FortiGate

PPTP VPN User Guide

Version 3.0 MR5

FORTINET

www.fortinet.com

FortiGate PPTP VPN User Guide
26 September 2007
01-30005-0349-20070926

Trademarks

Contents

Introduction

This section introduces you to FortiGate PPTP VPN technology and the following topics:

About FortiGate PPTP VPNs

A virtual private network (VPN) is a way to use a public network, such as the Internet, to provide remote offices or individual users with secure access to private networks. For example, a company that has two offices in different cities, each with its own private network, can use a VPN to create a secure tunnel between the offices. Similarly, telecommuters can use VPN clients to access private data resources securely from a remote location.

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

FortiGate units support the Point-to-Point Tunneling Protocol (PPTP), which enables interoperability between FortiGate units and Windows or Linux PPTP clients. Because FortiGate units support industry standard PPTP VPN technologies, you can configure a PPTP VPN between a FortiGate unit and most third-party PPTP VPN peers.

More detailed information regarding how the PPTP VPN works can be found in "Configuring PPTP VPNs".

For more information about FortiGate VPN interoperability, contact Fortinet Technical Support.

About this document

This document explains how to configure PPTP VPNs using the web-based manager. To define comparable parameters through the CLI, see the *FortiGate CLI Reference*.

This document contains the following chapters:

- Configuring PPTP VPNs provides an overview of the initial configuration requirements to set up the FortiGate unit as a PPTP server or use a pass through PPTP configuration, as well as the corresponding topologies.

- Configuring the FortiGate unit for PPTP VPN describes how to configure a FortiGate unit to act as a PPTP server and forward PPTP packets to an external PPTP server.
- Configuring PPTP clients describes how to configure the PPTP Windows and Linux clients.
- Monitoring and testing VPN tunnels outlines some basic maintenance and monitoring procedures for PPTP VPNs.

Document conventions

The following document conventions are used in this guide:

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

Note: Highlights useful additional information.

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

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	For the source address, enter the range of addresses that you reserved for PPTP clients (for example `192.168.10.[80-100]`).

Code examples	`config sys global`
	`  set ips-open enable`
	`end`

CLI command syntax	`config firewall policy`
	`  edit id_integer`
	`  set http_retry_count <retry_integer>`
	`  set natip <address_ipv4mask>`
	`  end`

Document names	*FortiGate Administration Guide*
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>`
Menu commands	Go to **VPN > PPTP > PPTP Range**.
Program output	`Welcome!`
Variables	`<address_ipv4>`

FortiGate documentation

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

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

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

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

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

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

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

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

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

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

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

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

  Explains how to configure a PPTP VPN using the web-based manager.

- *FortiGate Certificate Management User Guide*

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

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

Related documentation

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

FortiManager documentation

- *FortiManager QuickStart Guide*

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

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

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

FortiClient documentation

- *FortiClient Host Security User Guide*

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

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

FortiMail documentation

- *FortiMail Administration Guide*

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

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

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

FortiAnalyzer documentation

- *FortiAnalyzer Administration Guide*

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

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

Fortinet Tools and Documentation CD

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

Fortinet Knowledge Center

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

Comments on Fortinet technical documentation

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

Customer service and technical support

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

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

Configuring PPTP VPNs

This section describes how to configure a FortiGate unit to act as a PPTP server. It also describes how to configure the FortiGate unit to forward PPTP packets to an external PPTP server.

The following topics are included in this section:

How a PPTP VPN works

A virtual private network (VPN) is a way to use a public network, such as the Internet, to provide remote offices or individual users with secure access to private networks. The Point-to-Point Tunneling Protocol allows you to create a VPN between a remote client and your internal network. Because it is a Windows standard, PPTP does not require third-party software on the client computer. As long as the Internet Service Provider (ISP) supports PPTP on its servers, you can create a secure connection by making relatively simple configuration changes to the client computer and the FortiGate unit.

PPTP uses Point-to-Point (PPP) protocol authentication protocols so that standard PPP software can operate on tunneled PPP links. PPTP packages data in PPP packets and then encapsulates the PPP packets within IP packets for transmission through a VPN tunnel.

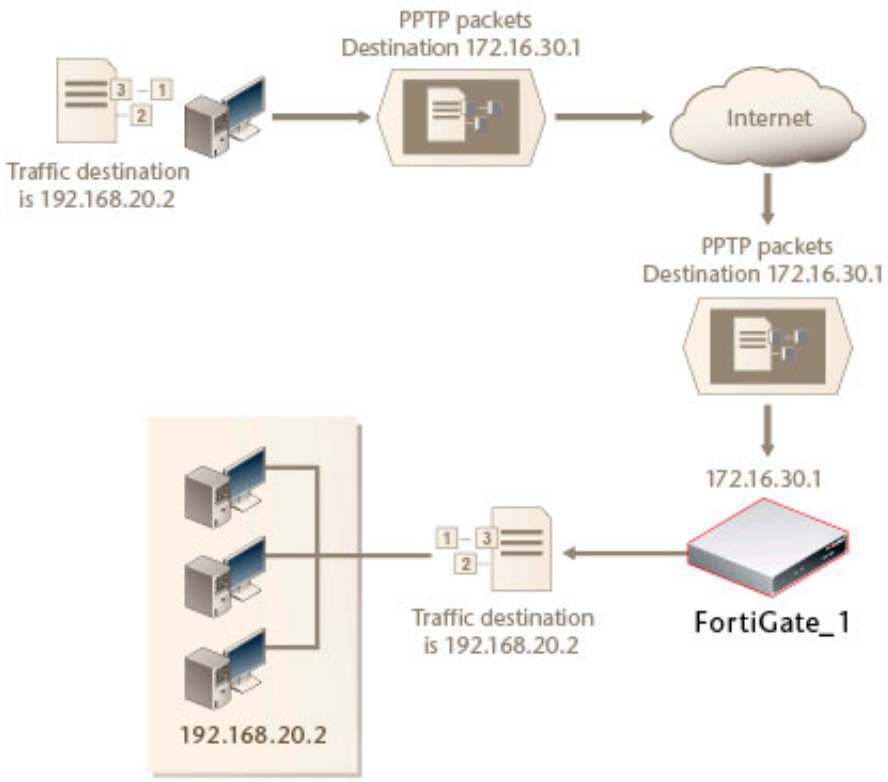
When the FortiGate unit acts as a PPTP server, a PPTP session and tunnel is created as soon as the PPTP client connects to the FortiGate unit. More than one PPTP session can be supported on the same tunnel. FortiGate units support PAP, CHAP, and plain text authentication. PPTP clients are authenticated as members of a user group.

Traffic from one PPTP peer is encrypted using PPP before it is encapsulated using Generic Routing Encapsulation (GRE) and routed to the other PPTP peer through an ISP network. PPP packets from the remote client are addressed to a computer on the private network behind the FortiGate unit. PPTP packets from the remote client are addressed to the public interface of the FortiGate unit. See Figure 1 on page 12.

Caution: PPTP control channel messages are not authenticated, and their integrity is not protected. Furthermore, encapsulated PPP packets are not cryptographically protected and may be read or modified unless appropriate encryption software such as Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) is used to transfer data after the tunnel has been established.

As an alternative, you can use encryption software such as Microsoft Point-to-Point Encryption (MPPE) to secure the channel. MPPE is built into Windows clients and can be installed on Linux clients. FortiGate units support MPPE.

Figure 1: Packet encapsulation



In Figure 1, traffic from the remote client is addressed to a computer on the network behind the FortiGate unit. When the PPTP tunnel is established, packets from the remote client are encapsulated and addressed to the FortiGate unit. The FortiGate unit forwards disassembled packets to the computer on the internal network.

When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

When the FortiGate unit receives a PPTP packet, the unit disassembles the PPTP packet and forwards the packet to the correct computer on the internal network. The firewall policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

Note: PPTP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate PPTP clients. All PPTP clients are challenged when a connection attempt is made.

FortiGate PPTP topologies

In a PPTP configuration, the FortiGate unit can act as a PPTP server or forward PPTP packets to a PPTP server.

Infrastructure requirements

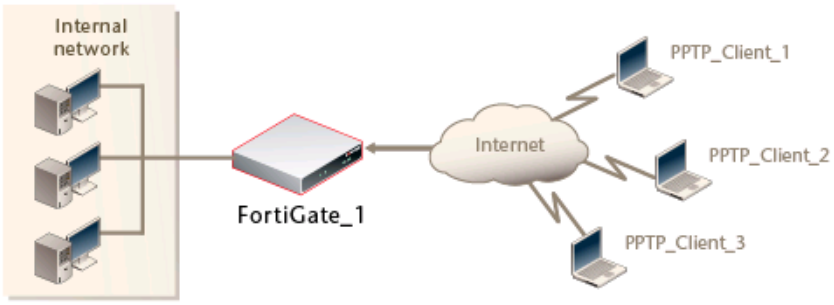
- The FortiGate unit operates in NAT/Route mode and has a static public IP address.
- The dialup client ISP account supports PPP connections with dynamically assigned IP addresses and if the ISP runs a PPTP server, the server must be configured to forward PPTP packets to the FortiGate unit.

The PPTP client includes PPP support (with MPPE if encryption is required).

FortiGate unit as a PPTP server

In the most common Internet scenario, the PPTP client connects to an ISP that offers PPP connections with dynamically-assigned IP addresses. The ISP forwards PPTP packets to the Internet, where they are routed to the FortiGate unit.

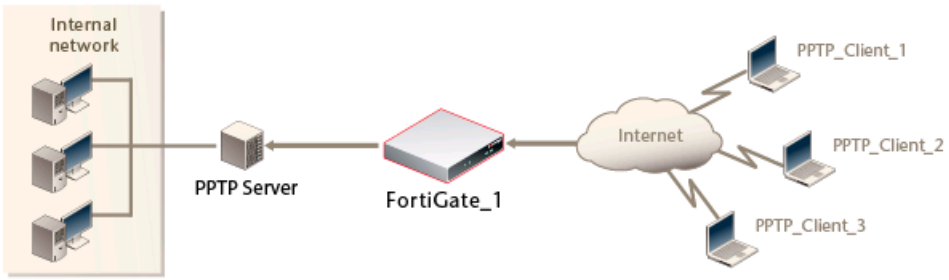
Figure 2: FortiGate unit as a PPTP server



FortiGate unit forwards traffic to a PPTP server

You may also configure the FortiGate unit to forward PPTP packets to a PPTP server on the network behind the FortiGate unit.

Figure 3: FortiGate unit forwards traffic to PPTP server



Configuring the FortiGate unit for PPTP VPN

The FortiGate unit provides two user interfaces to configure operating parameters—the web-based manager, and the CLI. In the web-based manager, PPTP settings are located on the **VPN > PPTP** tab. In the CLI, the `config vpn pptp` command is available to configure comparable VPN settings. For detailed information about these CLI commands, refer to the "vpn" and "execute" chapters of the *FortiGate CLI Reference*.

This section includes the following topics:

PPTP server configuration overview

If the FortiGate unit will act as a PPTP server, perform the following tasks in the order given:

- Configure user authentication for PPTP clients. See "Configuring user authentication for PPTP clients" on page 16, "Configuring a user account" on page 16, and "Configuring a user group" on page 17.
- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect. See "Enabling PPTP and specifying the PPTP IP address range" on page 18.
- Configure the PPTP server. See "Configuring the FortiGate unit as a PPTP server" on page 19.
- Configure the PPTP clients. For general guidelines, refer to "Configuring PPTP clients".

PPTP pass through configuration overview

To arrange for PPTP packets to pass through the FortiGate unit to an external PPTP server, perform the following tasks in the order given:

- Configure user authentication for PPTP clients. See "Configuring user authentication for PPTP clients" on page 16, "Configuring a user account" on page 16, and "Configuring a user group" on page 17.

- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect. See “Enabling PPTP and specifying the PPTP IP address range” on page 18.
- Configure PPTP pass through on the FortiGate unit. See “Configuring the FortiGate unit for PPTP pass through” on page 22.
- Configure the PPTP clients. For general guidelines, refer to “Configuring PPTP clients”.

Configuring user authentication for PPTP clients

To enable authentication for PPTP clients, you must create user accounts and a user group to identify the PPTP clients that need access to the network behind the FortiGate unit. Within the user group, you must add a user for each PPTP client.

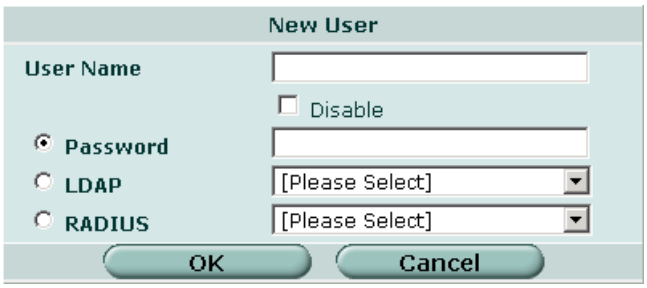
You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

For more information, see the “User” chapter of the *FortiGate Administration Guide*.

Configuring a user account

Go to **User > Local** and select Create New or the Edit icon of an existing user account.

Figure 4: Local user options



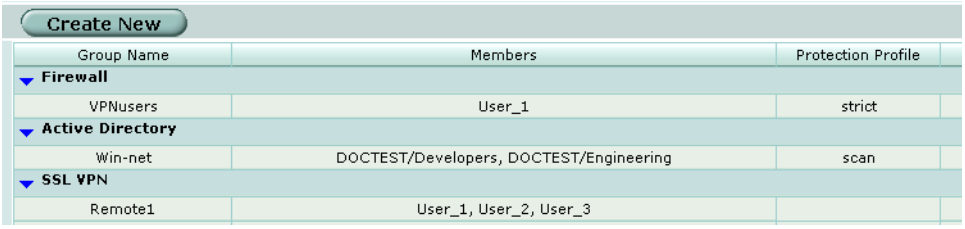
User Name	Type or edit the user name.
Disable	Select Disable to prevent this user from authenticating.
Password	Select Password to authenticate this user using a password stored on the FortiGate unit. Type or edit the password. The password should be at least six characters long.

LDAP	Select LDAP to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the drop-down list. **Note**: You can only select an LDAP server that has been added to the FortiGate LDAP configuration.
RADIUS	Select RADIUS to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the drop-down list. **Note**: You can only select a RADIUS server that has been added to the FortiGate RADIUS configuration.

Configuring a user group

1 Go to **User > User Group** to configure user groups.

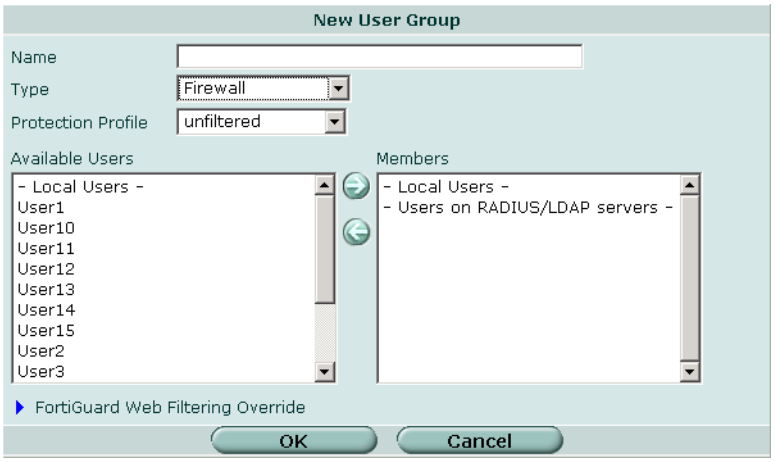
Figure 5: User group list



Create New	Add a new user group.
Group Name	The name of the user group. User group names are listed by type of user group: Firewall, Active Directory and SSL VPN.
Members	The users, RADIUS servers, or LDAP servers in the user group.
Protection Profile	The protection profile associated with this user group.
Delete icon	Delete the user group. **Note**: You cannot delete a user group that is included in a firewall policy, a dialup user phase 1 configuration, or a PPTP or L2TP configuration.
Edit icon	Edit the membership and options of the group.

2 Go to **User > Group** and select Create New or the Edit icon of an existing user group.

Figure 6: User group configuration



Name	Type or enter the name of the user group.
Type	Select the user group type.
Firewall	Select this group in any firewall policy that requires Firewall authentication.
Active Directory	Select this group in any firewall policy that requires Active Directory authentication.
SSL VPN	Select this group in any firewall policy with Action set to SSL VPN.
Protection Profile	Available only if Type is Firewall or Active Directory. Select a protection profile for this user group from the drop-down list. To create a new protection profile, select Create New.
Available Users	The list of users, RADIUS servers, or LDAP servers that can be added to the user group.
Members	The list of users, RADIUS servers, or LDAP servers that belong to the user group.
Right arrow button	Add a user or server to the Members list. Select a user or server name in the Available Users list and select the right arrow button to move it to the Members list.
Left arrow button	Remove a user or server from the Members list. Select a user name or server name in the Members list and select the left arrow button to move it to the Available Users list.
FortiGuard Web Filtering Override	Available only if Type is Firewall. Configure Web Filtering override capabilities for this group.
SSL-VPN User Group Options	Available only if Type is SSL-VPN.

Note: If you try to add LDAP servers or local users to a group configured for administrator authentication, an “Entry not found” error occurs.

Enabling PPTP and specifying the PPTP IP address range

The PPTP address range specifies the range of addresses reserved for remote PPTP clients. When a PPTP client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the PPTP client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the PPTP client appear to be part of the internal network.

Note: IP addresses used in this document are fictional and follow the technical documentation guidelines specific to Fortinet. Real external IP addresses are not used.

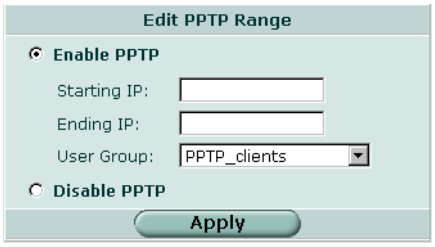
To enable PPTP and specify the PPTP address range

1 Go to **VPN > PPTP > PPTP Range**.

2 Select Enable PPTP and enter the following:

Starting IP	Enter the starting IP address in the range of reserved IP addresses.
Ending IP	Enter the ending IP address in the range of reserved IP addresses.
User Group	Select the name of the PPTP user group that you previously defined.

Figure 7: PPTP range configuration



3 Select Apply.

Configuring the FortiGate unit as a PPTP server

To configure a FortiGate unit to act as a PPTP server, you perform the following configuration tasks on the FortiGate unit:

- Define firewall source and destination addresses to indicate where packets transported through the PPTP tunnel will originate and be delivered. See "Defining firewall source and destination addresses" on page 19.
- Create the firewall policy and define the scope of permitted services between the source and destination addresses. "Adding the firewall policy" on page 20.

Defining firewall source and destination addresses

Before you define the firewall policy, you must define the source and destination addresses of packets that are to be transported through the PPTP tunnel:

- For the source address, enter the range of addresses that you reserved for PPTP clients (for example `192.168.10.[1-10]`).
- For the destination address, enter the IP addresses of the computers that the PPTP clients need to access on the private network behind the FortiGate unit (for example, `172.16.5.0/24` for a subnet, or `172.16.5.1/32` for a server or host, or `172.16.5.[1-10]` for an IP address range).

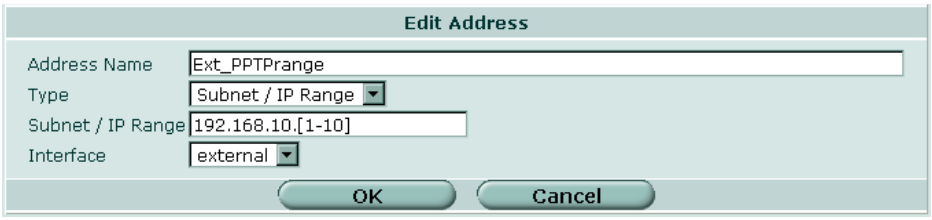
Note: IP addresses used in this document are fictional and follow the technical documentation guidelines specific to Fortinet. Real external IP addresses are not used.

To define the source IP address

1 Go to **Firewall > Address,** select Create New, and enter the following:

Address Name	Enter a name to identify the range of addresses that you reserved for PPTP clients (for example, `Ext_PPTPrange).`
Type	Select the type of address: Subnet/IP Range.
Subnet/IP Range	Enter the IP address range reserved for PPTP clients separated by a hyphen (for example, `192.168.10.[1-10]`).
Interface	Select the interface to the internet.

Figure 8: Firewall source address configuration



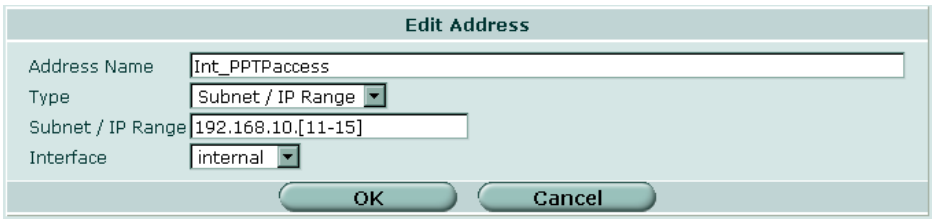
2 Select OK.

To define the destination IP address

1 Go to **Firewall > Address,** select Create New,and enter the following:

Address Name	Enter a name to identify the range of addresses that PPTP clients need to access on the private network behind the FortiGate unit (for example, `Int_PPTPrange`).
Type	Select the type of address: Subnet/IP Range.
Subnet/IP Range	Enter the IP address range that the PPTP clients need to access separated by a hyphen (for example, `192.168.10.[11-15]`).
Interface	Select the interface to the internal network.

Figure 9: Firewall destination address configuration



2 Select OK.

Adding the firewall policy

The firewall policy specifies the source and destination addresses that can generate traffic inside the PPTP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group. For more information, see the “Firewall Policy” chapter of the *FortiGate Administration Guide*.

To define the traffic and services permitted inside the PPTP tunnel

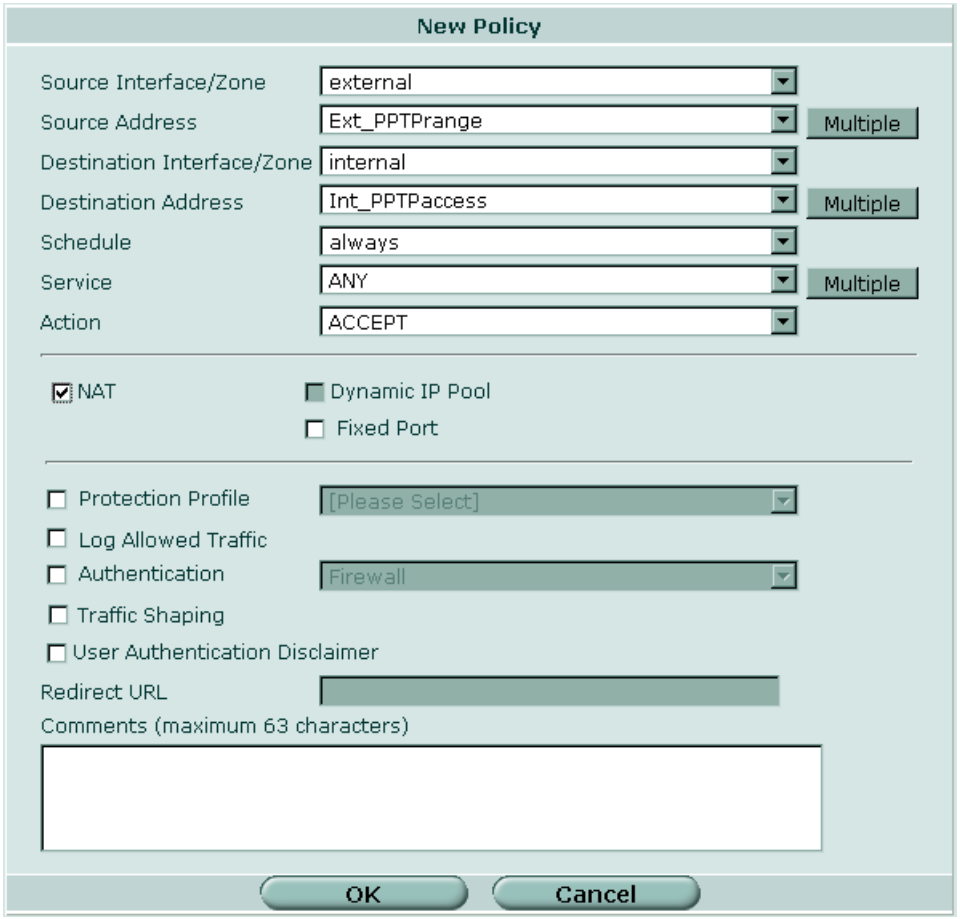
1 Go to **Firewall > Policy** and select Create New.

2 Enter these settings in particular:

Source
Interface/Zone
Select the FortiGate interface to the Internet.
Address Name
Select the name that corresponds to the range of addresses that you reserved for PPTP clients (for example, `Ext_PPTPrange`).

Destination
Interface/Zone
Select the FortiGate interface to the internal (private) network.
Address Name
Select the name that corresponds to the IP addresses behind the FortiGate unit (for example, `Int_PPTPaccess`).
Service
Select ANY, or if selected services are required instead, select the service group that you defined previously.
Action
Select ACCEPT.

Figure 10: Firewall policy for PPTP



3 You may enable NAT, event logging, and shape traffic. For details, see the "Firewall Policy" chapter of the *FortiGate Administration Guide*.

Note: Do not select Authentication, as this will cause the PPTP access to fail. Authentication is configured in the PPTP configuration setup.

4 Select OK.

Configuring the FortiGate unit for PPTP pass through

To forward PPTP packets to a PPTP server on the network behind the FortiGate unit, you perform the following configuration tasks on the FortiGate unit:

- Define a virtual IP address that points to the PPTP server. See "To define a virtual port-forwarding address for PPTP pass through" on page 22. The FortiGate unit will forward PPTP packets to the address you specify.
- Create a firewall policy that allows incoming PPTP packets to pass through to the PPTP server. See "To create a port-forwarding firewall policy for PPTP pass through" on page 23.

Note: The address range is the external (public) ip address range which requires access to the internal PPTP server through the FortiGate virtual port-forwarding firewall.
IP addresses used in this document are fictional and follow the technical documentation guidelines specific to Fortinet. Real external IP addresses are not used.

Defining a virtual port-forwarding address

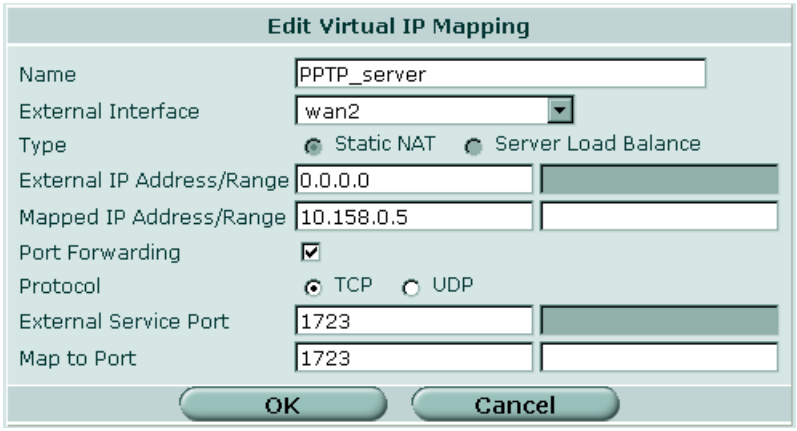
The IP address refers to the PPTP server host. The FortiGate unit will answer ARP requests for the IP address that you specify.

To define a virtual port-forwarding address for PPTP pass through

1 Go to **Firewall > Virtual IP,** select Create New, and enter the following:

Name	Enter a name to identify the virtual IP address (for example, `PPTP_server`).
External Interface	Select the FortiGate interface on which packets destined for the PPTP server arrive. The IP address is bound to this interface for the purpose of proxying ARP requests. In Figure 11, the value is `wan2`.
External IP Address/ Range	Enter the IP address of the FortiGate interface to the Internet.
Mapped IP Address/ Range	Enter the IP address of the PPTP server.
Port Forwarding	Select Port Forwarding to forward packets to the PPTP server.
Protocol	Select TCP.
External Service Port	Enter `1723` (TCP port `1723` is the PPTP port).
Map to Port	Enter `1723`.

Figure 11: Defining a virtual IP address



2 Select OK.

Configuring a port-forwarding firewall policy

To create a port-forwarding firewall policy for PPTP pass through

1 Go to **Firewall > Address,** select Create New, and enter the following:

Address Name	Enter a name to identify the range of external addresses that you reserved for PPTP clients (for example, `External_PPTP`).
Type	Select the type of address: Subnet/IP Range.
Subnet/IP Range	Enter the IP address range reserved for PPTP clients separated by a hyphen (for example, `10.3.3.[1-10]`).
Interface	Select the interface to the internet.

Figure 12: Firewall PPTP port-forwarding address configuration

2 Select OK.

Adding the firewall policy

1 Go to **Firewall > Policy,** select Create New, and enter these settings in particular:

Source	Interface/Zone Select the FortiGate interface to the Internet. Address Name Select the name that corresponds to the range of addresses that you reserved for external PPTP clients (for example, `External_PPTP`).
Destination	Interface/Zone Select the FortiGate interface to the PPTP server. Address Name Select the name that corresponds to the virtual IP address that you defined for the PPTP server (for example, `PPTP_server`). Service Select PPTP Action Select ACCEPT.

2 You may enable NAT, event logging, and shape traffic. See the “Firewall Policy” chapter of the *FortiGate Administration Guide*.

3 Select OK.

Configuring PPTP clients

This section includes the following topics:

Configuring a Windows client

The following procedures outline how to configure a Windows 2000 client and a Windows XP client to access resources behind a FortiGate unit that has been set up to accept PPTP connections. For details, refer to the software supplier's documentation.

To configure the client, you need to know the public IP address of the FortiGate unit. If required, contact the FortiGate administrator to obtain the IP address.

To set up an PPTP dialup connection on a Windows 2000 client

1. Go to **Start > Settings > Network and Dial-up Connections > Make New Connection**, and select Next.
2. Select Connect to a private network through the Internet, and select Next.
3. Select Do not dial the initial connection, and select Next.
4. In the Host name or IP address field, type the public IP address of the FortiGate unit, and select Next.
5. Select Only for myself, and select Next.
6. Type a name for the connection.
7. Select Add a shortcut to this connection to your desktop, and select Finish.
8. When you are prompted to connect to the FortiGate unit, select Cancel.

To set up a PPTP dialup connection on a Windows XP client

1. Go to **Start > Settings > Network Connections > New Connection Wizard**, and select Next.
2. Select Connect to the network at my workplace, and select Next.
3. Select Virtual Private Network Connection, and select Next.
4. In the Company Name field, type a name for the connection, and select Next.
5. In the Host name or IP address field, type the public IP address of the FortiGate unit, and select Next.
6. Select Add a shortcut to this connection to your desktop, and select Finish.
7. When you are prompted to connect to the FortiGate unit, select Cancel.

To connect to the FortiGate PPTP server

Note: Before you can connect to the FortiGate PPTP server, you need to know the user name and password that has been set up on the FortiGate unit to authenticate PPTP clients. Contact the FortiGate PPTP server administrator if required to obtain the user name and password.

1. Connect to the Internet.
2. On your desktop, double-click the PPTP connection shortcut.
3. In the User name field, type the PPTP user name.
4. In the Password field, type the PPTP password.
5. Select Connect.

   After the connection is established, the PPTP client computer is visible on the network behind the FortiGate unit and can be accessed using the IP address of the client PPP interface. Only the servers and hosts that the PPTP client has access to will be visible to the PPTP client.

   To disconnect, right-click the icon in the taskbar and then select Disconnect.

Configuring a Linux client

The following procedure outlines how to install PPTP Client software and run a PPTP tunnel on a Linux computer. Obtain a copy of PPTP Client that meets your requirements (for example, `pptp-linux`). If you need to encrypt traffic, obtain a copy that supports encryption using MPPE.

To establish a PPTP tunnel with a FortiGate unit that has been set up to accept PPTP connections, you can obtain and install the client software following these general guidelines:

1. If encryption is required but MPPE support is not already present in the kernel, download and install an MPPE kernel module and reboot your computer.
2. If required, download and install a PPP package that contains compatible MPPE support.
3. Download and install the PPTP Client package.
4. Configure a PPP connection to run the PPTP program.
5. Configure routes to determine whether all or some of your network traffic will be sent through the tunnel. You must define a route to the remote network over the PPTP link and a host route to the FortiGate unit.
6. Run `pppd` to start the tunnel.
7. Follow the software supplier's documentation to complete the steps.

Note: To configure the system, you need to know the public IP address of the FortiGate unit, and the user name and password that has been set up on the FortiGate unit to authenticate PPTP clients. If required, contact the FortiGate PPTP server administrator to obtain this information.

Monitoring and testing VPN tunnels

This chapter outlines some basic maintenance and monitoring procedures for PPTP VPNs and includes the following topics:

Monitoring PPTP sessions

You can display a list of all active sessions and view activity by port number. By default, port 1723 is used for PPTP VPN-related communications.

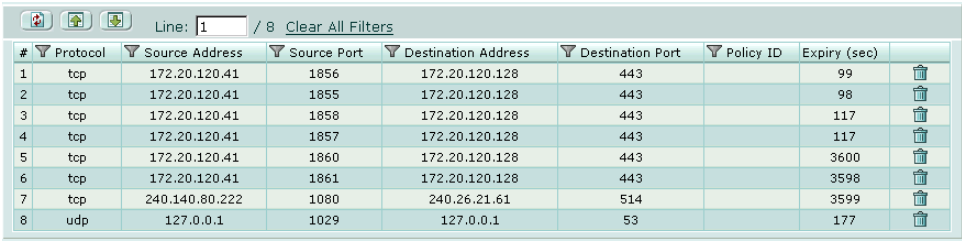
If required, active sessions can be stopped from this view. For more information, see the “System Status” chapter of the *FortiGate Administration Guide*.

To view the list of active sessions

1 Go to **System > Status**.

2 In the Statistics section, select Details on the Sessions line.

Figure 13: Session list



#	Protocol	Source Address	Source Port	Destination Address	Destination Port	Policy ID	Expiry (sec)	
1	tcp	172.20.120.41	1856	172.20.120.128	443		99	
2	tcp	172.20.120.41	1855	172.20.120.128	443		98	
3	tcp	172.20.120.41	1858	172.20.120.128	443		117	
4	tcp	172.20.120.41	1857	172.20.120.128	443		117	
5	tcp	172.20.120.41	1860	172.20.120.128	443		3600	
6	tcp	172.20.120.41	1861	172.20.120.128	443		3598	
7	tcp	240.140.80.222	1080	240.26.21.61	514		3599	
8	udp	127.0.0.1	1029	127.0.0.1	53		177	

Testing VPN connections

To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

Logging VPN events

You can configure the FortiGate unit to log VPN events. For PPTP VPNs, connection events and tunnel status (up/down) are logged. For information about how to interpret log messages, see the *FortiGate Log Message Reference*.

To log VPN events

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

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

- a FortiAnalyzer unit (FortiAnalyzer)
- the FortiGate system memory (Memory)
- a remote computer running a syslog server (Syslog)

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

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

4 If logs will be written to system memory, from the Minimum severity level list, select Information.

For more information, see the “Log & Report” chapter of the *FortiGate Administration Guide*.

5 Select Apply.

To filter VPN events

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

2 Select Enable, and then select L2TP/PPTP/PPPoE service event.

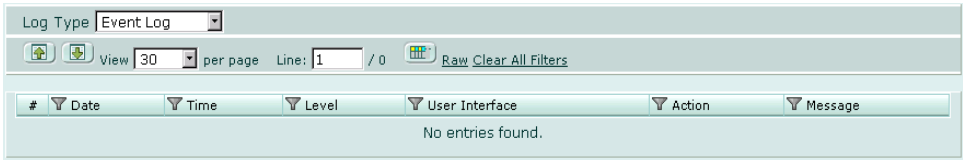
3 Select Apply.

To view event logs

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

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

Figure 14: Log Access > Memory



Index

www.fortinet.com

www.fortinet.com