to install an updated version. If the FortiGate unit has a newer version of the ActiveX plugin, it will install it automatically.

1. At the top of the web portal home page, select the Activate SSL-VPN Tunnel Mode link.
2. Select Uninstall.

## Logging out

To log out from the web portal, select the Logout button in the top right corner of the web portal home page.

Logout

# Index

www.fortinet.com

www.fortinet.com