FortiGate to Cisco VPN 3000 Concentrator Interoperability

Technical Note

FortiGate to Cisco VPN 3000 Concentrator Interoperability Technical Note	
Document Version:	Version 1
Publication Date:	28 March 2005
Description:	This technical note demonstrates how to set up an IPSec VPN tunnel between a FortiGate-800 Antivirus Firewall and a Cisco Systems VPN 3000 Concentrator. In the configuration example, the two VPN peers use preshared keys to authenticate each other.
Product:	FortiGate v2.80 MR7 VPN 3000 Concentrator Version 4.1.9.A
Document Number:	01-28007-0180-20050328

Fortinet Inc.

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

FortiGate to Cisco VPN 3000 Concentrator Interoperability Technical Note
FortiGate v2.80 MR7
28 March 2005
01-28007-0180-20050328

Trademarks
Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Table of Contents

FortiGate to Cisco VPN 3000 Concentrator Interoperability

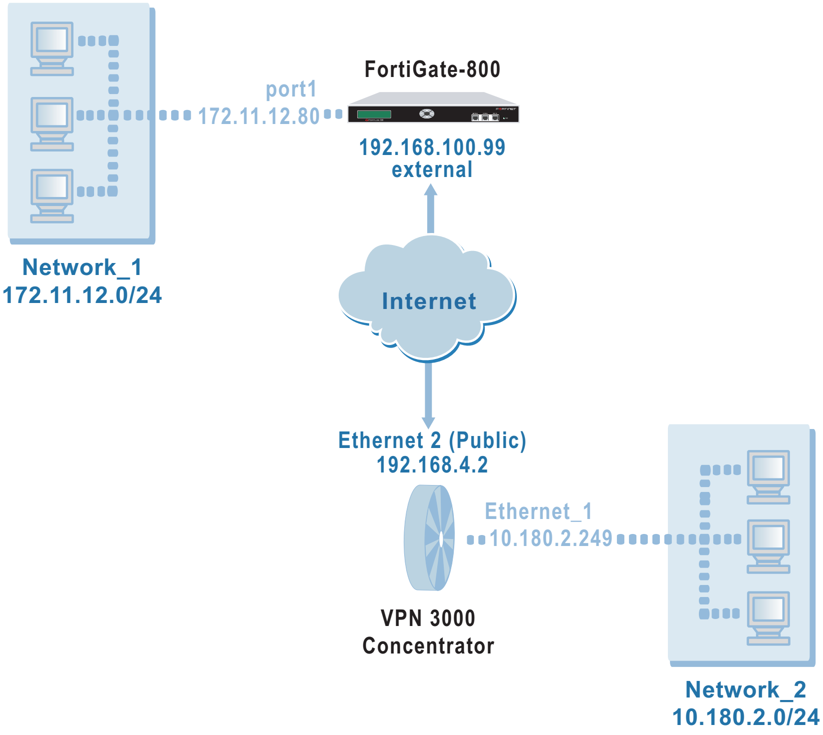
This technical note demonstrates how to set up an IPSec VPN tunnel between a FortiGate-800 Antivirus Firewall and a Cisco Systems VPN 3000 Concentrator. In the configuration example, the two VPN peers use preshared keys to authenticate each other. This technical note contains the following sections:

- Network topology
- Configuring the FortiGate-800
- Configuring the VPN 3000 Concentrator
- Monitoring and testing the VPN tunnel

Network topology

Figure 1 shows an example network configuration. Computers on private Network_2 behind the VPN 3000 Concentrator can access private Network_1 through the FortiGate-800 unit. All traffic generated by computers on Network_2 is subject to a FortiGate firewall encryption policy.

Figure 1: FortiGate-800 to VPN 3000 Concentrator IPSec VPN example



Infrastructure requirements

Throughout this technical bulletin, the following example configuration is assumed:

- The network devices are assigned IP addresses as shown in Figure 1.
- The FortiGate-800 unit is operating in NAT mode.
- Both VPN gateways are assigned static public IP addresses.

Configuring the FortiGate-800

When a FortiGate unit receives a connection request from a remote VPN peer, it uses IPSec phase 1 parameters to establish a secure connection and authenticate the VPN peer. Then, if the firewall policy permits the connection, the FortiGate unit establishes the tunnel using IPSec phase 2 parameters and applies the firewall encryption policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

To support these functions, the following general configuration steps must be performed at the FortiGate unit:

- Define the phase 1 parameters that the FortiGate unit needs to authenticate the remote peer and establish a secure connection. See “Define the phase 1 parameters” below.
- Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer. See “Define the phase 2 parameters” on page 7.
- Create a firewall encryption policy to control the permitted services and permitted direction of traffic between the IP source and destination addresses. A single encryption policy controls both inbound and outbound IP traffic through the VPN tunnel. See “Define the firewall encryption policy” on page 8.

Note: If the private network behind the FortiGate unit needs access to more than one private network behind the VPN 3000 Concentrator, you must create a phase 2 configuration and a firewall encryption policy for each private network behind the VPN 3000 Concentrator. You cannot use FortiGate address groups to define destination addresses for a firewall encryption policy.

Define the phase 1 parameters

The phase 1 configuration defines the parameters that the FortiGate unit will use to authenticate the VPN 3000 Concentrator and establish a secure connection. For the purposes of this example, a preshared key will be used to authenticate the VPN 3000 Concentrator. The same preshared key must be specified at the FortiGate-800 and the VPN 3000 Concentrator.

Before you define the phase 1 parameters, you need to:

- Reserve a name for the remote gateway.
- Obtain the IP address of the public interface to the remote gateway.
- Reserve a unique value for the preshared key.

The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

To define the phase 1 parameters

1. Go to **VPN > IPSEC > Phase 1**.
2. Select Create New, enter the following information:

Gateway Name	Type a name for the remote gateway (for example, `Cisco3005`).
Remote Gateway	Static IP Address
IP Address	`192.168.4.2`
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	Select the following Advanced options: • For DH Group, select 2 to match the default VPN 3000 Concentrator setting. The FortiGate setting must be identical to the VPN 3000 Concentrator setting. • If the VPN peers will establish a connection through a NAT device, select Nat-traversal Enable.

3. Make a note of the Advanced authentication, encryption, and DH Group settings for future reference, to ensure that you set the corresponding VPN 3000 Concentrator settings appropriately.
4. Select OK.

Define the phase 2 parameters

The basic phase 2 settings associate IPSec phase 2 parameters with the phase 1 configuration and specify the remote end point of the VPN tunnel. Before you define the phase 2 parameters, you need to reserve a name for the tunnel.

To define the phase 2 parameters

1. Go to **VPN > IPSEC > Phase 2**.
2. Select Create New, enter the following information:

Tunnel Name	Enter a name for the tunnel (for example, `cisco_3005`).

Remote Gateway	Select the gateway that you defined previously (for example, `Cisco3005`).
Advanced	Select these Advanced options: • Clear Enable replay detection. VPN 3000 Concentrators do not support replay detection, so this option must not be enabled. • Set DH Group to 2. The corresponding VPN 3000 Concentrator setting must be identical to this FortiGate setting. • Set Autokey Keep Alive to Enable.

3. Make a note of the Advanced authentication, encryption, and DH Group settings to compare to corresponding VPN 3000 Concentrator settings.
4. Select OK.

Define the firewall encryption policy

Firewall policies control all IP traffic passing between a source address and a destination address. A firewall encryption policy is needed to allow the transmission of encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy. A single encryption policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Before you define the policy, you must first specify the IP source and destination addresses. In a gateway-to-gateway configuration:

- The source IP address corresponds to the private network behind the FortiGate unit.
- The destination IP address refers to the private network behind the VPN 3000 Concentrator.

To define the IP source address of the network behind the FortiGate unit

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

Address Name	Enter an address name (for example, `Network_1`).
IP Range/Subnet	Enter the IP address of the private network behind the FortiGate unit (for example, `172.11.12.0/24`).

To specify the destination address of IP packets delivered to the VPN 3000 Concentrator

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

Address Name	Enter an address name (for example, `Network_2`).
IP Range/Subnet	Enter the IP address of the private network behind the VPN 3000 Concentrator (for example, `10.180.2.0/24`).

To define the firewall encryption policy

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the interface to the internal (private) network. For example, `port1`. Destination Select the interface to the external (public) network. For example, `external`.

Address Name	Source
	`Network_1`
	Destination
	`Network_2`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`cisco_3005`

3 Place the policy in the policy list above any other policies having similar source and destination addresses.

Configuring the VPN 3000 Concentrator

Configuring a VPN 3000 Concentrator to establish a tunnel with the FortiGate unit involves defining an IPSec LAN-to-LAN connection on the public interface of the VPN 3000 Concentrator.

When you configure the IPSec LAN-to-LAN connection, you set the FortiGate peer IP address, choose authentication, encryption, and IKE proposal settings, and define the local and remote networks. The Preshared Key, Authentication, Encryption, and IKE Proposal settings that you enter must be identical to the settings that you configured previously on the FortiGate unit.

Note: As shown in Figure 1 on page 5, the following procedure assumes that when the VPN 3000 Concentrator was installed, its Ethernet 2 (Public) interface (IP address 192.168.4.2) was configured to route IP packets destined for Network_1 (IP address 172.11.12.0/24) to a router that forwards the packets to the external interface (IP address 192.168.100.99) of the FortiGate unit. The local private network, Network_2, is assigned IP address 10.180.2.0/24.

To configure the IPSec LAN-to-LAN connection

1 Using a web browser, connect to the VPN 3000 Concentrator administration interface.

2 Go to **Configuration > Tunneling and Security > IPSec > LAN-to-LAN**.

3 Select Add.

4. Enter the following information, and select Apply:

Enable	Select the option.
Name	Type a name for the LAN-to-LAN connection (for example, `FortiGate-800`).
Interface	Ethernet 2 (Public) (192.168.4.2)
Connection Type	Bi-directional
Peers	Type the IP address of the FortiGate interface to the external (public) network (for example, `192.168.100.99`).
Digital Certificate	None (Use Preshared Keys)
Certificate Transmission	Identity certificate only
Preshared Key	Enter the preshared key.
Authentication	ESP/SHA/HMAC-160
Encryption	3DES-168
IKE Proposal	IKE-3DES-MD5
Network Autodiscovery	Clear the option.
IPSec NAT-T	If you selected the phase 1 Nat-traversal Enable option on the FortiGate unit, select the IPSec NAT-T option.
Bandwidth Policy	None
Routing	None
Local Network	Select these options: • From the Network List list, select Use IP Address/Wildcard-mask below. • In the IP Address field, type `10.180.2.0`. • In the Wildcard Mask field, type `0.0.0.255`.
Remote Network	Select these options: • From the Network List list, select Use IP Address/Wildcard-mask below. • In the IP Address field, type `172.11.12.0`. • In the Wildcard Mask field, type `0.0.0.255`.

5. Verify that the authentication, encryption, and Diffie-Hellman group settings here are identical to the corresponding phase 1 and 2 FortiGate settings that you noted previously.
6. Go to **Configuration > Tunneling and Security > IPSec > IKE Proposals**.
7. In the Active Proposals list, select the IKE proposal that you selected in Step 4 (IKE-3DES-MD5), and move the proposal to the top of the list.
8. Select Apply, and then select the Save icon in the upper-right corner.

Monitoring and testing the VPN tunnel

The FortiGate unit provides a number of tools for viewing and testing IPSec VPN tunnels:

- You can display the IPSec VPN tunnel list to view the status of all IPSec VPN tunnels. The list shows the status of all active tunnels as well as the tunnel time out values. To view IPSec VPN tunnel status, go to **VPN > IPSEC > Phase 2**.
- You can use the monitor to view activity on IPSec VPN tunnels and start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels. To view the list of tunnels, go to **VPN > IPSEC > Monitor**.
- You can display a list of all active IKE sessions and view activity by port number. To view the list of active IKE sessions, go to **System > Status > Session**.
- To confirm whether a VPN has been configured correctly, issue a ping command on the network behind the FortiGate unit to test the connection to a computer on the remote network. See “Using the ping generator to keep a tunnel open” in the “Configuring IPSec VPNs” chapter of the *FortiGate VPN Guide*. A VPN tunnel will be established automatically when the first data packet destined for the remote network is intercepted by the FortiGate unit.
- You can configure the FortiGate unit to log VPN events. For IPSec VPNs, phase 1 and phase 2 authentication and encryption events are logged. To log VPN events go to **Log&Report > Log Config > Log Setting**. To filter VPN events, go to **Log&Report > Log Config > Log Filter**. To view event logs, go to **Log&Report > Log Access > Event**.

For more information, see the “Monitoring and Testing VPN Tunnels” chapter of the *FortiGate VPN Guide*.