FortiGate to Cisco VPN 3000 Concentrator Series IPSec VPN Interoperability

Technical Note

FortiGate to Cisco VPN 3000 Concentrator Series IPSec VPN Interoperability Technical Note	
Document Version:	Version 1
Publication Date:	8 August 2003
Description:	Describes the setup of IPSec VPN tunnels between FortiGate and Cisco VPN 3000 Concentrator Series. Provides configuration examples and procedures for AutoIKE key network-to-network VPN.
Product:	FortiGate Antivirus Firewall 300 v2.50 Build 52 Cisco VPN 3000 Concentrator Series v 3.0

Fortinet Inc.

FortiGate to Cisco VPN 3000 Concentrator Series IPSec VPN Interoperability Technical Note
v2.50
8 August 2003

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

Network topology **1**
AutoIKE key VPN configuration (main mode) **2**
General configuration steps 2
Configuring the FortiGate unit (main mode) 3
Configuring the Cisco unit 7
Testing the AutoIKE key VPN 9
Viewing VPN tunnel status 9

FortiGate to Cisco VPN 3000 Concentrator Series IPSec VPN Interoperability

FortiGate products offer superior interoperability with other IPSec VPN gateway and client products. This technical note contains example procedures and configurations for IPSec VPN tunnels between FortiGate units and Cisco VPN 3000 Concentrator Series. These procedures and configurations are provided for FortiGate user reference.

This technical note contains the following sections:

- Network topology
- AutoIKE key VPN configuration (main mode)

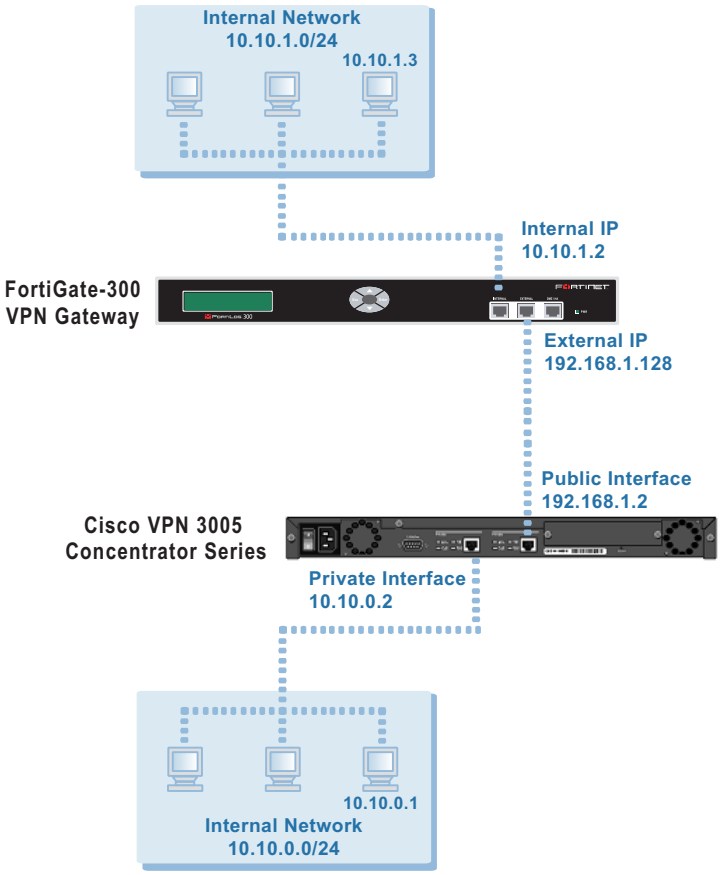
Network topology

The configurations described in this technical note are for the following firmware versions:

- Any FortiGate Antivirus Firewall with firmware 2.50 build 052
- A Cisco 3000 VPN Concentrator Series with firmware 3.0

Figure 1 shows the FortiGate IPSec VPN gateway to the Cisco Concentrator network topology used for the example configurations in this document. The diagram shows a FortiGate-300 unit and a Cisco VPN 3005 Concentrator.

Figure 1: FortiGate-300 to Cisco VPN Concentrator network topology



AutoIKE key VPN configuration (main mode)

This section describes how to configure an AutoIKE key VPN in main mode for the example network topology shown in Figure 1.

General configuration steps

1 Configure the FortiGate unit for AutoIKE key VPN (main mode).

- Add a remote gateway with Static IP Address and Main (ID Protection) selected. Set the IP address of the remote gateway to the external IP address of the Cisco unit.
- Add an AutoIKE key VPN tunnel between the FortiGate unit and the Cisco unit.
- Add a source address to specify the address or address range on the FortiGate internal network that is part of the VPN.
- Add a destination address to specify the address or address range on the Cisco internal network that is part of the VPN.

- Add an internal to external encrypt policy that includes the source and destination addresses and the AutoIKE key VPN tunnel.
- Place the encrypt policy in the policy list, in order from more specific to more general.

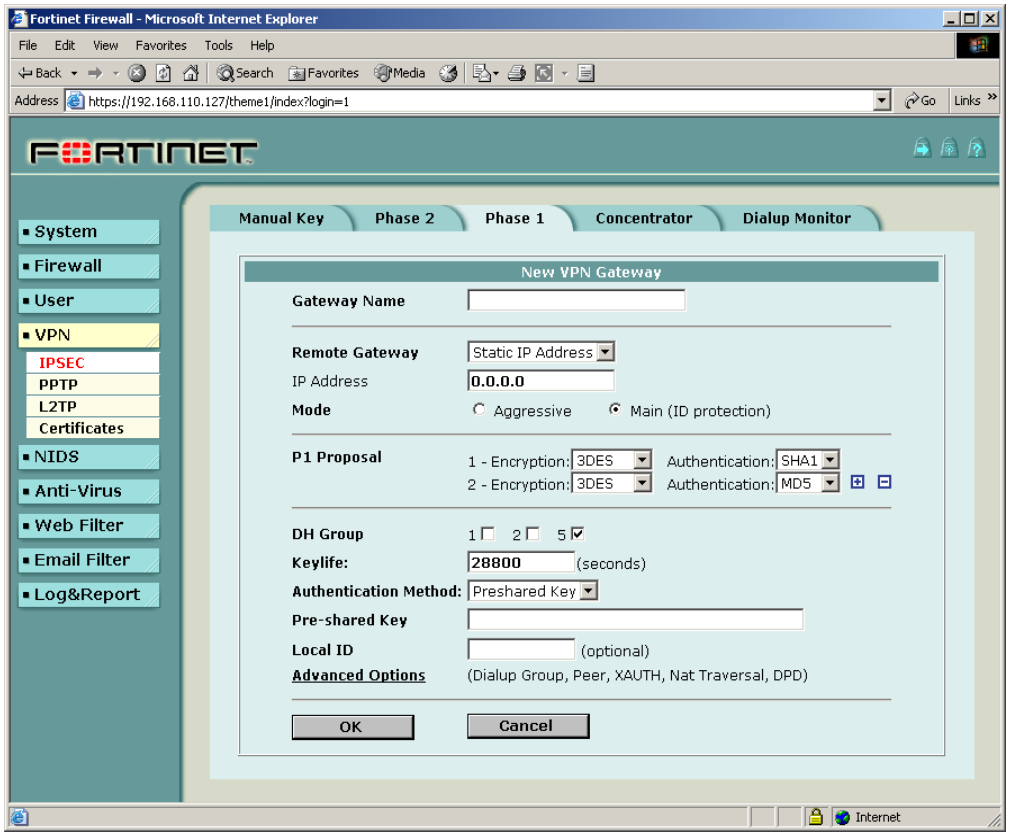
2 Configure the Cisco unit for AutoIKE key VPN.

- Configure the IPSec LAN-to-LAN settings, such as the local and remote IP addresses.
- Configure the IKE proposal and associate with the VPN tunnel.

Configuring the FortiGate unit (main mode)

Start the web-based FortiGate manager to configure the FortiGate unit.

Figure 2: FortiGate web-based manager



Configuration consists of five steps:

- Adding a remote gateway.
- Adding an AutoIKE key VPN tunnel.
- Adding the source address.
- Adding the destination address.
- Adding the internal-to-external encrypt policy.

To add a remote gateway

1 Go to **VPN > IPSEC > Phase 1.**

2 Select New.

3 Enter the following information and select OK:

Note: The Cisco unit does not support DH Group 5.

Gateway Name	Cisco_3000
Remote Gateway	Static IP Address
IP Address	192.168.1.2
Mode	Main (ID Protection)
P1 Proposal	1-Encryption 3DES, Authentication MD5
DH Group	2
Keylife	28800 (seconds)
Authentication Method	Preshared key
Pre-shared key	12345678 The key must contain at least 6 printable characters and should only be known by network administrators. To protect against the best-known attacks, a good pre-shared key should consist of a minimum of 16 randomly chosen alpha-numeric characters. The Cisco unit must use the same pre-shared key.
Local ID	
Peer Options	Accept any peer ID
XAuth	Disable
Nat-traversal	Disable
Keepalive Frequency	5 (seconds)
Dead Peer Detection	Disable
Short Idle	10 (seconds)
Retry Count	3 (times)
Retry Interval	5 (seconds)
Long Idle	300 (seconds)

To add an AutoIKE VPN tunnel

1 Go to **VPN > IPSEC > Phase 2.**

2 Select New.

3 Enter the following information and select OK:

Tunnel Name	test_to_Cisco_3000
Remote Gateway	Cisco_3000
P2 Proposal	1-Encryption 3DES, Authentication MD5
Enable replay detection	Disable
Enable perfect forward frequency	Disable
DH Group	2
Keylife	1800 (seconds)
Autokey Keep Alive	Disable
Concentrator	None

To add the source address

1. For a FortiGate-300 or lower model, go to **Firewall > Address > Internal**.
2. Select New.
3. Enter the following information and select OK:

Address Name	FG_private_net
IP Address	10.10.1.0
Netmask	255.255.255.0

To add the destination address

1. Go to **Firewall > Address > External**.
2. Select New.
3. Enter the following information and select OK:

Address Name	Cisco_private_net
IP Address	10.10.0.0
Netmask	255.255.255.0

To add the encrypt policy

1. Go to **Firewall > Policy > Int** ->**Ext**.
2. Select New.
3. Enter the following information and select OK:

Source	FG_private_net
Destination	Cisco_private_net
Schedule	Always
Service	Any
Action	ENCRYPT
VPN Tunnel	test_to_Cisco_3000
Allow Inbound	Select it to enable inbound users to connect to the source address.
Allow Outbound	Select it to enable outbound users to connect to the destination address.
Inbound NAT	Disable
Outbound NAT	Disable
Traffic Shaping	Configure settings as required for this policy.
Log Traffic	Select if you want to write messages to the traffic log whenever the policy processes a connection.
Anti-Virus & Web filter	Configure settings as required for this policy.
Comments	Optionally enter a short description of the firewall policy.

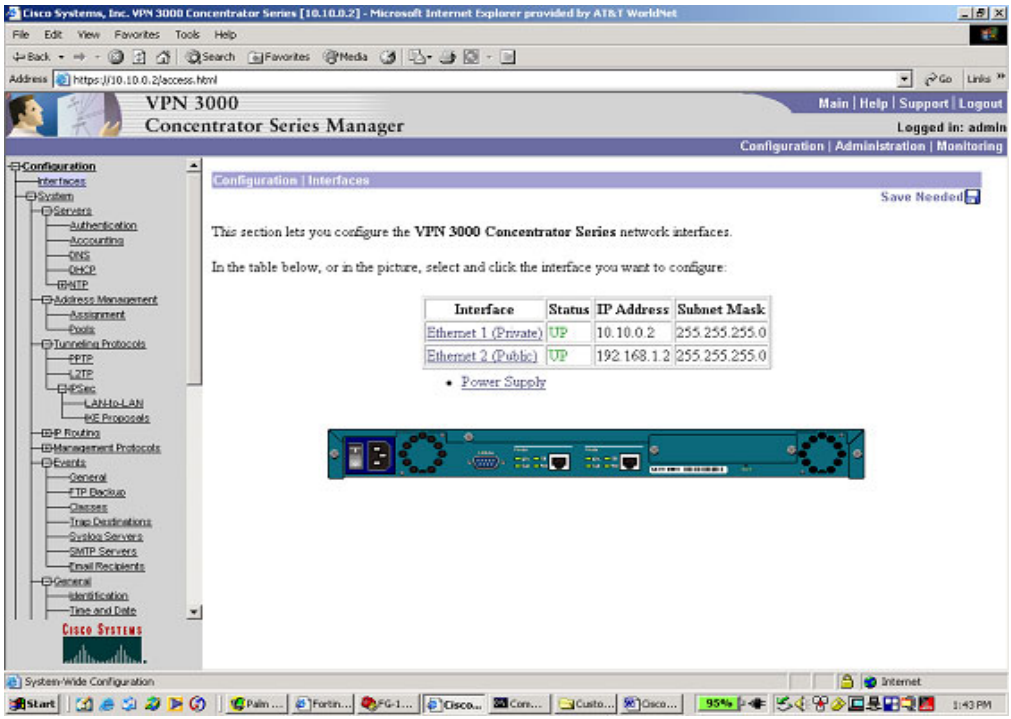
4 Go to **Firewall > Policy** and enable the newly created policy.

5 Place the policy in the policy list above other normal (non-encrypt) policies with similar source and destination addresses.

Configuring the Cisco unit

Start the web-based Cisco VPN 3000 Concentrator Series Manager to configure the Cisco unit.

Figure 3: Cisco VPN 3000 Concentrator Series Manager



Configuration consists of the following steps:

- Configuring the IPSec LAN-to-LAN settings.
- Configuring the IKE proposal.
- Configuring the Security Associations (SA) settings.
- Enabling the FortiGate policy

To configure the IPSec LAN-to-LAN settings

1. Go to **Configuration > System > Tunneling Protocols > IPSec > LAN to LAN.**
2. Enter the following information and click Apply:

Note: The Peer address must be the FortiGate external interface address. The Preshared Key, Authentication, Encryption, and IKE Proposal must match the FortiGate configuration.

Name	labtest
Interface	Ethernet 2 (Public)(192.168.1.2)
Peer	192.168.1.128
Digital Certificate	None
Preshared Key	12345678
Authentication	ESP/MD5/HMAC-128
Encryption	3DES-168
IKE Proposal	IKE-3DES-MD5
Network Autodiscovery	Disable
Network List (Local Network)	Use IP Address/Wildcard-mask below
IP Address (Local Network)	10.10.0.0
Wildcard Mask (Local Network)	0.0.0.255
Network List (Remote Network)	Use IP Address/Wildcard-mask below
IP Address (Remote Network)	10.10.1.0
Wildcard Mask (Remote Network)	0.0.0.255

To configure the IKE proposal

1 Go to **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**.

2 In the Active Proposals list, select the proposal that is used in the LAN-to-LAN configuration and move it to the top of the list.

3 Click Modify.

4 Make sure the settings for Authentication, Encryption, DH Group, and Time lifetime match those of the FortiGate unit.

To configure the Security Associations settings

1 Go to **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**.

1 Click Security Associations.

2 From the IPSec SAs list, select L2L: labtest, then click Modify.

This screen allows you select the IPSec (Phase2) parameters and associate them to the IKE Parameters set previously. Note that the parameters must match the FortiGate for Authentication, Encryption, Encapsulation (which must be set to Tunnel), PFS disabled (which is enabled by default on the FortiGate), and Time Lifetime in seconds.

3 Make sure you enter the following information and click Apply.

SA Name	L2L:labtest
Inheritance	From Rule
Authentication Algorithm	ESP/MD5/HMAC-128
Encryption Algorithm	3DES-168
Encapsulation Mode	Tunnel
Perfect Forward Secrecy	Disabled
Lifetime Measurement	Time
Data Lifetime	10000
Time Lifetime	1800
IKE Peer	192.168.1.128
Negotiation Mode	Main
Digital Certificate	None
IKE Proposal	IKE-3DES-MD5

Testing the AutoIKE key VPN

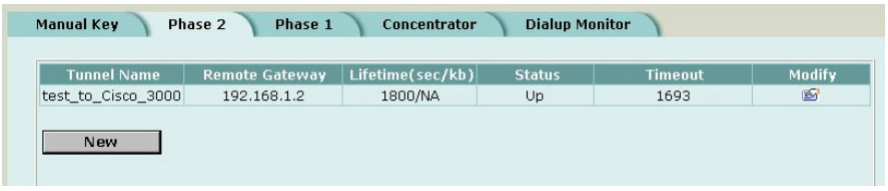
To confirm that the AutoIKE key VPN has been configured correctly, use the ping command between a computer on the FortiGate internal network and a computer on the Cisco internal network. The IPSec VPN tunnel starts automatically when the first data packet destined for the VPN is intercepted by the gateway for your internal network.

Viewing VPN tunnel status

To view VPN tunnel status on the FortiGate unit

- Go to **VPN > IPSEC > Phase 2.**

Figure 4: Cisco VPN 3000 Concentrator Series Manager



For each tunnel, the list shows the status of the tunnel as well as the tunnel timeout.

The Status column displays the status of each tunnel. If Status is Up, the tunnel is active. If Status is Down, the tunnel is not active.

The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.

To view VPN tunnel status on the Cisco unit

- Go to **Monitoring > Sessions**.

Figure 5: VPN tunnel status on the Cisco unit