FortiGate® SSL VPNs

FortiOS™ Handbook 4.0 MR1
## Contents

**What's in this book?**  
- Audience .................................................. 7  
- Restrictions .............................................. 7  
- Registering your Fortinet product .................... 7  
- Customer service and technical support .............. 8  
- Training .................................................... 8  
- Documentation ........................................... 8  
  - Fortinet Tools and Documentation CD ............... 8  
  - Fortinet Knowledge Base .................................. 8  
  - Comments on Fortinet technical documentation .... 8  
- Conventions ............................................... 9  
  - IP addresses .............................................. 9  
  - CLI constraints .......................................... 9  
  - Notes, Tips and Cautions ................................ 9  
  - Typographical conventions ............................ 9  

**Introduction to SSL VPN**  
- History .................................................... 11  
- What is a VPN? ............................................ 12  
- What is SSL? .............................................. 12  
  - Goals of SSL ............................................ 12  
  - SSL certificates ......................................... 14  
  - Choosing the level of security for your SSL VPN tunnel .... 14  
- Choosing between SSL and IPSec VPN ................. 14  
  - Legacy versus web-enabled applications ............ 14  
  - Authentication differences ............................ 15  
  - Connectivity considerations .......................... 15  
  - Relative ease of use ................................... 15  
  - Client software requirements .......................... 15  
  - Access control ......................................... 15  
  - Session failover support ............................... 15  
- General topology ......................................... 16  
- SSL VPN modes of operation ............................ 16  
  - Web-only mode .......................................... 17
## Contents

- Configuring routing for tunnel mode ........................................ 56
- Adding an Internet browsing policy. ..................................... 57
- Enabling connection to an IPsec VPN .................................. 57
- Viewing SSL VPN logs ..................................................... 59
- Monitoring active SSL VPN sessions ................................. 61
- Troubleshooting .............................................................. 62

### Working with the web portal

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting to the FortiGate unit</td>
<td>63</td>
</tr>
<tr>
<td>Web portal overview</td>
<td>63</td>
</tr>
<tr>
<td>Applications</td>
<td>64</td>
</tr>
<tr>
<td>Using the Bookmarks widget</td>
<td>65</td>
</tr>
<tr>
<td>Adding bookmarks</td>
<td>66</td>
</tr>
<tr>
<td>Using the Connection Tool</td>
<td>67</td>
</tr>
<tr>
<td>Tunnel-mode features</td>
<td>74</td>
</tr>
<tr>
<td>Using the SSL VPN Virtual Desktop</td>
<td>75</td>
</tr>
</tbody>
</table>

### Using the SSL VPN tunnel client

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client configurations</td>
<td>77</td>
</tr>
<tr>
<td>Web mode</td>
<td>77</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>77</td>
</tr>
<tr>
<td>Virtual desktop application</td>
<td>78</td>
</tr>
<tr>
<td>Downloading the SSL VPN tunnel mode client</td>
<td>78</td>
</tr>
<tr>
<td>Installing the tunnel mode client</td>
<td>79</td>
</tr>
<tr>
<td>Windows</td>
<td>79</td>
</tr>
<tr>
<td>Linux</td>
<td>79</td>
</tr>
<tr>
<td>MAC OS client</td>
<td>79</td>
</tr>
<tr>
<td>Using the tunnel mode client</td>
<td>80</td>
</tr>
<tr>
<td>Windows client</td>
<td>80</td>
</tr>
<tr>
<td>Linux client</td>
<td>82</td>
</tr>
<tr>
<td>MAC OS X client</td>
<td>84</td>
</tr>
<tr>
<td>Uninstalling the tunnel mode client</td>
<td>86</td>
</tr>
</tbody>
</table>

### Examples

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic SSL VPN example</td>
<td>87</td>
</tr>
<tr>
<td>Infrastructure requirements</td>
<td>88</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>88</td>
</tr>
<tr>
<td>Creating the firewall addresses</td>
<td>88</td>
</tr>
<tr>
<td>Creating the destination address</td>
<td>88</td>
</tr>
</tbody>
</table>
Contents

Creating the tunnel client range address ........................................... 89
Enabling SSL VPN and setting the tunnel user IP address range ............... 89
Creating the web portal ................................................................. 89
Creating the user account and user group ....................................... 90
Creating the firewall policies ....................................................... 91
Add routing to tunnel mode clients .............................................. 92

Multiple user groups with different access permissions example .......... 93
General configuration steps ........................................................ 93
Creating the firewall addresses .................................................... 94
Creating the destination addresses ............................................... 94
Creating the tunnel client range addresses ..................................... 94
Creating the web portals ............................................................... 95
Creating the user accounts and user groups .................................. 96
Creating the firewall policies ....................................................... 97
Create the static route to tunnel mode clients ................................ 100
Enabling SSL VPN operation ....................................................... 100

OS patch check example ............................................................. 101

Index 103
What’s in this book?

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

The following chapters are included in this document:

**Introduction to SSL VPN** - If you are new to SSL VPN or if you need guidelines to decide what features to use, this chapter provides useful general information about VPN and SSL, how the FortiGate unit implements them, and gives guidance on how to choose between SSL and IPSec.

**Setting up the FortiGate unit** - The first step in building a VPN involves configuring the FortiGate unit and the web portal. Along with these configuration details, this chapter also explains how to grant unique access permissions, configure the SSL virtual interface (ssl.root), and describes the SSL VPN OS Patch Check feature that allows a client with a specific OS patch to access SSL VPN services.

**Working with the web portal** - This chapter explains how to use a web portal and its widgets. Access to different network resource types, such as SMB, FTP, RDP is covered.

**Using the SSL VPN tunnel client** - This chapter explains how to install and use the tunnel mode clients for Windows, Linux, and Mac OS X.

**Examples** - Several configuration scenarios are explored with step-by-step instructions. While the information provided is enough to set up the described SSL VPN configurations, these scenarios are not the only possible SSL VPN setups.

**Audience**

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

**Restrictions**

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

**Registering your Fortinet product**


Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article Registration Frequently Asked Questions.
Customer service and technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article What does Fortinet Technical Support require in order to best assist the customer?

Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email them at training@fortinet.com.

Documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

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

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

CLI constraints

CLI constraints, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable input for a given parameter or variable value. CLI constraint conventions are described in the CLI Reference document for each product.

Notes, Tips and Cautions

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.

Note: Also presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.

Tip: Highlights useful additional information, often tailored to your workplace activity.

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

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field, or check box label</td>
<td>From Minimum log level, select Notification.</td>
</tr>
<tr>
<td>CLI input</td>
<td>config system dns set primary <code>&lt;address_ipv4&gt;</code> end</td>
</tr>
<tr>
<td>CLI output</td>
<td>FGT-602803030703 # get system settings comments : (null) opmode : nat</td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are not secure and can be intercepted by a third party.</td>
</tr>
<tr>
<td>File content</td>
<td><code>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</code></td>
</tr>
</tbody>
</table>
Table 1: Typographical conventions in Fortinet technical documentation

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as Central_Office_1.</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to VPN &gt; IPSEC &gt; Auto Key (IKE).</td>
</tr>
<tr>
<td>Publication</td>
<td>For details, see the FortiGate Administration Guide.</td>
</tr>
</tbody>
</table>
Introduction to SSL VPN

This section provides information about setting up the SSL VPN client for use in an SSL VPN tunnel or web-mode operation.

The following topics are included in this section:

- History
- What is a VPN?
- What is SSL?
- Choosing between SSL and IPSec VPN
- General topology
- SSL VPN modes of operation
- Single Sign-on (SSO)

History

Over the past several years, as organizations have grown and become more complex, secure remote access to network resources has become critical for day-to-day operations. In addition, businesses are expected to provide clients with efficient, convenient services including knowledge bases and customer portals, and employees travelling across the country or around the world require timely and comprehensive access to network resources. Initial access to network resources used private networks and leased lines - options that were inflexible and costly. As a result of the growing need for providing remote/mobile clients with easy, cost-effective and secure access to a multitude of resources, the concept of a Virtual Private Network was developed.

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

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

Virtual Private Network (VPN) technology allows clients to connect to remote networks in a secure way. A VPN is a secure logical network created from physically separate networks. VPNs use encryption and other security methods to ensure that only authorized users can access the network. VPNs also ensure that the data transmitted between computers cannot be intercepted by unauthorized users. When data is encoded and transmitted over the Internet, the data is said to be sent through a “VPN tunnel”. A VPN tunnel is a non-application oriented tunnel that allows the users and networks to exchange a wide range of traffic regardless of application or protocol.

Figure 1: Encoded data going through a VPN tunnel

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

What is SSL?

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

Goals of SSL

SSL has four main goals:
1. Confidentiality of communications
2. Integrity of data
3. Authentication of server
4. Authentication of client (non-repudiation)

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

There are four cryptographic primitives that are specific to VPNs:

1. **Symmetric ciphers** (confidentiality) — Symmetric encryption uses a very fast block-level algorithm to encrypt and decrypt data, and is the primary primitive used to protect data confidentiality. Both sides of the tunnel will use the same encrypt/decrypt key, which is the primary weakness of symmetric ciphers. A key is usually a large number that is fed to a cryptographic algorithm to encrypt plaintext data into ciphertext or to decrypt ciphertext data into plaintext.

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

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

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

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

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

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

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

Choosing the level of security for your SSL VPN tunnel

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

Choosing between SSL and IPSec VPN

The FortiGate unit supports both SSL and IPSec VPN technologies. Each combines encryption and VPN gateway functions to create private communication channels over the Internet. Both enable you to define and deploy network access and 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 or routers are used to provide network protection, and company-sanctioned client computers are issued to users. SSL VPNs are a good choice for roaming users who depend on a wide variety of thin-client computers to access enterprise applications and/or company resources from a remote location.

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

Legacy versus web-enabled applications

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

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

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

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

Connectivity considerations

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

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

Relative ease of use

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

Client software requirements

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

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

Access control

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

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

Access to SSL VPN applications is controlled through user groups.

Session failover support

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

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

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

**Figure 2: Example SSL VPN configuration**

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

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

The general infrastructure requirements are quite simple:

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

**SSL VPN modes of operation**

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on user name, password, and authentication domain. A successful login determines the access rights of remote users according to user group. The user group settings specify whether the connection will operate in web-only mode (see “Web-only mode” on page 17) or tunnel mode (see “Tunnel mode” on page 18).
You can enable a host integrity checker to scan the remote client. The integrity checker probes the remote client computer to verify that it is safe before access is granted. Security attributes recorded on the client computer (for example, in the Windows registry, in specific files, or held in memory due to running processes) are examined and uploaded to the FortiGate unit.

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

**Web-only mode**

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

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

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

When the FortiGate unit provides services in web-only mode, a secure connection between the remote client and the FortiGate unit is established through the SSL VPN security in the FortiGate unit and the SSL security in the web browser. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

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

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

**Web-only mode client requirements**

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

- Microsoft Windows 2000/XP/2003/Vista, Linux, Mac OS X, or UNIX operating system
- Microsoft Internet Explorer 6.0 (or later), Netscape Navigator 7.0 (or later), Mozilla Foundation/Firefox 1.5 (or later), or Apple Safari 1.3 (or later)
- If Telnet/ or RDP are used, Sun Java runtime environment 1.4 (or later), with Java applet access, JavaScript access, and enabled cookie acceptance
Tunnel mode

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

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

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

Configuring the FortiGate unit to establish a tunnel with remote clients involves enabling the feature through SSL VPN configuration settings and selecting the appropriate web portal configuration for tunnel-mode access in the user group settings. The 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 or 2003, XP or Vista (32 or 64-bit), Mac OS X v10.3.9 “Panther”, v10.4 “Tiger”, v10.5 “Leopard”, or Linux Distributions RedHat (Enterprise 4 or higher), RedHat Enterprise Linux Desktop 5, Fedora 7 & 8, CentOS 5,2, Debian 4 r1, Ubuntu 6.06, 7, and 8.04, and SUSE Enterprise 10
- Microsoft Internet Explorer 6.0 (or later) with ActiveX enabled, or Mozilla Foundation/Firefox (1.5 or later) with Java Platform enabled

The browser requirements only apply if you use the tunnel mode client on Windows through the browser interface. You do not need a browser if you use the standalone tunnel client.
The web portal can provide bookmarks to connect to network resources. A web (HTTP/HTTPS) bookmark can include login credentials so that the FortiGate unit automatically logs the user into the web site. This means that the user logs into the SSL VPN and then does not have to enter any more credentials to visit preconfigured web sites.

Both the administrator and the end user can configure bookmarks, including SSO bookmarks.

To add bookmarks as an administrator, see "Adding, editing, or deleting bookmarks" on page 38. To add bookmarks as a web portal user, see "Adding bookmarks" on page 66.

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

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

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

- Before you begin
- General configuration steps
- Configuring SSL VPN settings
- Configuring SSL VPN web portals
- Configuring user accounts and SSL VPN user groups
- Configuring firewall policies
- Viewing SSL VPN logs
- Monitoring active SSL VPN sessions
- Troubleshooting

Before you begin

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

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

Refer also to the “Examples” chapter for example SSL VPN configurations.
General configuration steps

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

1. Enable SSL VPN connections and set the basic options needed to support SSL VPN configurations. See “Configuring SSL VPN settings” on page 22.

2. Create a web portal to define user access to network resources. If you want to provide different types of access to different groups of users, you need to create multiple web portals. See “Configuring SSL VPN web portals” on page 30.

3. Create user accounts for the remote clients. Create SSL VPN user groups and associate them with the web portal or portals that you created. Assign users to the appropriate SSL VPN user groups. See “Configuring user accounts and SSL VPN user groups” on page 47.

4. Configure the firewall policies and the remaining parameters needed to support the VPN mode of operation. See “Configuring firewall policies” on page 49.

5. For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface. See “Configuring routing for tunnel mode” on page 56.

6. Optionally, define SSL VPN event-logging parameters, and monitor active SSL VPN sessions. See “Viewing SSL VPN logs” on page 59, and “Monitoring active SSL VPN sessions” on page 61.

If you have problems during SSL VPN configuration in this chapter, see “Troubleshooting” on page 62 for assistance.

Configuring SSL VPN settings

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

- “Enabling SSL VPN operation” on page 23.
- “Specifying an IP address range for tunnel-mode clients” on page 23 (required only for tunnel-mode).

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

- “Adding WINS and DNS services for clients” on page 24.
- “Setting the idle timeout setting” on page 25.
- “Setting the client authentication timeout” on page 25.
- “Specifying the cipher suite for SSL negotiations” on page 25. The cipher suite determines the level of data security, but it must be compatible with the capabilities of the clients’ browsers.
- “Changing the port number for web portal connections” on page 27. By default, SSL VPN connections use port 10443.
- “Customizing the web portal login page” on page 28.

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

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

To enable SSL VPN operation - web-based manager

1. Go to VPN > SSL > Config.
2. Select Enable SSL-VPN.
3. Select Apply.

To enable SSL VPN operation - CLI

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

Specifying an IP address range for tunnel-mode clients

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

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

- The VPN > SSL > Config page IP Pools setting applies to all web portals that do not specify their own IP Pools.
- The web portal Tunnel Mode widget IP Pools setting, if used, applies only to the web portal and overrides the setting in VPN > SSL > Config. See “Configuring tunnel mode settings” on page 35.

Caution: Take care to prevent overlapping IP addresses. Do not assign to clients any IP addresses that are already in use on the private network. As a precaution, consider assigning IP addresses from a network that is not commonly used (for example, 10.254.254.0/24).
To set tunnel-mode client IP address range - web-based manager

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

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

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

To set tunnel-mode client IP address range - CLI

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

```
config firewall address
  edit SSL_tunnel_users
    set type iprange
    set end-ip 10.254.254.100
    set start-ip 10.254.254.80
  end
end
config vpn ssl settings
  set tunnel-ip-pools SSL_tunnel_users
end
```

Adding WINS and DNS services for clients

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

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

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

1. Go to VPN > SSL > Config.
2. Select the Expand Arrow to display the Advanced section.
3. Enter the IP addresses of DNS servers in the DNS Server fields as needed.
4. Enter the IP addresses of WINS servers in the WINS Server fields as needed.
5. Select Apply.
To specify WINS and DNS services for clients - CLI

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

Setting the idle timeout setting

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

To set the idle timeout - web-based manager

1. Go to VPN > SSL > Config.
2. In the Idle Timeout field, enter the timeout value.
   - The valid range is from 10 to 28800 seconds.
3. Select Apply.

To set the idle timeout - CLI

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

Setting the client authentication timeout

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

**Note:** The default value is 28800 seconds (8 hours). You can only modify this timeout value in the CLI.

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

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

Specifying the cipher suite for SSL negotiations

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

To set the encryption algorithm - web-based manager

1. Go to VPN > SSL > Config.
2 In *Encryption Key Algorithm*, select one of the following options:

- 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**.

**To set the encryption algorithm - CLI**

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

**Enabling strong authentication through X.509 security certificates**

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

For information about obtaining and installing certificates, see the *FortiGate Certificate Management User Guide*.

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

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

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

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

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

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

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

**Configuring the FortiGate unit to provide strong authentication**

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

In the FortiGate unit SSL VPN settings, you can select which certificate the FortiGate offers to authenticate itself. By default, the FortiOS™ unit offers its factory installed (self-signed) certificate from Fortinet to remote clients when they connect.
To enable FortiGate unit authentication by certificate - web-based manager

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

To enable FortiGate unit authentication by certificate - CLI

For example, to use the example_cert certificate

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

Changing the port number for web portal connections

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

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

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

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

To change the SSL VPN port - web-based manager

1. If <<Global>> appears in the left menu, select it to enter global configuration.
2. Go to System > Admin > Settings.
3. Type an unused port number in SSLVPN Login Port, and select Apply.

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

To change the SSL VPN port - CLI

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

```
config global
  config system global
    set sslvpn-sport 10443
end
```
Customizing the web portal login page

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

Figure 4: Default SSL VPN web portal login page

![Default SSL VPN web portal login page](image)

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

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

1. If you want to edit the global login page and <<Global appears in the left menu, select <<Global to enter global configuration.
2. Go to System > Config > Replacement Messages.
3. Expand the SSL VPN row and select the Edit icon for the SSL VPN login message.

```
<html>
<head>
<title>Login</title>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Cache-Control" content="no-cache">
<meta http-equiv="Cache-Control" content="must-revalidate">
<link href="/style.css" rel="stylesheet" type="text/css">
<script language="JavaScript">
<!--if (top != parent.location != window.location)
```

Caution: Before you begin, copy the default web portal login page text to a separate text file for safe-keeping. Afterward, if needed you can restore the text to the original version.
4 Edit the HTML text, subject to the following restrictions:
   • The login page must be an HTML page containing a form with
     `ACTION="%%SSL_ACT%%"` and `METHOD="%%SSL_METHOD%%"
   • The form must contain the `%%SSL_LOGIN%%` tag to provide the login form.
   • The form must contain the `%%SSL_HIDDEN%%` tag.

5 Select OK.

To configure the SSL VPN login page - CLI

Do one of the following:
   • If VDOMs are enabled and you want to modify the global login page, enter:
     `config global
     config system replacemsg sslvpn sslvpn-login`
   • If you want to modify the login page for a VDOM, enter:
     `config vdom
     edit <vdom_name>
     config system replacemsg-group
     edit default
     config sslvpn
     edit sslvpn-login`

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

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

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

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

At minimum, you need to set up one web portal. See “Configuring basic web portal settings” on page 32. For each portal, you can configure additional security features:

- “Configuring host checking” on page 42
  Check that client computers are running security software.

- “Configuring cache cleaning” on page 44
  Remove session information from the client’s computer after logout.

- “Configuring virtual desktop” on page 44
  Provide a separate Windows desktop environment while connected to the VPN. Control which applications users can run on their virtual desktop using virtual desktop application control.

- “Configuring client OS Check” on page 46
  Check that the client’s Windows operating system is up-to-date.

Before you begin

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

One of the pre-defined web portals might meet your needs. See “Default web portal configurations”. If needed, you can modify these portals using the procedures in this section.

Default web portal configurations

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

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

- **tunnel-access**: Includes *Session Information* and *Tunnel Mode* widgets.

- **web-access**: Includes *Session Information* and *Bookmarks* widgets.
Figure 5: Default web portals

![Default web portals diagram](image)

Figure 6: Default tunnel-access web portal

![Default tunnel-access web portal diagram](image)
Figure 7: Default web access web portal

![Default web access web portal](image)

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

**Configuring basic web portal settings**

This section describes the basic configuration to enable users to access web resources through the portal.

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

1. Go to VPN > SSL > Portal and do one of the following:
   - Select Create New.
   - Select the Edit icon for an existing portal, then select Settings.

   The web portal settings dialog box opens.

   ![Web portal settings](image)

   2. Enter the following information:
      - **Name**: Enter a name to identify this web portal.
      - **Applications**: Select the applications that users can access through this web portal.
      - **Portal Message**: Enter the text that will appear at the top of the web portal window.
      - **Theme**: Select the color scheme for this web portal.
      - **Page Layout**: Select either the single-column or two-column layout.
      - **Redirect URL**: The web portal can display a second HTML page in a popup window when the web portal home page is displayed. Enter the URL.
3 Optionally, you can select the Virtual Desktop tab to configure the Virtual Desktop feature. See "Configuring virtual desktop" on page 44. Or, you can leave this configuration for later.

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

   For information on these features, see “Configuring cache cleaning” on page 44 and “Configuring host checking” on page 42.

5 Select OK.
   The web portal is displayed.

6 Select Apply to save the settings.

To configure basic web portal settings - CLI

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

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

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

Configuring the web portal page layout

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

Figure 9: Configuring the SSL VPN web portal page
To configure the web portal page - web-based manager

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

- Arrange widgets on the page by dragging them by their title bar.
- Add a widget by choosing a widget from the Add Widget list.
- Remove a widget by selecting the Remove icon in the widget title bar.
- Configure a widget by selecting the Edit icon in the widget title bar. For configuration information about each widget type, see the following sections:
  - “Configuring tunnel mode settings” on page 35
  - “Configuring the Session Information widget” on page 37
  - “Configuring the Connection Tool widget” on page 41
  - “Adding, editing, or deleting bookmarks” on page 38
- To modify the color scheme and other basic settings, select the Settings button. See “Configuring basic web portal settings” on page 32. You can also configure several advanced features. For more information, see
  - “Configuring host checking” on page 42
  - “Configuring cache cleaning” on page 44
  - “Configuring virtual desktop” on page 44
  - “Configuring client OS Check” on page 46 (CLI only)

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

To configure the web portal page - CLI

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

For example, to create the portal layout shown in Figure 9 on page 33, you would enter:

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

1. Go to VPN > SSL > Portal.
2. Select the Edit icon for the portal.
3. Select Settings.
4. Type the caption in the Portal Message field, and select OK.

To add a custom web portal caption - CLI

For example, to apply a custom caption to portal2, you could enter:

```
config vpn ssl web portal
edit portal2
set heading "Welcome to the example.com portal"
end
```

Configuring tunnel mode settings

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

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

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

To configure tunnel mode settings - web-based manager

1. Do one of the following:
   - Create a new web portal and complete the basic configuration. See “Configuring basic web portal settings” on page 32.
   - Go to VPN > SSL > Portal and select the Edit icon for an existing portal.
2. If the Tunnel Mode widget is missing, add it by selecting Tunnel Mode from the Add Widget list in the top right corner of the window.
3. Select the Edit icon in the Tunnel Mode widget title bar.
4 Enter the following information:

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

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

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

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

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

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

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

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

5 Select OK in the Tunnel Mode widget.

6 Select Apply.

To configure tunnel mode settings - CLI

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

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

The preceding example applies to a web portal that does not already have a tunnel mode widget. To modify the settings on an existing tunnel mode widget, you need to determine the widget’s number. Enter:
config vpn ssl web portal
   edit portal1
      config widget
         show
In the output, you will see, for example,
   edit 3
      set name "Tunnel Mode"
      set type tunnel
      ...
You can now enter edit 3 and modify the tunnel mode widget's settings.

Configuring the Session Information widget

The Session Information widget displays the login name of the user, the amount of time
the user has been logged in, and the inbound and outbound traffic statistics of HTTP and
HTTPS. You can change the widget name.
To edit the session information, in the Session Information widget select Edit.

Figure 11: Session Information widget - Edit

**Session Information**

<table>
<thead>
<tr>
<th>Time Logged In:</th>
<th>HTTP Inbound/Outbound Traffic:</th>
<th>HTTPS Inbound/Outbound Traffic:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bytes / bytes</td>
<td>bytes / bytes</td>
</tr>
</tbody>
</table>

**Edit**
Select to edit the information in the widget.

**Remove widget**
Select to close the widget and remove it from the web portal home page.

**OK**
Select to save the Session Information configuration.

**Cancel**
Select to exit the Session Information widget without saving any changes.

**Name**
Enter a customized name for the Session Information widget.

---

To configure Session Information settings - CLI

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

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

Configuring the Bookmarks widget

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

To configure the Bookmarks widget

1. Do one of the following:
   - Create a new web portal and complete the basic configuration. See “Configuring basic web portal settings” on page 32.
   - Go to VPN > SSL > Portal and select the Edit icon for an existing portal.
2. If the Bookmarks widget is missing, add it by selecting Bookmarks from the Add Widget list in the top right corner of the web portal window.
4. Optionally, you can change the Name of the Bookmarks widget.
5. Select the Applications check boxes for the types of bookmarks that you want to support.
6. Select OK.

Adding, editing, or deleting bookmarks

You can add bookmarks to the Bookmarks widget. These bookmarks are available to users of the SSL VPN web portal. If needed, you can also modify existing bookmarks.

To delete bookmarks

1. Open the web portal.
2. In the Bookmarks widget, select the Edit button.

Figure 12: Deleting bookmarks
3 Select the X to the right of the bookmark that you want to delete.
4 Select Done.

To add or edit bookmarks - web-based manager
1 Open the web portal.
2 In the Bookmarks widget, do one of the following:
   • To add a bookmark, select Add.
   • To edit an existing bookmark, select the Edit button and then select the bookmark.
3 Enter or edit the following information:

### Adding

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the bookmark.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of application to which the bookmark links. For example, select HTTP/HTTPS for a web site. Only the application types that you configured for this widget are in the list. You can select Edit in the widget title bar to enable additional application types. See “Configuring the Bookmarks widget” on page 38.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the destination of the bookmark. For HTTP, enter the URL or just the hostname. For HTTPS, enter the URL. For RDP, VNC, Telnet or SSH, enter the hostname. For FTP or SMB, enter hostname or //&lt;hostname&gt;/&lt;path&gt;.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a descriptive tooltip for the bookmark.</td>
</tr>
<tr>
<td>SSO</td>
<td>A Single Sign-On (SSO) bookmark automatically enters the login credentials for the bookmark destination. Select one of: Disabled — This is not an SSO bookmark. Automatic — Use the user’s SSL VPN credentials for login. Static — Use the login credentials defined below.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Name</td>
<td>Enter a required login page field name, “User Name” for example.</td>
</tr>
</tbody>
</table>
To configure the Bookmarks widget and add/edit bookmarks - CLI

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

```
config vpn ssl web portal
edit web-access
config widget
edit 1
set type bookmark
set allow-apps ftp web
config bookmarks
edit "example"
set apptype web
set description "example bookmark"
set url "http://example.com"
end
end
end
```

To delete bookmarks - CLI

To delete the bookmark added above, you would enter:

```
config vpn ssl web portal
edit web-access
config widget
edit 1
config bookmarks
delete example
end
end
end
```
Configuring the Connection Tool widget

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

To configure the Connection Tool widget

1. Do one of the following:
   - Create a new web portal and complete the basic configuration. See “Configuring basic web portal settings” on page 32.
   - Go to VPN > SSL > Portal and select the Edit icon for an existing portal.
2. If the Connection Tool widget is missing, add it by selecting Connection Tool from the Add Widget list in the top right corner of the web portal window.
3. Select the Edit icon in the Connection Tool widget title bar.
4. Optionally, enter a new Name for the widget.
5. Select the types of Applications (protocols and services) that the Connection Tool is enabled to access.
6. Select OK.

To configure the Connection Tool widget - CLI

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

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

To increase the security of your network, you can require your SSL VPN clients to have antivirus or firewall software installed on their computers. Only clients that meet the requirements are permitted to log on.

To configure host checking - web-based manager

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

<table>
<thead>
<tr>
<th>Host Check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV</td>
<td>Check for a running antivirus application recognized by the Windows Security Center.</td>
</tr>
<tr>
<td>FW</td>
<td>Check for a running firewall application recognized by the Windows Security Center.</td>
</tr>
<tr>
<td>AV-FW</td>
<td>Check for both an antivirus application and a firewall application recognized by the Windows Security Center.</td>
</tr>
<tr>
<td>Custom</td>
<td>Check for security applications that you choose from the VPN &gt; SSL &gt; Host Check page. See the Policy field.</td>
</tr>
<tr>
<td>None</td>
<td>Select to disable host checking.</td>
</tr>
</tbody>
</table>

5. Select OK.

To configure host checking - CLI

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

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

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

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

If you configure a custom host check for your web portal (see "Configuring host checking" on page 42), you choose security applications from the list on the VPN > SSL > Host Check page. The Host Check list includes default entries for many security software products. You can add, remove, or modify entries in this list.

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

1. Go to VPN > SSL > Host Check.
2. Select Create New and enter the following information:
   - **Name**: Enter a name for the application. The name does not need to match the actual application name.
   - **Type**: Select the type of security application. Can be AV for antivirus or FW for firewall.
   - **GUID**: Enter the Globally Unique IDentifier (GUID) for the host check application, if known. The GUID is usually in the form `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx`, where each x is a hexadecimal digit. Windows uses GUIDs to identify applications in the Windows Registry.
   - **Version**: The version of the security application.
   - **Add button**: If you do not know the GUID, add alternative checks for the application. The security software is considered found only if all checks succeed.
   - **Check Item entry**: These fields are available when you select the Add button.
     - **Type**: Select how to check for the application:
       - **File** — Look for a file. This could be the application’s executable file or any other file that would confirm the presence of the application. In File/Path, enter the full path to the file. Where applicable, you can use environment variables enclosed in percent (%) marks. For example, `%ProgramFiles%\Fortinet\FortiClient\FortiClient.exe`
       - **Process** — Look for the application as a running process. In Process, enter the application’s executable file name.
       - **Registry** — Search for a Windows Registry entry. In Registry, enter a registry item, for example `HKLM\SOFTWARE\Fortinet\FortiClient\Misc`
     - **Action**: Select one of
       - **Require** — If the item is found, the client meets the check item condition.
       - **Deny** — If the item is found, the client is considered to not meet the check item condition. Use this option if it is necessary to prevent use of a particular security product.
   - **MD5 Signatures**: If Type is File or Process, enter one or more known MD5 signatures for the application executable file. You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application.
3. Select OK.
4. Select OK.
### Configuring cache cleaning

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

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

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

1. Go to **VPN > SSL > Portal** and select the **Edit** icon for the web portal.
2. Select the **Settings** button.
3. Select the **Security Control** tab.
4. Select **Clean Cache**.
5. Select **OK**.
6. Select **Apply**.

**To enable cache cleaning - CLI**

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

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

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

### Configuring virtual desktop

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

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

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

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

1. Go to **VPN > SSL > Portal** and select the **Edit** icon for the web portal.
2. Select the **Settings** button.
3. Select the **Virtual Desktop** tab.
4. Select **Enable Virtual Desktop**.
5. Enable the other options as needed.
6. Optionally, select an Application Control List.
   
   See "Configuring virtual desktop application control".
Setting up the FortiGate unit

Configuring SSL VPN web portals

7 Select OK.
8 Select Apply.

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

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

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

There are two types of application control list:
- allow the listed applications and block all others
- block the listed applications and allow all others.

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

To create an Application Control List - web-based manager
1 Go to VPN > SSL > Virtual Desktop Application Control.
2 Enter a Name for the list.
3 Select one of the following:
   - Allow the applications on this list and block all others
   - Block the applications on this list and allow all others
4 Select Add.
5 Enter a Name for the application.
   This can be any name and does not have to match the official name of the application.
6 Enter one or more known MD5 Signatures for the application executable file.
   You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application.
7 Select OK.
8 Repeat steps 4 through 7 for each additional application.
9 Select OK.

To create an Application Control List - CLI
If, for example, you want to add BannedApp to List1, a list of blocked applications, you would enter:

```plaintext
config vpn ssl web virtual-desktop-app-list
edit "List1"
set action block
config apps
```
Configuring client OS Check

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

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

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

To configure OS Check - CLI

OS Check is configurable only in the CLI.

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>set os-check {disable</td>
<td>enable}</td>
<td>Enable or disable SSL VPN OS patch level check. Default disable.</td>
</tr>
<tr>
<td>config os-check-list {windows-2000</td>
<td>windows-xp</td>
<td>windows-vista}</td>
</tr>
<tr>
<td>set action {allow</td>
<td>check-up-to-date</td>
<td>deny}</td>
</tr>
<tr>
<td>set latest-patch-level {disable</td>
<td>0 - 255}</td>
<td>Specify the latest allowed patch level. Available when <code>action</code> is check-up-to-date.</td>
</tr>
<tr>
<td>set tolerance {tolerance_num}</td>
<td>Specify the allowable patch level tolerance. Lowest acceptable patch level equals latest-patch-level minus tolerance. Available when <code>action</code> is set to check-up-to-date.</td>
<td>0</td>
</tr>
</tbody>
</table>
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 can use a password defined on the FortiGate unit or optionally use established external authentication mechanisms such as RADIUS or LDAP.

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

Creating user accounts

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

For information about how to create RADIUS, LDAP, TACACS+ or PKI user accounts, see the “User” chapter of the FortiGate Administration Guide. For information about importing certificates, see the “System Certificates” chapter of the FortiGate Administration Guide. For information about certificate authentication, see the FortiGate Certificate Management User Guide.

To create a user account - web-based manager

1. Go to User > Local, select Create New, and enter the following information:

   **Figure 13: Creating a Local user**

   ![Image of user account creation](image)

   - **User Name**: Type or edit the remote user name (for example, User_1).
   - **Disable**: Select to prevent this user from authenticating.
   - **Password**: Select to authenticate this user using a password stored on the FortiGate unit, and then enter the password. The password should be at least six characters long.
   - **LDAP**: Select to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the list. You can select only an LDAP server that has been added to the FortiGate LDAP configuration.
   - **RADIUS**: Select to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the list. You can select only a RADIUS server that has been added to the FortiGate configuration.
   - **TACACS+**: Select to authenticate this user using a password stored on a TACACS+ server. Select the TACACS+ server from the list. You can select only a TACACS+ server that has been added to the FortiGate TACACS+ configuration.

2. Select OK.
To create a user account - CLI
If you want to create a user account, for example User_1 with the password "1_user", you would enter:

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

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

To create an SSL VPN user group - web-based manager
1. Go to User > Group, select Create New, and enter the following information:

   ![](Figure 14: Configuring an SSL VPN user group)

   **New User Group**
   - **Name**: Type or edit the user group name (for example, Web-only_group).
   - **Type**: Select the user group type - SSL VPN.
   - **Portal**: Select the SSL VPN web portal configuration to use with the User Group. For more information, see "Configuring SSL VPN web portals" on page 30.
   - **Available Users/Groups**: The list of Local users, RADIUS servers, LDAP servers, TACACS+ servers, or PKI users that can be added to the user group. To add a member to this list, select the name and then select the right arrow button.
   - **Members**: The list of Local users, RADIUS servers, LDAP servers, TACACS+ servers, or PKI users that belong to the user group. To remove a member, select the name and then select the left arrow button.

2. Select OK.

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

```
config user group
edit web_only
end
```
Setting up the FortiGate unit

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 47.

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

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

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

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

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

Figure 15: Example of firewall policies for SSL VPN

Configuring firewall addresses

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

For tunnel mode, you will already have defined firewall addresses for the IP address ranges that the FortiGate unit will assign to SSL VPN clients. See “Specifying an IP address range for tunnel-mode clients” on page 23.
The source address for your SSL VPN firewall policies will be the pre-defined “all” address. If this address is missing, you can add it. Both the address and the netmask are 0.0.0.0. The “all” address is used because VPN clients will be connecting from various addresses, not just one or two known networks. For improved security, if clients will be connecting from one or two known locations you should configure firewall addresses for those locations, instead of using the “all” address.

To create a firewall address

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

**Figure 16: Firewall address**

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Enter a name to identify the firewall address. Addresses, address groups, and virtual IPs must have unique names.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Subnet/IP Range.</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>Enter the firewall IP address in any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• an IP address and a subnet mask, separated by a slash, for example 172.16.10.0/255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>• a CIDR-format IP address with netmask, for example 172.16.10.0/24</td>
</tr>
<tr>
<td></td>
<td>• a single address, for example 172.16.10.3</td>
</tr>
<tr>
<td></td>
<td>• an IP address range, for example 172.16.10.[4-5]</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface, zone, or virtual domain (VDOM) link to which you want to bind the IP address. Select Any if you want to bind the IP address to the interface/zone when you create a firewall policy.</td>
</tr>
</tbody>
</table>

To create a firewall address - CLI

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

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

In the following example, there are firewall addresses defined for the protected network OfficeLAN and the SSL VPN tunnel user IP address range SSL_tunnel_users. You can also see the “all” preconfigured address.
Configuring the SSL VPN firewall policy

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

If you provide tunnel mode access, you will need a second firewall policy to permit traffic between the SSL VPN tunnel and the protected networks. See “Configuring the tunnel mode firewall policy” on page 55.

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

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

The SSL VPN firewall policy specifies:

• the source address that corresponds to the IP address of the remote user.

• the destination address that corresponds to the IP address or addresses that remote clients need to access.

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

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

• the level of SSL encryption to use and the authentication method

• which SSL VPN user groups can use the firewall policy

• the times (schedule) and types of services that users can access

• the protection profile and logging that are applied to the connection
To create an SSL-VPN firewall policy - web-based manager

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

Figure 18: Configuring a new SSL VPN firewall policy

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Select the name of the FortiGate network interface to that connects to the Internet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Select all.</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the FortiGate network interface that connects to the protected network.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select the firewall address you created that represents the networks and servers to which the SSL VPN clients will connect. If you want to associate multiple firewall addresses or address groups with the Destination Interface/Zone, from Destination Address, select Multiple. In the dialog box, move the firewall addresses or address groups from the Available Addresses section to the Members section, then select OK.</td>
</tr>
<tr>
<td>Action</td>
<td>Select SSL-VPN. This option is available only if there is at least one SSL-VPN user group.</td>
</tr>
<tr>
<td>SSL Client Certificate Restrictive</td>
<td>Allow access only to holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field. See “Enabling strong authentication through X.509 security certificates” on page 26.</td>
</tr>
<tr>
<td>Cipher Strength</td>
<td>Select the bit level of SSL encryption. The web browser on the remote client must be capable of matching the level that you select: Any, High &gt;= 164, or Medium &gt;= 128.</td>
</tr>
</tbody>
</table>
**User Authentication Method**

Select the authentication server type by which the user will be authenticated:

- **Local**
  For a local user group that will be bound to this firewall policy.

- **RADIUS**
  For remote clients that will be authenticated by an external RADIUS server.

- **LDAP**
  For remote clients that will be authenticated by an external LDAP server.

- **TACACS+**
  For remote clients that will be authenticated by an external TACACS+ server.

- **Any**
  Accept any of the above authentication methods. Local is attempted first, then RADIUS, then LDAP, then TACACS+.

**NAT**

Enable or disable Network Address Translation (NAT) of the source address and port. When NAT is enabled, you can also configure Dynamic IP Pool.

If you select a virtual IP as the Destination Address, but do not select the NAT option, the FortiGate unit performs destination NAT (DNAT) rather than full NAT. Source NAT (SNAT) is not performed.

If you enable NAT, the IP address of the outgoing interface of the FortiGate unit is used as the source address for new sessions started by SSL VPN.

**Comments**

Optionally, add information about the policy. The maximum length is 63 characters.

*Identity Based Policy* is automatically enabled for SSL VPN firewall policies. The following steps define the identity based policy.

3 Select Add.

The *New Authentication Rule* dialog box opens.

**Figure 19: New Authentication Rule**
4 Enter the following information:

**User Group**

- **Available User Groups** List of user groups available for inclusion in this authentication rule.
  - To add a user group to the list, select the name and then select the right arrow.
- **Selected User Groups** List of user groups that are included in this authentication rule.
  - To remove a user group from the list, select the name and then select the left arrow.

**Move Up**

**Move Down** Change the position of the selected group in the Selected User Groups list. The authentication rule checks each group in the list in descending order until it finds a group to which the user belongs.

**Service**

- **Available Services** List of available services to include in this authentication rule.
  - To add a service to the list, select the name of the service and then select the right arrow.
  - If the SSL VPN users can access all services, select the ANY service.
- **Selected Services** List of services that are included in the authentication rule.
  - To remove a service from the list, select the service name and then select the left arrow.

**Schedule**

Select a one-time or recurring schedule that controls when the policy is in effect.

- To make the SSL VPN always available, select the predefined always schedule.

**Protection Profile**

Optionally, you can apply a protection profile to this policy. For more information, see the FortiGate Administration Guide.

*Note:* Protection profiles apply only to tunnel-mode operations.

**Log Allowed Traffic**

Select to record messages to the traffic log whenever the policy processes a connection.

To log allowed traffic, you must also:

- enable traffic log for a logging location (syslog, WebTrends, local disk if available, memory, or FortiAnalyzer)
- set the logging severity level to Notification or lower using the Log and Report screen.

For more information see the Log&Report chapter of the FortiGate Administration Guide.

5 Select OK.

You can repeat the preceding two steps to add identity-based policies for other user groups as needed. If you have more than one SSL VPN web portal, you will have multiple user groups.

Your identity-based policies are listed in the firewall policy table. The FortiGate unit searches the table from the top down to find a policy to match the client's user group. Using the move icon in each row, you can change the order of the policies in the table to ensure the best policy will be matched first. You can also use the icons to edit or delete policies.
Figure 20: Identity-based policies to authenticate user groups

To create an SSL VPN firewall policy - CLI
To create the firewall policy shown in Figure 18 on page 52, enter the following CLI commands.

```bash
config firewall policy
edit 0
set srcintf port1
set dstintf port2
set srcaddr all
set dstaddr OfficeLAN
set action ssl-vpn
set nat enable
config identity-based-policy
edit 0
set groups SSL-VPN
set schedule always
set service ANY
end
end
```

Configuring the tunnel mode firewall policy
If your SSL VPN will provide tunnel mode operation, you need to create a firewall policy to enable traffic to pass between the SSL VPN virtual interface and the protected networks. This is in addition to the SSL VPN firewall policy that you created in the preceding section. Similar to an IPsec virtual interface, the SSL VPN virtual interface is the FortiGate unit end of the SSL tunnel that connects to the remote client. It is named `ssl.<vdom_name>`. In the root VDOM, for example, it is named `ssl.root`. If VDOMs are not enabled on your FortiGate unit, the SSL VPN virtual interface is also named `ssl.root`.

To configure the tunnel mode firewall policy - web-based manager
1. Go to Firewall > Policy and select Create New.
2. Enter the following information and select OK.

- **Source Interface/Zone**: Select the virtual SSL VPN interface, such as `ssl.root`.
- **Source Address**: Select the firewall address you created that represents the IP address range assigned to SSL VPN clients, such as `SSL_VPN_tunnel_users`.
- **Destination Interface/Zone**: Select the FortiGate network interface that connects to the protected network.
To configure the tunnel mode firewall policy - CLI

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

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

You must also add a static route for tunnel mode operation. See the following section.

### Configuring routing for tunnel mode

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

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

1. Go to **Router > Static** and select **Create New**.
2. Enter the following information and select **OK**.
   - **Destination IP/Mask**: Enter the Tunnel IP address range that you assigned to users of the web portal. See “Configuring tunnel mode settings” on page 35.
   - **Device**: Select the SSL VPN virtual interface, `ssl.root` for example.
   - **Distance**: Optionally you can set the distance on the SSL VPN higher than the default route to ensure only SSL VPN traffic uses this route.

Leave other settings at their default values.
To add the tunnel mode route - CLI

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

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

Adding an Internet browsing policy

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

To add an Internet browsing policy

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

   - **Source Interface/Zone**: Select the virtual SSL VPN interface, `ssl.root`, for example.
   - **Source Address**: Select the firewall address you created that represents the IP address range assigned to SSL VPN clients.
   - **Destination Interface/Zone**: Select the FortiGate network interface that connects to the Internet.
   - **Destination Address**: Select `all`.
   - **Action**: Select `Accept`.
   - **NAT**: Enable.
   - **Protection Profile**: Fortinet recommends selecting a protection profile to protect your clients.

   Leave other settings at their default values.

To configure the Internet browsing firewall policy - CLI

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

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

Enabling connection to an IPsec VPN

You might want to provide your SSL VPN clients access to another network, such as a branch office, that is connected by an IPsec VPN. To do this, you need only to add the appropriate firewall policy. For information about route-based and policy-based IPsec VPNs, see the [IPsec VPN Guide](http://docs.fortinet.com/).
To configure interconnection with a route-based IPsec VPN - web-based manager

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

   - **Source Interface/Zone**: Select the virtual SSL VPN interface, `ssl.root`, for example.
   - **Source Address**: Select the firewall address you created that represents the IP address range assigned to SSL VPN clients.
   - **Destination Interface/Zone**: Select the FortiGate network interface that connects to the Internet.
   - **Destination Address**: Select the address of the IPsec VPN remote protected subnet.
   - **Action**: Select ACCEPT.
   - **NAT**: Enable.
   - Leave other settings at their default values.

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

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

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

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

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

   - **Source Interface/Zone**: Select the virtual SSL VPN interface, `ssl.root`, for example.
   - **Source Address**: Select the firewall address you created that represents the IP address range assigned to SSL VPN clients.
   - **Destination Interface/Zone**: Select the FortiGate network interface that connects to the Internet.
   - **Destination Address**: Select the address of the IPsec VPN remote protected subnet.
   - **Action**: Select IPSEC.
   - **VPN tunnel**: Select the Phase 1 configuration name of your IPsec VPN.
   - **Allow inbound**: Enable
   - **Allow outbound**: Enable
   - **NAT inbound**: Enable
   - Leave other settings at their default values.
To configure interconnection with a policy-based IPsec VPN - CLI

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

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

In this example, port1 is connected to the Internet.

Viewing SSL VPN logs

You can view SSL VPN logs on your FortiGate unit. For information about how to interpret log messages, see the FortiGate Log Message Reference.

To enable logging - web-based manager

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 expand arrow beside each option to reveal and configure associated settings.
4. If logs will be written to system memory, from the Log Level list, select Information. For more information, see the “Log & Report” chapter of the FortiGate Administration Guide.
5. Select Apply.

To enable logging - CLI

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

For some log locations, there are additional options that you can set.
To enable logging of SSL VPN events - web-based manager

2. Select Enable, and then select one or more of the following options:
   - SSL VPN user authentication event
   - SSL VPN administration event
   - SSL VPN session event
3. Select Apply.

To enable logging of SSL VPN events - CLI

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

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

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

To enable logging of SSL VPN traffic - CLI

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

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

To view SSL VPN logs - web-based manager

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

   In event log entries look for the sub-types “sslvpn-session” and “sslvpn-user”. In the traffic logs, look for the sub-type “allowed”. For web-mode traffic, the source is the host IP address. For tunnel-mode traffic, the source is the address assigned to the host from the SSL VPN address pool.
To view SSL VPN logs - CLI

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

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the command
execute log filter start-line 1

Monitoring active SSL VPN sessions

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

To monitor SSL VPNs - web-based manager

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

Figure 21: SSL VPN monitor list

<table>
<thead>
<tr>
<th>No.</th>
<th>User</th>
<th>Source IP</th>
<th>Begin Time</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSL</td>
<td>172.20.120.42</td>
<td>Tue Feb 6 09:08:10 2007</td>
<td>Subsession</td>
<td>Tunnel IP: 10.200.260.0</td>
</tr>
</tbody>
</table>

No. | The connection identifiers.
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 the services provided by an SSL VPN tunnel session.
Subsession
Tunnel IP: IP address that the FortiGate unit assigned to the remote client.
Delete icon: Delete current subsession.
Action | Delete a web session.

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 22).

Figure 22: SSL VPN monitor list - Tunnel-mode user

<table>
<thead>
<tr>
<th>No.</th>
<th>User</th>
<th>Source IP</th>
<th>Begin Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User_4</td>
<td>172.20.120.20</td>
<td>Tue Aug 23 10:26:34 2005</td>
<td>Web Application:TELNET 10.10.10.10</td>
</tr>
</tbody>
</table>
Subsession
Subsession
Tunnel IP: 10.10.264.1 |

Delete

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

To monitor SSL VPNs - web-based manager

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

```
get vpn ssl monitor
```

To delete tunnel-mode or web-mode sessions:

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

<table>
<thead>
<tr>
<th>No response from SSL VPN URL</th>
<th>Check that SSL VPN is enabled. Check SSL VPN port assignment (default 10443). Check SSL VPN firewall policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error: “The web page cannot be found.”</td>
<td>Check URL: https://&lt;FortiGate_IP&gt;:&lt;SSLVPN_port&gt;/remote/login</td>
</tr>
<tr>
<td>Tunnel connects, but there is no communication.</td>
<td>Check that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface. See “Configuring routing for tunnel mode” on page 56.</td>
</tr>
</tbody>
</table>
| Tunnel-mode connection shuts down after a few seconds | This issue occurs when there are multiple interfaces connected to the Internet, for example, a dual WAN configuration. Upgrade the FortiGate unit firmware to at least v3.0 MR4 or higher, then use the following CLI command:  
```
config vpn ssl settings
set route-source-interface enable
end
```
| Error: “Destination address of Split Tunneling policy is invalid.” | The SSL VPN firewall policy uses the ALL address as its destination. Specify the address of the protected network instead. |
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
- Web portal overview
- Using the Bookmarks widget
- Using the Connection Tool
- Tunnel-mode features
- Using the SSL VPN Virtual Desktop

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/login).

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

   A second message may be displayed to inform you that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. You can ignore the message.

2. When you are prompted for your user name and password:
   - In the Name field, type your user name.
   - In the Password field, type your password.

3. Select Login.

   The FortiGate unit will redirect your web browser to the FortiGate SSL VPN web portal home page automatically.
Web portal overview

After you log in, you see a web portal page like the following:

Figure 23: FortiGate SSL VPN web portal page

Four “widgets” provide the web portal’s features:

- **Session Information** displays the elapsed time since login and the volume of HTTP and HTTPS traffic, both inbound and outbound.
- **Bookmarks** provides links to network resources. You can use the administrator-defined bookmarks and you can add your own bookmarks. See “Using the Bookmarks widget” on page 65.
- **Connection Tool** enables you to connect to network resources without using or creating a bookmark.
- **Tunnel Mode** connects and disconnects the tunnel mode SSL connection to the FortiGate unit. While the tunnel is active, the widget displays the amount of data that is sent and received. For more information, see “Tunnel-mode features” on page 74.

Tunnel mode requires a downloadable client application. If your computer is running Microsoft Windows, the Tunnel Mode widget provides a download link if you need to install the client on your computer. If you are using Macintosh or Linux, you can obtain and install an appropriate client application from the Fortinet Support site. For more information, see “Downloading the SSL VPN tunnel mode client” on page 78.

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

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

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

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

Depending on the web portal configuration and user group settings, one or more of the following server applications are available to you through Bookmarks or the Connection Tool:

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

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

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

Using the Bookmarks widget

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

Figure 24: Bookmarks widget

The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the My Bookmarks list. For more information, see "Adding bookmarks" on page 66.

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. For more information, see "Using the Connection Tool" on page 67.
Adding bookmarks

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

To add a bookmark

1. In the Bookmarks widget, select Add.
2. Enter the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name to display in the Bookmarks list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the abbreviated name of the server application or network service from the drop-down list.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the IP address or FQDN of the server application or network service. For RDP connections, you can append some parameters to control screen size and keyboard layout. See “To start an RDP session” on page 70.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally enter a short description. The description displays when you pause the mouse pointer over the hyperlink.</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On (SSO) is available for HTTP/HTTPS bookmarks only. <strong>Disabled</strong> — This is not an SSO bookmark. <strong>Automatic</strong> — Use your SSL VPN credentials or an alternate set. See the SSO Credentials field. <strong>Static</strong> — Supply credentials and other required information (such as an account number) to a web site that uses an HTML form for authentication. You provide a list of the form field names and the values to enter into them. This method does not work for sites that use HTTP authentication, in which the browser opens a pop-up dialog box requesting credentials.</td>
</tr>
</tbody>
</table>

   **SSO fields**

   **SSO Credentials**

   | Field Name | Enter the field name, as it appears in the HTML form. |
   | Value      | Enter the field value. To use the values from SSO Credentials, enter %passwd% for password or %username% for username. |

3. Select OK and then select Done.
Using the Connection Tool

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

See the following procedures:

• “To connect to a web server” on page 67
• “To ping a host or server behind the FortiGate unit” on page 67
• “To start a telnet session” on page 67
• “To start an FTP session” on page 68
• “To start an SMB/CIFS session” on page 69
• “To start an SSH session” on page 70
• “To start an RDP session” on page 70
• “To start a VNC session” on page 73

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

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

To connect to a web server

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

To ping a host or server behind the FortiGate unit

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

To start a telnet session

1. In Type, select Telnet.
2. In the Host field, type the IP address of the telnet host.
   - For example: 10.11.101.12
3 Select Go.
A Telnet window opens.

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

To start an FTP session
1 In Type, select FTP.
2 In the Host field, type the IP address of the FTP server. For example: 10.11.101.12
3 Select Go.
A login window opens.
4 Enter your user name and password and then select Login.
You must have a user account on the remote host to log in.

Figure 25: An FTP session
5 Manipulate the files in any of the following ways:
   • To download a file, select the file link in the Name column.
   • To access a subdirectory (Type is Folder), select the link in the Name column.
   • To create a subdirectory in the current directory, select New directory.
   • To delete a file or subdirectory from the current directory, select its Delete icon.
   • To rename a file in the current directory, select its Rename icon.
   • To upload a file from the current directory from your client computer, select Upload.
   • When the current directory is a subdirectory, you can select Up to access the parent directory.

6 To end the FTP session, select Logout.

To start an SMB/CIFS session
1 In Type, select SMB/CIFS.
2 In the Host field, type the IP address of the SMB or CIFS server.
   For example: 10.11.101.12
3 Select Go.
   A login window opens.
4 Enter your user name and password and then select Login.
   You must have a user account on the remote host to log in.

5 Manipulate the files in any of the following ways:
   • To download a file, select the file link in the Name column.
   • To access a subdirectory (Type is Folder), select the file link in the Name column.
   • To create a subdirectory in the current directory, select New Directory.
   • To delete a file or subdirectory from the current directory, select its Delete icon.
   • To rename a file, select its Rename icon.
   • To upload a file from your client computer to the current directory, select Upload.
   • When the current directory is a subdirectory, you can select Up to access the parent directory.

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

1. In Type, select SSH.
2. In the Host field, type the IP address of the SSH host.
   For example: 10.11.101.12
3. Select Go.
   A login window opens.
4. Select Connect.
   A SSH session starts and you are prompted to log in to the remote host. You must have a user account to log in. After you log in, you may enter any series of valid commands at the system prompt.

5. To end the session, select Disconnect (or type exit) and then close the SSH connection window.

To start an RDP session

1. In Type, select RDP.
2. In the Host field, type the IP address of the RDP host.
   For example: 10.11.101.12
3. Optionally, you can also specify language and locale by adding the -m parameter,
   For example: 10.11.101.12 -m fr
   Select the locale 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:

<table>
<thead>
<tr>
<th>Code</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>ar</td>
<td>Arabic</td>
</tr>
<tr>
<td>da</td>
<td>Danish</td>
</tr>
<tr>
<td>de</td>
<td>German</td>
</tr>
<tr>
<td>de-ch</td>
<td>Swiss German</td>
</tr>
<tr>
<td>en</td>
<td>English</td>
</tr>
<tr>
<td>en-us</td>
<td>English, US</td>
</tr>
<tr>
<td>es</td>
<td>Spanish</td>
</tr>
<tr>
<td>fi</td>
<td>Finnish</td>
</tr>
<tr>
<td>fr</td>
<td>French</td>
</tr>
<tr>
<td>fr-be</td>
<td>Belgian French</td>
</tr>
<tr>
<td>fr-ch</td>
<td>Swiss French</td>
</tr>
<tr>
<td>hr</td>
<td>Croatian</td>
</tr>
<tr>
<td>it</td>
<td>Italian</td>
</tr>
<tr>
<td>ja</td>
<td>Japanese</td>
</tr>
<tr>
<td>ja-ja</td>
<td>Japanese, Japan</td>
</tr>
<tr>
<td>de-de</td>
<td>German, Germany</td>
</tr>
<tr>
<td>mk</td>
<td>Macedonian</td>
</tr>
<tr>
<td>no</td>
<td>Norwegian</td>
</tr>
<tr>
<td>pt</td>
<td>Portuguese</td>
</tr>
<tr>
<td>pt-br</td>
<td>Brazilian Portuguese</td>
</tr>
<tr>
<td>ru</td>
<td>Russian</td>
</tr>
<tr>
<td>sl</td>
<td>Slovenian</td>
</tr>
<tr>
<td>sv</td>
<td>Sudanese</td>
</tr>
<tr>
<td>sr</td>
<td>Serbian</td>
</tr>
<tr>
<td>tr</td>
<td>Turkish</td>
</tr>
</tbody>
</table>

Please enter SSH user name and password:

User Name: 
Password: 
OK Cancel
4 Optionally, you can specify the screen resolution.
   Add \(-f\) to run RDP full-screen. For example: \(10.11.101.12\ -f\)
   Add \(-g\ <\text{width}>x<\text{height}>\) to specify the screen size in pixels.
   For example: \(10.11.101.12\ -g\ 800x600\)

5 Select Go.
   A login window opens.

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

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

9 To end the RDP session, Log out of Windows or select Cancel from the Logon window.
To start a VNC session

1. In Type, select VNC.
2. In the Host field, type the IP address of the VNC host.
   For example: 10.11.101.12
3. Select Go.
   A login window opens.
4. Type your user name and password when prompted to log in to the remote host.
   You must have a user account on the remote host to log in.
5. Select OK.
6. To end the VNC session, close the VNC window.
Tunnel-mode features

For Windows users, the web portal Tunnel Mode widget provides controls for your tunnel mode connection and also provides status and statistics about its operation. You can also control and monitor tunnel mode operation from the standalone client application. For more information, see "Using the tunnel mode client" on page 80.

Figure 26: Fortinet SSL VPN tunnel mode widget

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

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

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

You can use the virtual desktop just as you use your regular desktop, subject to the limitations that virtual desktop application control imposes. See “Configuring virtual desktop application control” on page 45.

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

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

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

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

The following topics are included in this section:

• Client configurations
• Downloading the SSL VPN tunnel mode client
• Installing the tunnel mode client
• Using the tunnel mode client
• Uninstalling the tunnel mode client

Client configurations

There are several configurations of SSL VPN applications available.

• web mode
• tunnel mode
• virtual desktop

Web mode

SSL VPN web mode requires nothing more than a web browser. Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari browsers are supported. See “Web-only mode client requirements” on page 17 for detailed requirements.

Tunnel mode

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

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

If your computer runs Linux or Mac OS X, you can obtain an appropriate tunnel mode client application from the Fortinet Support web site. See “Tunnel-mode client requirements” on page 18 for the specific operating system versions that are supported.

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

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

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

Downloading the SSL VPN tunnel mode client

SSL VPN standalone tunnel client applications are available for Windows, Linux, and Mac OS X systems (see “Tunnel-mode client requirements” on page 18 for the specific versions that are supported). There are separate download files for each operating system.

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

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

To download the SSL VPN tunnel client

2. Select Firmware Images and then FortiGate.
   The Support FTP site opens.
3. Select v4.00 and then select the latest firmware release, 4.0MR2, for example.
   The list of firmware images opens.
4. Select SSL VPN Clients.
5. Select the appropriate client.
   Windows: SslvpnClient.exe or SslvpnClient.msi
   Linux: forticlientsslvpn_linux_<version>.tar.gz
   Mac OS X: forticlientsslvpn_macosx_<version>.dmg

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

Follow the instructions for your operating system.

Windows

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

Linux

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

When you run the install program for the first time, you will have to set up system parameters (root privileges) before you run the program or before other users without administrator privileges can use the application.

2. In the First Run dialog, select OK.
   The command line terminal window opens.

3. If you are asked for your password, enter it.
   The License Agreement dialog appears in the command line terminal window.

4. Read the License Agreement and enter Yes to accept it.
   The FortiClient SSL VPN tunnel client (Linux) opens. You can begin using the application immediately or close it.

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

MAC OS client

1. Double-click on the forticlientsslvpn_macosx_<version>.dmg file.
   The Mac mounts the disk image as forticlientsslvpn.

2. Double-click the forticlientsslvpn.pkg file inside the disk image and follow the instructions.
   The application installs the program forticlientsslvpn.app in the Applications folder.

3. Unmount the disk image by selecting the disk image file forticlientsslvpn_macosx_<version>.dmg and dragging it into the Trash.
Using the tunnel mode client

Follow the instructions for your operating system.

**Windows client**

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

1. Go to **Start > All Programs > FortiClient > FortiClient SSL VPN**.

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

   - **Connection Name**: If you have pre-configured the connection settings, select the connection from the list and then select **Connect**. Otherwise, enter the settings in the fields below.
     To pre-configure connection settings, see “To configure tunnel client settings (Windows)” on page 81.

   - **Server Address**: Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN.

   - **Username**: Enter your user name.

   - **Password**: Enter the password associated with your user account.

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

   - **Connection Status**: Connected or Disconnected

     - **Duration**: Hours, minutes, seconds since session started
     - **Bytes Sent / Bytes Received**: amount of data transferred

   - **Settings...**: Select to open the **Settings** dialog. See “To configure tunnel client settings (Windows)” on page 81.

   - **Connect**: Start tunnel mode operation.

   - **Disconnect**: Stop tunnel mode operation.

   - **Exit**: Close the tunnel mode client application.
To configure tunnel client settings (Windows)

1. Go to Start > All Programs > FortiClient > FortiClient SSL VPN.
2. Select Settings....
3. Select New Connection, or select an existing connection and then select Edit.
4. Enter the Connection Name.
5. Enter the connection information. You can also enter a Description. Select OK.
6. Optionally, select Keep connection alive until manually stopped to prevent tunnel connections from closing due to inactivity.
7. Select OK.
Linux client

To use the SSL VPN standalone tunnel client (Linux)

1 Go to the folder where you installed the Linux tunnel client application and double-click on ‘forticlientsslvpn’.

   The FortiClient SSL VPN tunnel client opens.

   ![FortiClient SSL VPN tunnel client interface]

<table>
<thead>
<tr>
<th>Connection:</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server:</td>
<td></td>
</tr>
<tr>
<td>User:</td>
<td></td>
</tr>
<tr>
<td>Password:</td>
<td></td>
</tr>
<tr>
<td>Certificate:</td>
<td></td>
</tr>
<tr>
<td>Password:</td>
<td></td>
</tr>
</tbody>
</table>

   ![Connection status]

<table>
<thead>
<tr>
<th>Connection:</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server:</td>
<td>172.20.120.141:10443</td>
</tr>
<tr>
<td>Status:</td>
<td>Tunnel running</td>
</tr>
<tr>
<td>Receive bytes:</td>
<td>225</td>
</tr>
<tr>
<td>Send bytes:</td>
<td>1.690 K</td>
</tr>
</tbody>
</table>

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

   **Connection**
   - If you have pre-configured the connection settings, select the connection from the list and then select Connect. Otherwise, enter the settings in the fields below.
   - To pre-configure connection settings, see “To configure tunnel client settings (Windows)” on page 81.

   **Server**
   - Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN.
   - In the smaller field, enter the SSL VPN port number (default 10443).

   **User**
   - Enter your user name.

   **Password**
   - Enter the password associated with your user account.

   **Certificate**
   - Use this field if the SSL VPN requires a certificate for authentication.
   - Select the certificate file (PKCS#12) from the drop-down list, or select the Browse (...) button and find it.

   **Password**
   - Enter the password required for the certificate file.

   **Settings...**
   - Select to open the Settings dialog. See “To configure tunnel client settings (Linux)” on page 83.

   **Connect**
   - Start tunnel mode operation.

   **Stop**
   - Stop tunnel mode operation.
To configure tunnel client settings (Linux)

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

2. Select Settings....

3. Optionally, select Keep connection alive until manually stopped to prevent tunnel connections from closing due to inactivity.

4. Optionally, select Start connection automatically. The next time the tunnel mode application starts, it will start the last selected connection.

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

6. Select the + button to define a new connection, or select from the list an existing connection to modify.
   
   For a new connection, the Connection window opens. For an existing connection, the current settings appear in the Settings window and you can modify them.

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

   See “To use the SSL VPN standalone tunnel client (Linux)” on page 82 for information about the fields.

8. Select Done.
MAC OS X client

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

1  Go to the Applications folder and double-click on forticlientsslvpn.app.
   The FortiClient SSL VPN tunnel client (Mac OS X) opens.

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

   **Connection**
   - If you have pre-configured the connection settings, select the connection from the list and then select Connect. Otherwise, enter the settings in the fields below.
   - To pre-configure connection settings, see “To configure tunnel client settings (Mac OS X)” on page 85.

   **Server**
   - Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN. In the smaller field, enter the SSL VPN port number (default 10443).

   **User**
   - Enter your user name.

   **Password**
   - Enter the password associated with your user account.

   **Certificate**
   - Use this field if the SSL VPN requires a certificate for authentication. Select the certificate file (PKCS#12) from the drop-down list, or select the Browse (...) button and find it.

   **Password**
   - Enter the password required for the certificate file.

   **Settings...**
   - Select to open the Settings dialog. See “To configure tunnel client settings (Mac OS X)” on page 85.

   **Connect**
   - Start tunnel mode operation.

   **Stop**
   - Stop tunnel mode operation.
To configure tunnel client settings (Mac OS X)

1. Go to the Applications folder and double-click on forticlientsslvpn.app. The FortiClient SSL VPN tunnel client (Mac OS X) opens.

2. Select Settings.

3. Optionally, select Keep connection alive until manually stopped to prevent tunnel connections from closing due to inactivity.

4. Optionally, select Start connection automatically. The next time the tunnel mode application starts, it will start the last selected connection.

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

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

To uninstall from Windows

1. In the Control Panel, select Programs and Features (Add or Remove Programs in Windows XP).
2. Select FortiClient SSL VPN and then Remove.

To uninstall from Linux

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

To uninstall from Mac OS X

In the Applications folder, select forticlientsslvpn.app and drag it into the Trash. After you empty the Trash folder, the installed program is removed from the user computer.
Examples

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

At the FortiGate unit, you configure user groups and 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.

This section contains the following topics:

- Basic SSL VPN example
- Multiple user groups with different access permissions example

Basic SSL VPN example

A common application for an SSL VPN is to provide access to the office network for employees traveling or working from home. For example, Figure 27 shows a FortiGate gateway (FortiGate_1) that connects the office network to the Internet. Users on the office network have access to the Internet, but access to the office network from the Internet is available only to authenticated users of the SSL VPN.

Figure 27: Example SSL VPN configuration
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.
- For client requirements, see “Web-only mode client requirements” on page 17 and “Tunnel-mode client requirements” on page 18.

General configuration steps

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

Creating the firewall addresses

In FortiOS 4.0, firewall policies do not accept direct entry of IP addresses and address ranges. You must define firewall addresses in advance.

Creating the destination address

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

To define destination addresses - web-based manager

1. Go to Firewall > Address.
2. Select Create New, enter the following information, and select OK:
   
<table>
<thead>
<tr>
<th>Address Name</th>
<th>OfficeLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.101.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>port2</td>
</tr>
</tbody>
</table>

To define destination addresses - CLI

```
config firewall address
edit OfficeLAN
   set type ipmask
   set subnet 10.11.101.0/24
   set associated-interface port2
end
```
Creating the tunnel client range address

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

To define tunnel client addresses - web-based manager

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

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Type</th>
<th>Subnet / IP Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_tunnel_users</td>
<td>Subnet / IP Range</td>
<td>10.11.254.0/24</td>
</tr>
<tr>
<td>Any</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To define destination addresses - CLI

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

Enabling SSL VPN and setting the tunnel user IP address range

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

To enable SSL VPN and set tunnel address range - web-based manager

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

To enable SSL VPN and set tunnel address range - CLI

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

Creating the web portal

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

To create the portal1 web portal

1. Go to VPN > SSL > Portal and select Create New.
2. In the Name field, enter portal1.
3. In Applications, select the application types to permit.
4 Select OK, then select OK again.

To create the web portals - CLI

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

Creating the user account and user group

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

To create the user account - web-based manager

1 Go to User > Local and select Create New.
2 In User Name, enter user1.
3 Select Password and enter the password in the field on the right.
4 Select OK.

To create the user account - CLI

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

To create the user group - web-based manager

1 Go to User > User Group.
2 Select Create New and enter the following information:

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

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

To create the user group - CLI

```
config user group
edit group1
  set group-type sslvpn
  set member user1
  set sslvpn-portal portall
end
```
Creating the firewall policies

You need to define firewall policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected network behind the FortiGate unit. Before you create the firewall policies, you must define the source and destination addresses to include in the policy. See “Creating the firewall addresses” on page 88.

Two types of firewall policy are required:

- An SSL VPN policy enables clients to authenticate and permits a web-mode connection to the destination network. The authentication, ensures that only authorized users access the destination network.

- A tunnel-mode policy is a regular ACCEPT firewall policy that enables traffic to flow between the SSL VPN tunnel interface and the protected network. A tunnel-mode policy is required if you want to provide a tunnel-mode connection for your clients.

To create the SSL VPN firewall policy - web-based manager

1. Go to Firewall > Policy.
2. Select Create New and enter the following information:
   - Source Interface/Zone: port1
   - Source Address: All
   - Destination Interface/Zone: port2
   - Destination Address: OfficeLAN
   - Action: SSL-VPN
   - User Authentication Method: Local
   - NAT: Enable

3. Select Add and enter the following information:
   - User Group: group1
   - Service: Any
   - Schedule: always

4. Select OK, and then select OK again.

To create the SSL VPN firewall policy - CLI

```bash
config firewall policy
edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr all
    set dstaddr OfficeLAN
    set action ssl-vpn
    set nat enable
config identity-based-policy
edit 1
    set groups group1
    set schedule always
    set service ANY
end
end
```
To create the tunnel-mode firewall policy - web-based manager

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

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

To create the tunnel-mode firewall policy - CLI

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

Add routing to tunnel mode clients

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

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

1. Go to Router > Static > Static Route and select Create New.
2. Enter the following information and select OK.

   - Destination IP/Mask: 10.11.254.0/24
     This is the IP address range that you assigned to users of the web portal. See “Creating the tunnel client range address” on page 89.
   - Device: Select the SSL VPN virtual interface, ssl.root for example.
     Leave other settings at their default values.

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

```bash
config router static
edit 0
   set device ssl.root
   set dst 10.11.254.0/24
end
```
Multiple user groups with different access permissions example

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

Figure 28: SSL VPN configuration for different access permissions by user group

In this example configuration, there are two users:
- user1 can access the servers on Subnet_1
- user2 can access the workstation PCs on Subnet_2

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

General configuration steps

1. Create firewall addresses for
   - the destination networks
   - two non-overlapping tunnel IP address ranges that the FortiGate unit will assign to tunnel clients in the two user groups

2. Create two web portals.

3. Create two user accounts, user1 and user2.
4 Create two user groups. For each group, add a user as a member and select a web portal. In this example, user1 will belong to group1, which will be assigned to portal1.

5 Create firewall policies:
   • two SSL VPN firewall policies, one to each destination
   • two tunnel-mode policies to allow each group of users to reach its permitted destination network

6 Create the static route to direct packets for the users to the tunnel.

Creating the firewall addresses

In FortiOS 4.0, firewall policies do not accept direct entry of IP addresses and address ranges. You must define firewall addresses in advance.

Creating the destination addresses

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

To define destination addresses - web-based manager

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

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

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

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

To define destination addresses - CLI

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

Creating the tunnel client range addresses

To accommodate the two groups of users, split an otherwise unused subnet into two ranges. The tunnel client addresses must not conflict with each other or with other addresses in your network.
To define tunnel client addresses - web-based manager

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

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

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

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Tunnel_group2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.254.[51-100]</td>
</tr>
<tr>
<td>Interface</td>
<td>Any</td>
</tr>
</tbody>
</table>

To define tunnel client addresses - CLI

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

Creating the web portals

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

To create the portal1 web portal

1. Go to VPN > SSL > Portal and select Create New.
2. Enter portal1 in the Name field and select OK.
3. In Applications, select all of the application types that the users can access.
4. Select the Edit icon on the Tunnel Mode widget.
5. In IP Pools, select Edit.
6. In the Available list, select Tunnel_group1 and then select the down arrow button. Select OK.
7. Select OK in the Tunnel Mode widget.
8. Select OK.

To create the portal2 web portal

1. Go to VPN > SSL > Portal and select Create New.
2. Enter portal2 in the Name field and select OK.
3. In Applications, select all of the application types that the users can access.
4. Select the Edit icon on the Tunnel Mode widget.
5. In IP Pools, select Edit.
6. In the Available list, select Tunnel_group2 and then select the down arrow button. Select OK.
7. Select OK in the Tunnel Mode widget.
8. Select OK.

To create the web portals - CLI

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

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

Creating the user accounts and user groups

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

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

To create the user groups - web-based manager

2. Select Create New and enter the following information:

   - Name: group1
   - Type: SSL VPN
   - Portal: portal1

3. From the Available list, select user1 and move it to the Members list by selecting the right arrow button.
Figure 29: group1 user group attributes

4 Select OK.
5 Repeat steps 2 through 4 to create group2, assigned to portal2, with user2 as its only member.

To create the user groups - CLI

```
config user group
edit group1
set group-type sslvpn
set member user1
set sslvpn-portal portal1
next
edit group2
set group-type sslvpn
set member user2
set sslvpn-portal portal2
end
```

Creating the firewall policies

You need to define firewall policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected networks behind the FortiGate unit. Before you create the firewall policies, you must define the source and destination addresses to include in the policy. See “Creating the firewall addresses” on page 94.

Two types of firewall policy are required:

- An SSL VPN policy enables clients to authenticate and permits a web-mode connection to the destination network. In this example, there are two destination networks, so there will be two SSL VPN policies. The authentication, ensures that only authorized users access the destination network.

- A tunnel-mode policy is a regular ACCEPT firewall policy that enables traffic to flow between the SSL VPN tunnel interface and the protected network. Tunnel-mode policies are required if you want to provide tunnel-mode connections for your clients. In this example, there are two destination networks, so there will be two tunnel-mode policies.
To create the SSL VPN firewall policies - web-based manager

1. Go to Firewall > Policy.
2. Select Create New and enter the following information:
   - Source Interface/Zone: port1
   - Source Address: All
   - Destination Interface/Zone: port2
   - Destination Address: Subnet_1
   - Action: SSL-VPN
   - User Authentication Method: Local
   - NAT: Enable
3. Select Add and enter the following information:
   - User Group: group1
   - Service: Any
4. Select OK, and then select OK again.
5. Select Create New and enter the following information:
   - Source Interface/Zone: port1
   - Source Address: All
   - Destination Interface/Zone: port3
   - Destination Address: Subnet_2
   - Action: SSL-VPN
   - User Authentication Method: Local
   - NAT: Enable
6. Select Add and enter the following information:
   - User Group: group2
   - Service: Any
7. Select OK, and then select OK again.

To create the SSL VPN firewall policies - CLI

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

Multiple user groups with different access permissions example

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

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

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

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

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

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

To create the tunnel-mode firewall policies - CLI

config firewall policy
   edit 0
   set srcintf ssl.root
   set dstintf port2
   set srcaddr Tunnel_group1
   set dstaddr Subnet_1
   set action accept
   set schedule always
   set service ANY
   set nat enable
next
   edit 0
   set srcintf ssl.root
   set dstintf port3
   set srcaddr Tunnel_group2
Create the static route to tunnel mode clients

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

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

1. Go to Router > Static > Static Route and select Create New.
2. Enter the following information and select OK.
   - Destination IP/Mask: 10.11.254.0/24
     This IP address range covers both ranges that you assigned to SSL VPN tunnel-mode users. See “Creating the tunnel client range addresses” on page 94.
   - Device: Select the SSL VPN virtual interface, ssl.root for example.
     Leave other settings at their default values.

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

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

Enabling SSL VPN operation

By default, SSL VPN is not enabled.

To enable SSL VPN - web-based manager

1. Go to VPN > SSL > Config.
2. Ensure that Enable SSL-VPN is selected.
3. Select Apply.

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

The following example shows how you would add an OS check to the g1portal web portal. This OS check accepts all Windows XP users and Windows 2000 users running patch level 2.

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

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

Symbols
%passwd%, 66
%username%, 66

A
adding bookmarks, 66
Address Name
firewall address, 50
authentication timeout setting, 25

B
bookmarks
user-defined, 66
bookmarks, web-portal, 65

C
cache cleaner
introduction, 17
certificates
self signed, 63
cipher suite, SSL negotiations, 25
client
downloading, 78
using Linux, 82
using Mac OS, 84
using Windows, 80
client requirements
tunnel mode, 18
web-only mode, 17
comments
firewall policy, 53, 56
comments, documentation, 8
configuration, general steps, 21
connecting
to FTP server, 68
to PC by RDP, 70
to PC by VNC, 73
to secure HTTP gateway, 63
to SMB/CIFS file share, 69
to SSH server, 70
to telnet server, 67
to web portal, 63
to web server, 67
to web-based manager, 22
Connection Tool
using, 67
connections
defining bookmarks to, 66
connectivity, testing for, 67
customer service, 8

D
deployment topology, 16, 88
destination
firewall policy, 52, 55, 57, 58, 91, 92, 98, 99
destination NAT (DNAT), 53
documentation
commenting on, 8
Fortinet, 8
downloading
tunnel client, 78

E
example
complex SSL VPN, 93
OS patch check, 101

F
firewall address
address name, 50
IP range/subnet, 50
subnet, 50
firewall policy
comments, 53, 56
destination, 52, 55, 57, 58, 91, 92, 98, 99
log traffic, 54
protection profile, 54
source, 52, 55, 57, 58, 91, 92, 98, 99
web-only mode access, 49
FortiGate documentation
commenting on, 8
Fortinet customer service, 8
Fortinet documentation, 8
Fortinet Knowledge Center, 8
FTP server, connecting to, 68

H
home page, web portal features, 64
host check
introduction, 17
OS, 46
host OS
patch check, 46

I
idle timeout setting, 25
infrastructure requirements, 16, 88
overall, 16, 88
tunnel-mode clients, 18
installation
note re installation on Vista, 19
introduction
  deployment topology, 16
  Fortinet documentation, 8
  general configuration steps, 21
IP address range, tunnel mode, 23
IP range/subnet
  firewall address, 50
IPSec VPN
  comparison to SSL, 14

K
  keyboard
    for RDP connection, 70

L
  language
    for RDP connection, 70
  locale
    for RDP connection, 70
  log
    traffic, firewall policy, 54
  logging
    enabling SSL VPN events, 60
    setting event-logging parameters, 59
    viewing SSL VPN logs, 60, 61
  logging in
    to FortiGate secure HTTP gateway, 63

M
  modes of operation
    overview, 16
    tunnel mode, 18
    web-only mode, 17

N
  network configuration, 16, 88
    recommended, 16

O
  OS
    host patch check, 46
  OS patch check
    example, 101

P
  patch check
    host OS, 46
  ping host from remote client, 67
  policy
    comments, 53, 56
    log traffic, 54
    protection profile, 54
  port number
    for web-portal connections, 27
  protection profile
    firewall policy, 54

R
  RDP
    setting locale, 70
    setting screen resolution, 71
  RDP session, establishing, 70
  replacement message, to customize web portal login page, 28

S
  screen resolution
    for RDP connection, 71
  security
    choosing security level, 14
  Single Sign On (SSO)
    bookmarks, 66
  Single Sign-on (SSO)
    adding SSO bookmark (user), 66
      overview, 19
  SMB/CIFS file share
    connecting to, 69
  source
    firewall policy, 52, 55, 57, 58, 91, 92, 98, 99
  source NAT (SNAT), 53
  SSH server, connecting to, 70
  SSL VPN
    configuration overview, 21
    default web portal, 32
    downloading client, 78
    enabling, 100
    event logging, 59
    host OS patch check, 46
    using Linux client, 82
    using Mac OS client, 84
    using Windows client, 80
    Virtual Desktop, 78
  SSL VPN web portal, 30
    default, 32
  SSLv2 support
    note regarding, 18
  subnet
    firewall address, 50

T
  technical support, 8
  telnet server, connecting to, 67
  tunnel mode, 18
  client requirements, 18
  configuring FortiGate server, 55
  IP address range, 23
  web portal features, 74
  tunnel mode client
    installing in Linux, 79
    installing in Mac OS, 79
    installing in Windows, 79
    using in Linux, 82
    using in Mac OS, 84
    using in Windows, 80

U
  URL
    for user log in, 63
Index

user accounts, creating, 47
user groups
  for different access permissions, example, 93
user groups, creating, 47

V
Virtual Desktop, 78
  using, 75
VNC
  starting a session, 73

W
web portal, 66
  adding caption to home page, 35
  customizing login page, 28
  home page features, 64
  logging in, 63
  server applications, 65
  setting login page port number, 27
SSL VPN, SSL VPN web portal
  customize, 30
  tunnel mode features, 74
  using bookmarks, 65
  widgets, 64
web server
  connecting to, 67
web-based manager
  connecting to, 22
web-only mode, 17
  client requirements, 17
  firewall policy for, 49
widget
  tunnel mode, 74
widgets
  web portal, 64

X
X.509 security certificates, 26