FortiGate Firewall to Linksys Router IPSec VPN Interoperability

Technical Note

FortiGate Firewall to Linksys Router IPSec VPN Interoperability Technical Note	
Document Version:	Version 2.50
Publication Date:	7 November 2003
Description:	Describes the setup of IPSec VPN tunnels between FortiGate firewalls and Linksys Cable/DSL routers. Provides configuration examples and procedures for AutoIKE key network-to-network VPN.
Product:	FortiGate Antivirus Firewall 300 Linksys EtherFast® Cable/DSL VPN Router, model BEFVP41

Fortinet Inc.

FortiGate Firewall to Linksys Router IPSec VPN Interoperability Technical Note
v2.50
7 November 2003

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

FortiGate Firewall to Linksys Router IPSec VPN Interoperability Technical Note

FortiGate antivirus firewalls offer superior interoperability with other IPSec VPN gateways and client products. This technical note contains example procedures and configurations for IPSec VPN tunnels between FortiGate firewalls and Linksys cable/DSL VPN routers.

This technical note contains the following sections:

- Network topology
- IPSec VPN with pre-shared keys
  - Configuring the FortiGate unit
  - Configuring the Linksys router
  - Testing the VPN connection

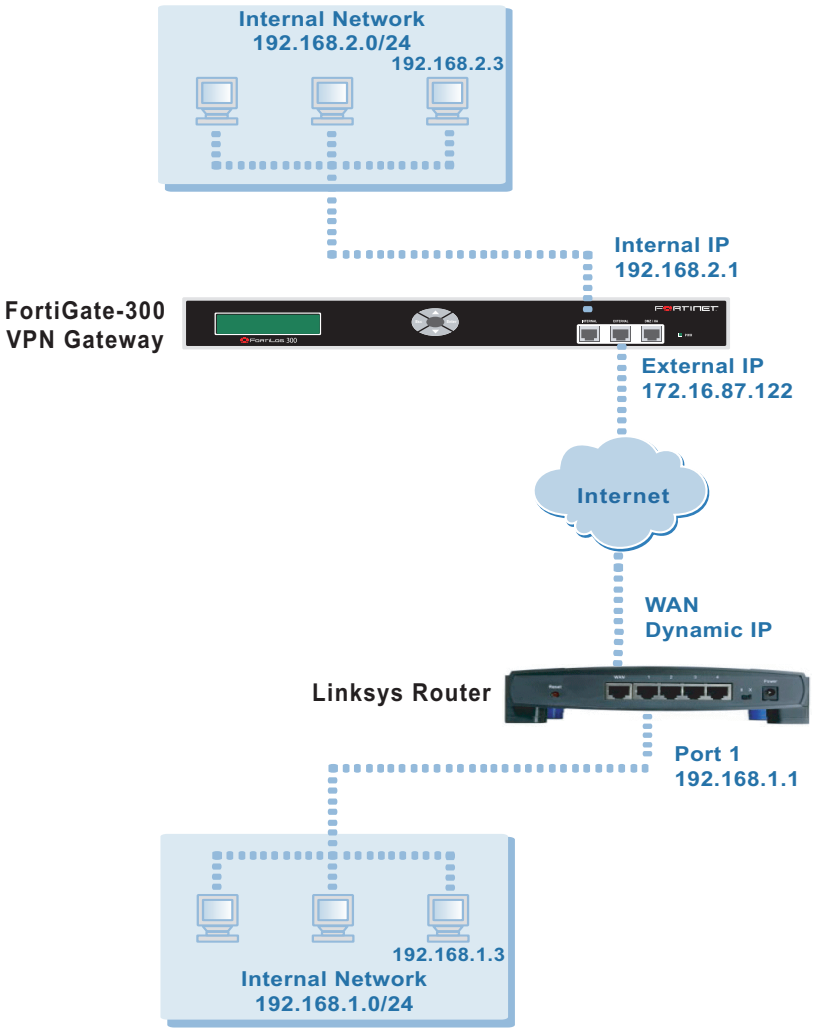
Network topology

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

- Any FortiGate Antivirus Firewall with firmware 2.50 MR5 build 133.
- A Linksys Cable/DSL VPN router with firmware version 1.40.2.

Figure 1 shows the FortiGate IPSec VPN gateway to the Linksys router network topology used for the example configurations in this document. The diagram shows a FortiGate-300 unit and a Linksys EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch.

Figure 1: FortiGate-300 to Linksys VPN router network topology



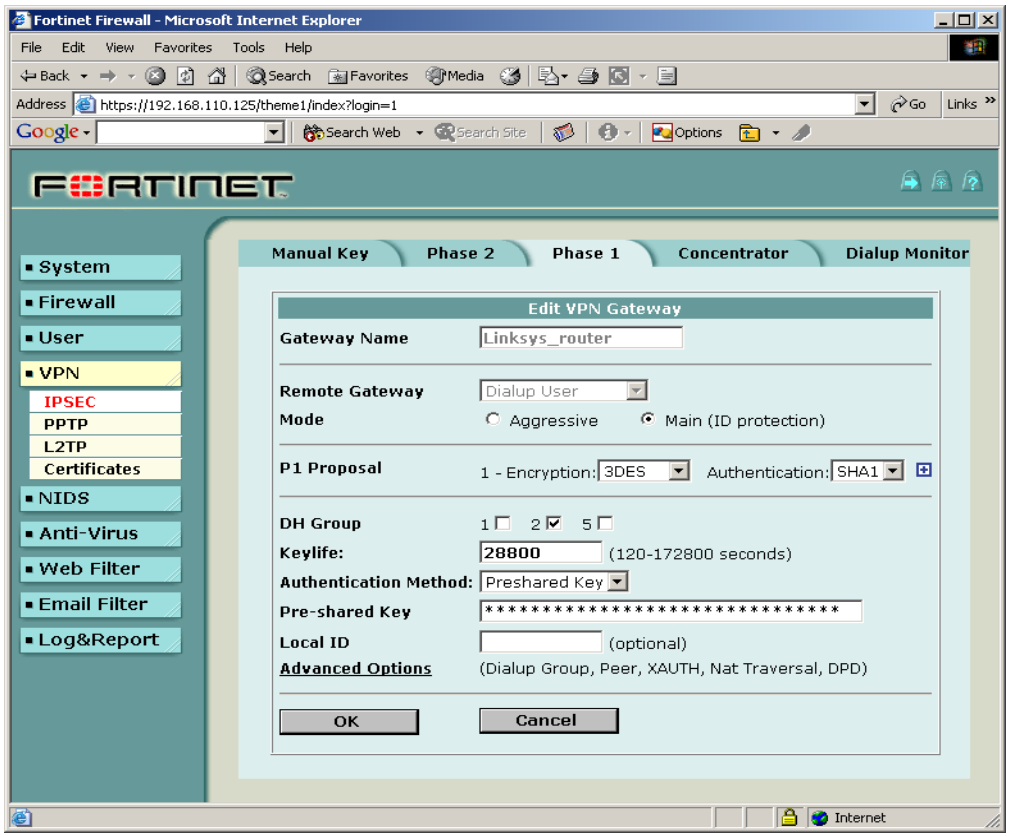
IPSec VPN with pre-shared keys

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

Configuring the FortiGate unit

Start the FortiGate web-based manager.

Figure 2: FortiGate web-based manager



The FortiGate configuration consists of five steps:

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

Note: Because the remote VPN client is a dialup user, you do not need to add a destination address.

To add a remote gateway

1. Go to **VPN > IPSEC > Phase 1.**
2. Select New.
3. Enter the following information and select OK.

Gateway Name	Linksys_router
Remote Gateway	Dialup User
Mode	Main (ID Protection)
P1 Proposal	1-Encryption 3DES, Authentication SHA1
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 Linksys router must use the same pre-shared key.
Local ID	
Peer Options	Accept any peer ID
XAuth	Disable
Nat-traversal	Enable
Keepalive Frequency	5 (seconds)
Dead Peer Detection	Enable
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	FGT_to_Linksys
Remote Gateway	Linksys_router
P2 Proposal	1-Encryption 3DES, Authentication SHA1
Enable replay detection	Enable
Enable perfect forward frequency	Enable
DH Group	2
Keylife	3600 (seconds)
Autokey Keep Alive	Disable
Concentrator	None
Quick Mode Identities	Use selectors from policy

To add the source address

1 Go to **Firewall > Address > Address**.

2 From the Interface list, select Internal.

3 Select New.

4 Enter the following information and select OK.

Address Name	FGT_private_net
IP Address	192.168.2.0
Netmask	255.255.255.0

To add the encrypt policy

1 Go to **Firewall > Policy > Internal** ->**External.**

2 Select Edit.

3 Select New.

4 Enter the following information and select OK.

Source	FGT_private_net
Destination	External_All
Schedule	Always
Service	Any
Action	ENCRYPT
VPN Tunnel	FGT_to_Linksys
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.

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

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

You have configured the FortiGate unit for the VPN connection.

Configuring the Linksys router

After you have configured the FortiGate unit, you can configure the Linksys router.

The Linksys configuration consists of the following steps:

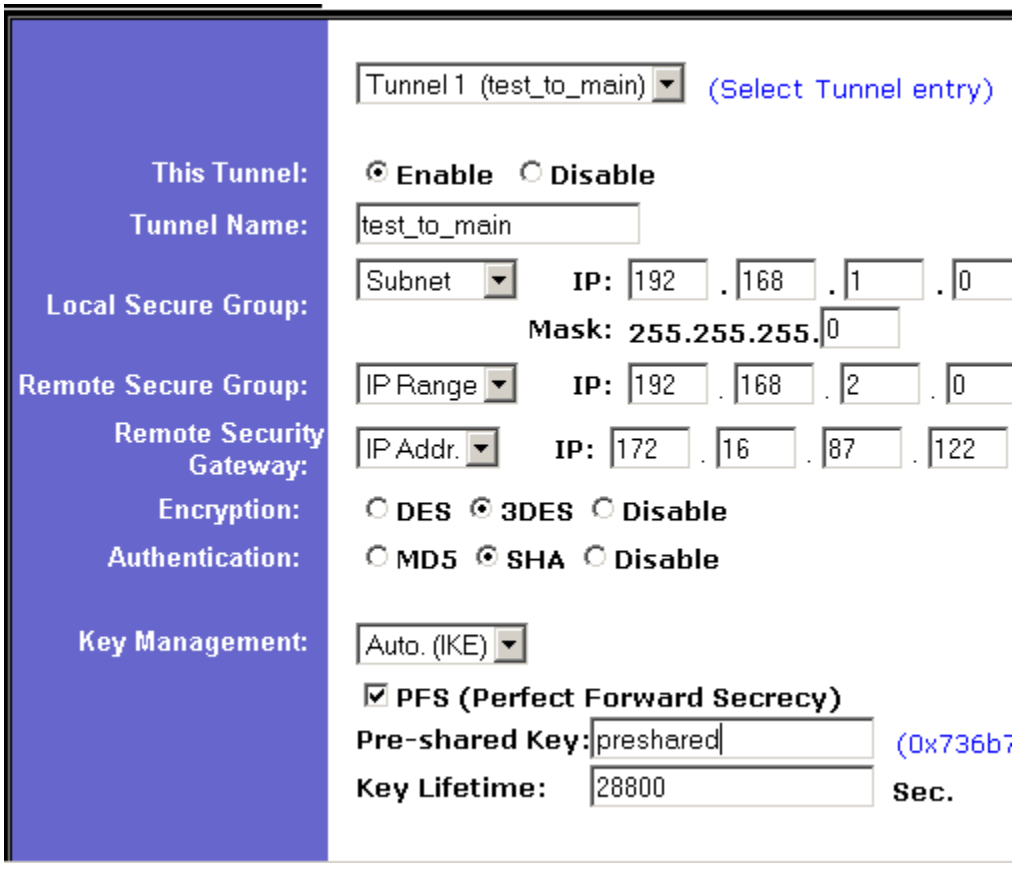
- Adding the VPN tunnel with the local network address, Local Source Group address, and the Remote Secure Group address.
- Adding the remote gateway address.
- Specifying the encryption and authentication methods.
- Adding the pre-shared key.

To configure the Linksys router

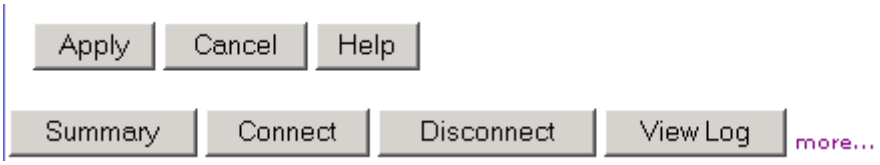
1 Start and log on to the Linksys Cable/DSL VPN Router's Web-based Utility.

2 On the VPN tab, enter the following information and select Apply.

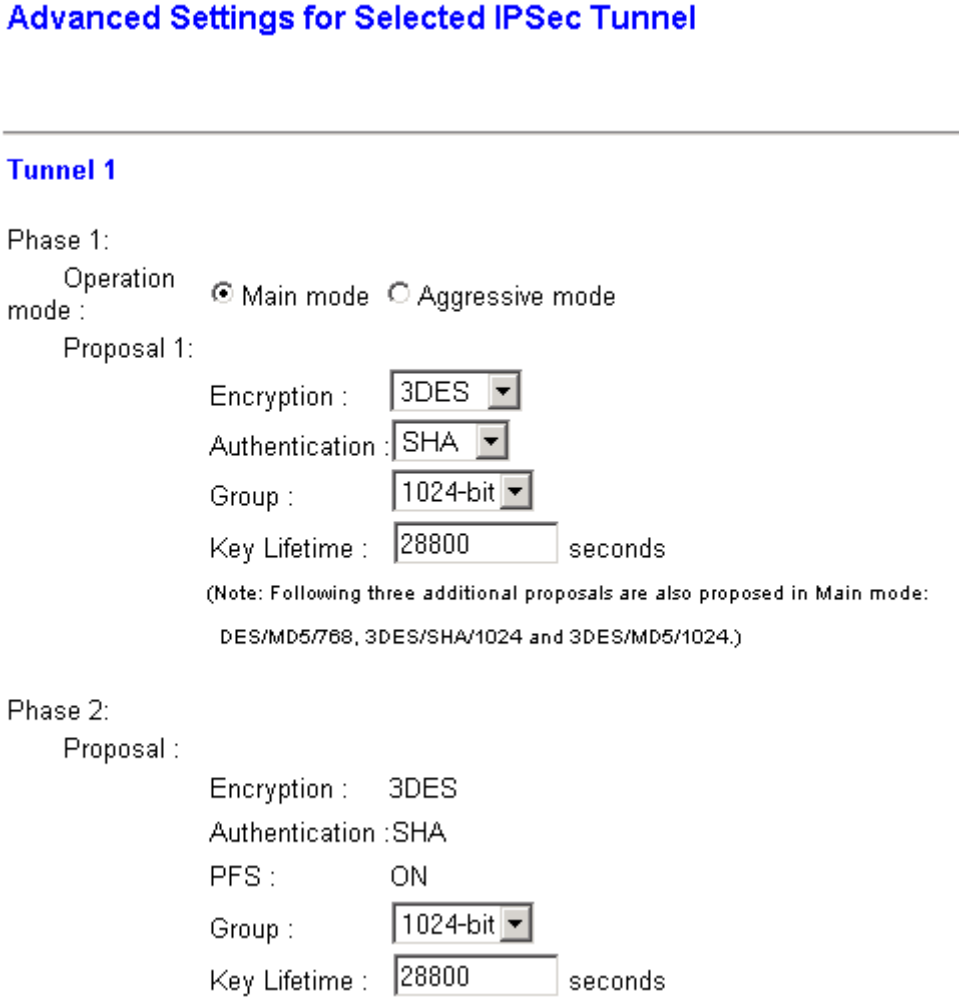
Figure 3: VPN Tab of the Linksys Cable/DSL VPN Router's Web-based Utility



3 Click the more... link to configure the advanced settings.



4 On the Advanced Settings for Selected IPSec Tunnel page, enter the following information and select Apply.



Testing the VPN connection

After you have configured both the FortiGate unit and the Linksys router, you can test the VPN connection from either the network behind the FortiGate unit or the network behind the Linksys router.

To test the VPN connection from the network behind the FortiGate unit

1. From a computer in the network behind the FortiGate unit, ping a computer in the network behind the Linksys router.

   The IPSec VPN tunnel starts automatically when the first data packet destined for the VPN is intercepted by the FortiGate unit.

2. Go to **VPN > IPSEC > Phase 2** to view the VPN connection status.

   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 test the VPN connection from the Linksys router

1. On the VPN tab of the Linksys router's Web-based Utility, select Connect.

   If the VPN connection is successful, the word "Connected" is displayed under Status. Otherwise, the word "Disconnected" is displayed.