FortiGate to SSH Sentinel IPSec VPN Interoperability

Technical Note

FortiGate to SSH Sentinel IPSec VPN Interoperability Technical Note	
Document Version:	Version 2
Publication Date:	4 September 2003
Description:	Describes the setup of IPSec VPN tunnels between a FortiGate dialup server and the SSH Sentinel dialup client. Provides configuration examples and procedures for aggressive mode, main mode, NAT traversal, and exporting and importing SSH Sentinel policies.
Product:	FortiGate Antivirus Firewall v2.50 SSH Client v1.4

Fortinet Inc.

FortiGate to SSH Sentinel IPSec VPN Interoperability Technical Note
v2.50
4 September 2003

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

FortiGate to SSH Sentinel 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 AutoIKE key VPN tunnels between a client PC running the SSH Sentinel VPN client and a FortiGate Antivirus Firewall running FortiOS v2.50.

This technical note contains the following sections:

Network topologies

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

- Any FortiGate unit with firmware 2.50
- SSH Sentinel VPN client with firmware 1.4 and 1.41

Figure 1 shows the SSH Sentinel to FortiGate IPSec network topology used for the examples in "FortiGate to SSH Sentinel VPN with pre-shared keys" on page 7 and "FortiGate to SSH Sentinel VPN with certificates" on page 26. The diagram shows a FortiGate-300 unit, but the procedures and configurations could be applied to any FortiGate unit.

Figure 1: SSH Sentinel to FortiGate-300 network topology

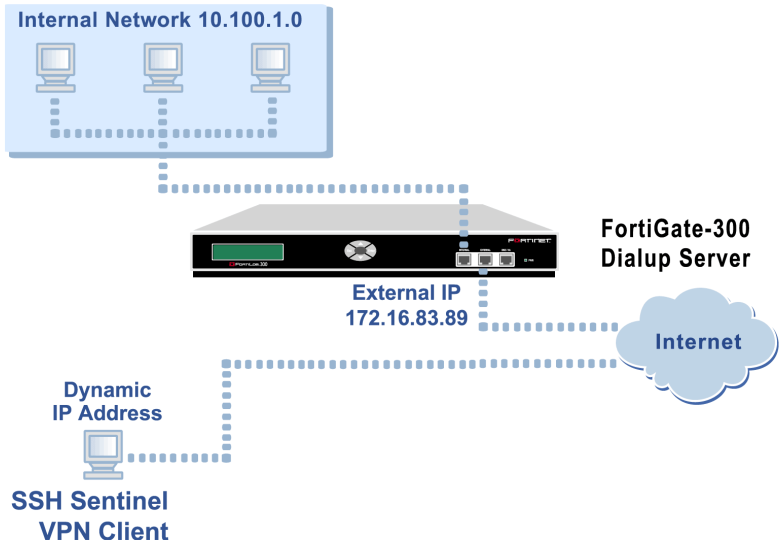
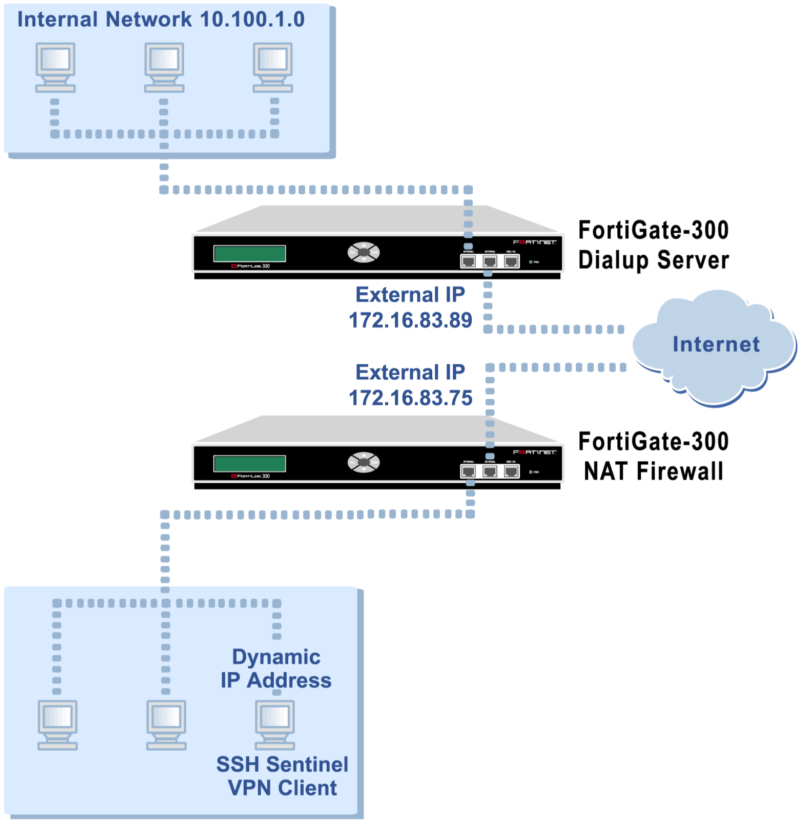


Figure 2 shows the network topology used for the examples in "FortiGate to SSH Sentinel VPN with pre-shared keys (NAT traversal)" on page 17. The diagram shows a FortiGate-300 dialup server, but the procedures and configurations could be applied to any FortiGate unit. The FortiGate-300 NAT firewall could be any firewall.

Figure 2: SSH Sentinel to FortiGate-300 network topology with NAT traversal



FortiGate to SSH Sentinel VPN with pre-shared keys

This section describes how to configure and test a dialup VPN in main mode, for a network topology similar to that shown in Figure 1. In this case, the FortiGate unit is the dialup server and the SSH Sentinel is the dialup client. Both ends use pre-shared keys.

General configuration steps

1 Configure the FortiGate unit as a dialup server.

- Add a remote gateway.
- Add an AutoIKE key VPN tunnel.
- Add a source address to specify the address or address range on the FortiGate internal network that is part of the VPN.
- Add an internal to external encrypt policy that includes the source address, the destination address External_All, and the dialup VPN tunnel.
- Place the encrypt policy above the non-encrypt policies in the policy list.

2 Configure the SSH Sentinel as a dialup VPN client.

- Add a VPN connection between the SSH Sentinel and the FortiGate dialup server.
- Add the FortiGate remote network.
- Add the pre-shared key to be used during phase 1 negotiations.
- Apply the pre-shared key to the VPN policy and select main mode.
- Configure WINS and DNS server access.
- Test the VPN connection.
- Start the VPN tunnel between the SSH Sentinel and the FortiGate dialup server.

Configuring the FortiGate unit for dialup VPN

To add the remote gateway

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

2 Select New.

3 Enter the following information, then select OK.

Gateway Name	Dialup_Client
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	1234567 The SSH Sentinel client must use the same pre-shared 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.
Local ID	

To add the VPN tunnel

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

2 Select New.

3 Enter the following information, then select OK.

Tunnel Name	Client_IKE
Remote Gateway	Dialup_Client
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	Enable
Concentrator	None
Quick Mode Identities	Use selectors from policy

To add the source address

1. Go to **Firewall > Address > Internal.**
2. Select New.
3. Enter the following information, then select OK.

Address Name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

To add the firewall policy

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

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

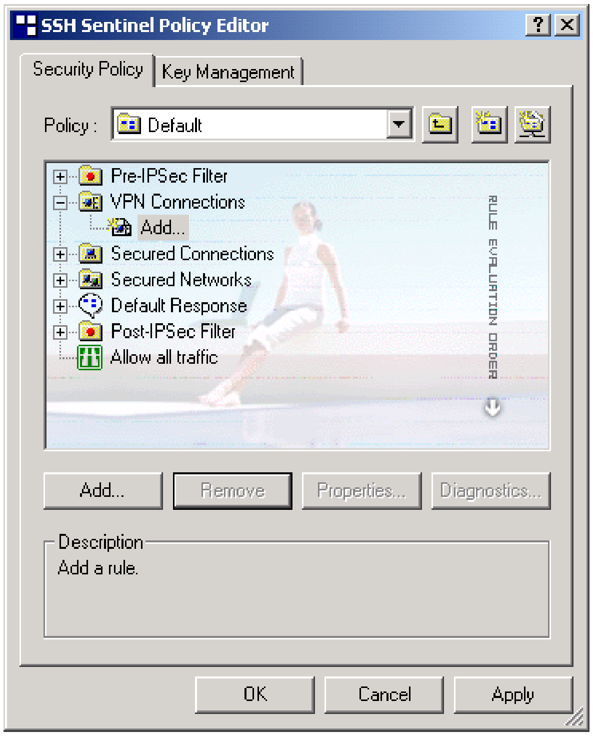
4 Place the policy in the policy list above non-encrypt policies. If there are more than one encrypt policies in the list, place the more specific ones above the more general ones with similar source and destination addresses.

Configuring the SSH Sentinel for pre-shared key VPN

Creating a new VPN connection

1 Right-click on the SSH icon ⊞ and select Run Policy Editor.

Figure 3: Policy Editor Security Policy menu



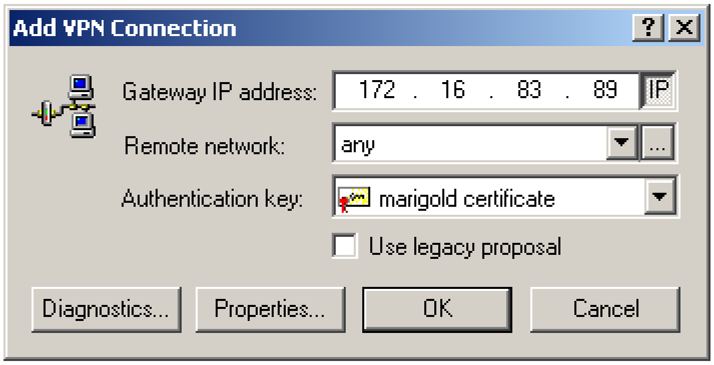
Policy : Default

Description
Add a rule.

2 Select Security Policy.

3 Select VPN Connections and select Add.

Figure 4: Adding a VPN connection



Gateway IP address: 172 . 16 . 83 . 89

Remote network: any

Authentication key: marigold certificate

□ Use legacy proposal

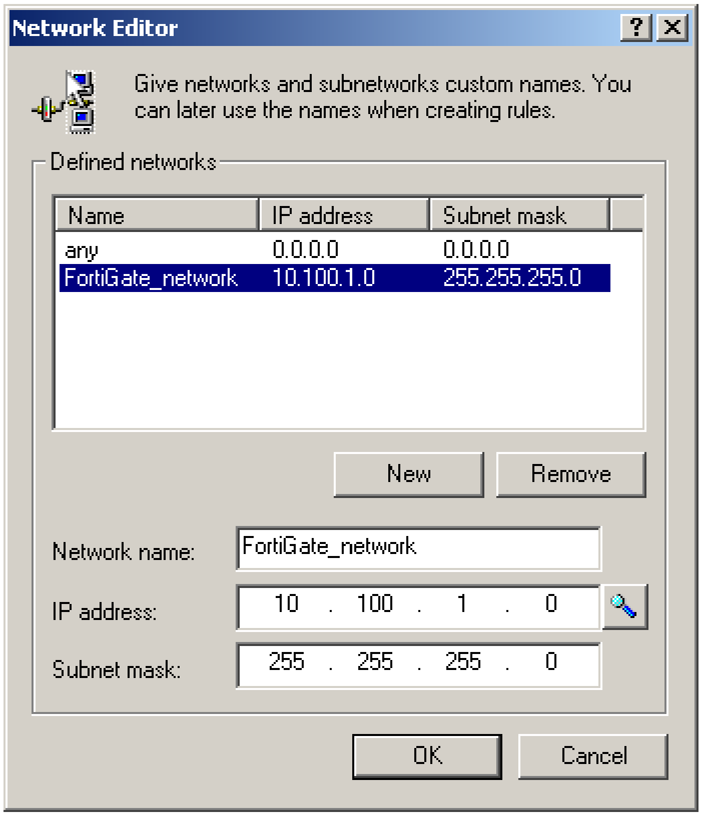
4 In the Add VPN Connection dialog box, select IP.

5 In the Gateway IP address box, enter 172.16.83.89.

6 Select ☐ to add a new remote network.

7 In the Network Editor dialog box, select New.

Figure 5: Adding a remote network in the Network Editor



Network Editor

Give networks and subnetworks custom names. You can later use the names when creating rules.

Defined networks

Name	IP address	Subnet mask
any	0.0.0.0	0.0.0.0
FortiGate_network	10.100.1.0	255.255.255.0

Network name: FortiGate_network

IP address: 10 . 100 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

8 Enter the following information, then select OK.

Network name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

Adding the pre-shared key

Note: The SSH client pre-shared key must match the FortiGate authentication key.

1 Go to **SSH Sentinel Policy Editor > Key Management > My Keys**.

2 Select Add.

3 On the New Authentication Key wizard, select Create a pre-shared key.

4 Select Next.

5 In the Pre-Shared Key Information dialog box, enter the following information, then select Finish:

Name	test
Shared secret	12345678
Confirm shared secret	12345678

Applying the pre-shared key to the VPN policy

1 Go to **SSH Sentinel Policy Editor > Security Policy**.

2 Select the VPN Connection that you added in “Creating a new VPN connection” on page 10.

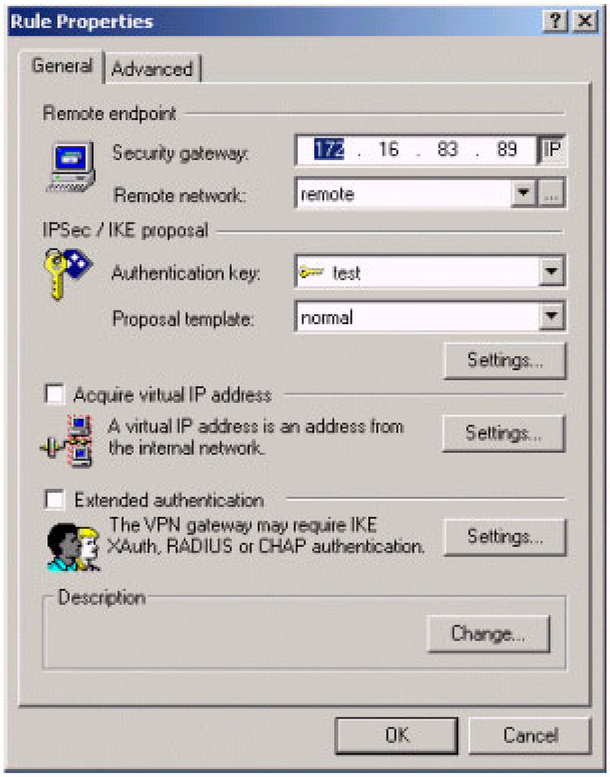
3 Select Properties.

4 In the Rule Properties dialog box, enter the following information:

Remote network	FortiGate_network
Authentication key	test

5 Under IPSec/IKE proposal, select Settings.

Figure 6: Selecting the new pre-shared key



Rule Properties

Remote endpoint

Security gateway: 172 . 16 . 83 . 89

Remote network: remote

IPSec / IKE proposal

Authentication key: test

Proposal template: normal

☐ Acquire virtual IP address

A virtual IP address is an address from the internal network.

☐ Extended authentication

The VPN gateway may require IKE XAuth, RADIUS or CHAP authentication.

Description

6 In the Proposal Parameters dialog box, select the following IKE proposal parameters:

Encryption algorithm	3DES
Integrity function	SHA-1
IKE mode	main mode
IKE group	MODP 1024 (group 2)

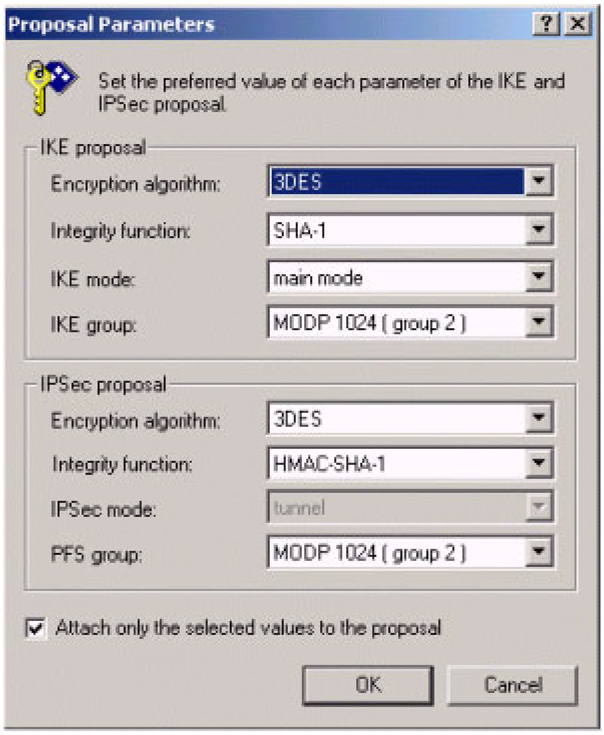
7 Select the following IPSec proposal parameters:

Encryption algorithm	3DES
Integrity function	HMAC-SHA-1
PFS group	MODP 1024 (group 2)

8 Select this option: Attach only selected values to the proposal.

9 Select OK.

Figure 7: Selecting IKE and IPSec proposal parameters



Proposal Parameters

Set the preferred value of each parameter of the IKE and IPSec proposal.

IKE proposal

Encryption algorithm: 3DES

Integrity function: SHA-1

IKE mode: main mode

IKE group: MODP 1024 (group 2)

IPSec proposal

Encryption algorithm: 3DES

Integrity function: HMAC-SHA-1

IPSec mode: tunnel

PFS group: MODP 1024 (group 2)

☑ Attach only the selected values to the proposal

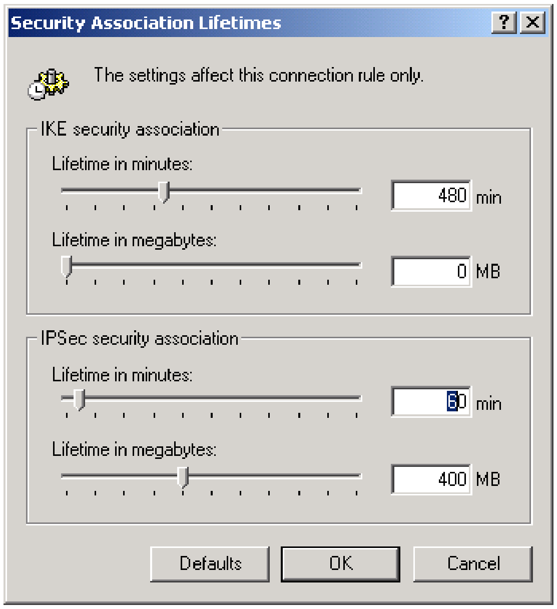
10 Go to **Rule Properties > Advanced**.

11 For Security association lifetimes, select Settings.

12 In the Security Associations dialog box, enter the following information, then select OK.

IKE security association: **Lifetime in minutes** **Lifetime in megabytes**	480 0
IPSec security association: **Lifetime in minutes** **Lifetime in megabytes**	60 400

Figure 8: Setting security association lifetimes for the VPN connection



Security Association Lifetimes

The settings affect this connection rule only.

IKE security association

Lifetime in minutes: 480 min

Lifetime in megabytes: 0 MB

IPSec security association

Lifetime in minutes: 60 min

Lifetime in megabytes: 400 MB

Testing the VPN connection

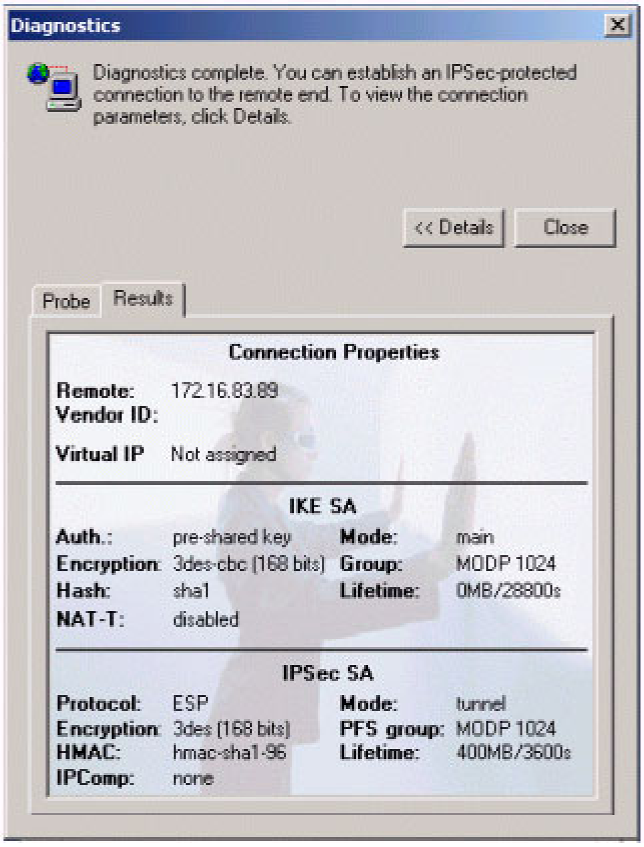
1 Go to **SSH Sentinel Policy Editor > Security Policy.**

2 Select the new VPN connection: 172.16.83.89.

3 Select Diagnostics.

If the VPN connection is active, the Diagnostics screen displays a confirmation message.

Figure 9: Testing the VPN connection



Diagnostics complete. You can establish an IPSec-protected connection to the remote end. To view the connection parameters, click Details.

Connection Properties

Remote: 172.16.83.89
Vendor ID:
Virtual IP Not assigned

IKE SA

Auth.:	pre-shared key	Mode:	main
Encryption:	3des-cbc (168 bits)	Group:	MODP 1024
Hash:	sha1	Lifetime:	0MB/28800s
NAT-T:	disabled		

IPSec SA

Protocol:	ESP	Mode:	tunnel
Encryption:	3des (168 bits)	PFS group:	MODP 1024
HMAC:	hmac-sha1-96	Lifetime:	400MB/3600s
IPComp:	none		

Starting the dialup VPN connection

Note: To automatically open any VPN connection when the Policy Manager starts, select the VPN connection in the Policy Editor, go to Properties > Advanced > Advanced options, and select Open on start-up.

1 Right-click on the SSH icon ▣.

2 Go to **Select VPN** to select the dialup VPN connection to start: 172.16.83.89 (FortiGate_network).

Viewing VPN connection status on the FortiGate unit

On the FortiGate unit, you can use the dialup monitor to view the status of dialup VPNs. The dialup monitor lists the remote gateways and the active VPN tunnels for each gateway.

1 Go to **VPN > IPSec > Dialup**.

- The Lifetime column displays how long the connection has been up.
- 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.
- The Proxy ID Source column displays the actual IP address or subnet address of the remote peer.
- The Proxy ID Destination column displays the actual IP address or subnet address of the local peer.

FortiGate to SSH Sentinel VPN with pre-shared keys (NAT traversal)

This section describes how to configure and test a dialup VPN with NAT traversal, for a network topology similar to that shown in Figure 2. In this case, the FortiGate-300 unit is the dialup server and the SSH Sentinel is the dialup client with a dynamically assigned IP address behind a FortiGate-300 NAT firewall.

You must enable NAT traversal on both the dialup server and the VPN client. Configure the FortiGate-300 unit as a dialup VPN server. Configure the SSH Sentinel as a VPN client that can connect to the FortiGate dialup server configured using the procedure in “Configuring the FortiGate unit for dialup VPN” on page 8.

General configuration steps

1 Configure the FortiGate unit as a dialup server.

- Add a remote gateway with Dialup User, Aggressive mode, and Nat-traversal selected.
- Add an AutoIKE key VPN tunnel.
- Add a source address to specify the address or address range on the FortiGate internal network that is part of the VPN.
- Add an internal to external encrypt policy that includes the source address, the destination address External_All, and the dialup VPN tunnel.
- Place the encrypt policy above the non-encrypt policies in the policy list.

2 Configure the SSH Sentinel as a dialup VPN client.

- Add a VPN connection between the SSH Sentinel and the FortiGate dialup server.
- Add the FortiGate remote network.
- Enable NAT-T for the VPN connection.
- Add the pre-shared key to be used during phase 1 negotiations.
- Apply the pre-shared key to the VPN policy and select aggressive mode.
- Configure WINS and DNS server access.
- Test the VPN connection.
- Start the VPN tunnel between the SSH Sentinel and the FortiGate dialup server.

Configuring the FortiGate unit for dialup VPN

To add the remote gateway

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

2 Select New.

3 Enter the following information, then select OK.

Gateway Name	Dialup_Clent
Remote Gateway	Dialup User
Mode	Aggressive
P1 Proposal	1-Encryption 3DES, Authentication SHA1
DH Group	2
Keylife	28800 (seconds)
Authentication Method	Preshared key
Pre-shared key	12345678 The SSH Sentinel client must use the same pre-shared key. You can use any ASCII characters for the Authentication key. 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.
Nat-traversal	Enable
Keepalive Frequency	5 (seconds)

To add the VPN tunnel

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

2 Select New.

3 Enter the following information, then select OK.

Tunnel Name	Client_IKE
Remote Gateway	Dialup_Client
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	Enable
Concentrator	None
Quick Mode Identities	Use selectors from policy

To add the source address

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

2 Select New.

3 Enter the following information, then select OK.

Address Name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

To add the firewall policy

1 Go to **Firewall > Policy > Int->Ext.**

2 Select New.

3 Enter the following information, then select OK.

Source	FortiGate_network
Destination	External_All
Schedule	Always
Service	Any
Action	ENCRYPT
VPN Tunnel	Client_IKE
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 the firewall policy.

4 Place the policy in the policy list above non-encrypt policies. If there are more than one encrypt policies in the list, place the more specific ones above the more general ones with similar source and destination addresses.

Configuring the SSH Sentinel for pre-shared key VPN

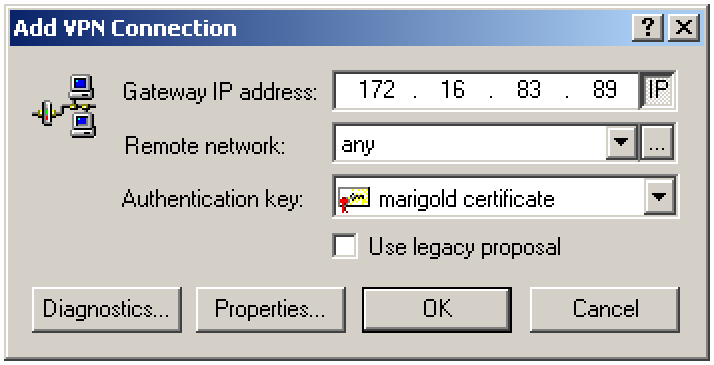
Creating a new VPN connection

1 Right-click on the SSH icon ▦ and select Run Policy Editor.

2 Select Security Policy.

3 Select VPN Connections and select Add.

Figure 10: Adding a VPN connection



Gateway IP address: 172 . 16 . 83 . 89

Remote network: any

Authentication key: marigold certificate

☐ Use legacy proposal

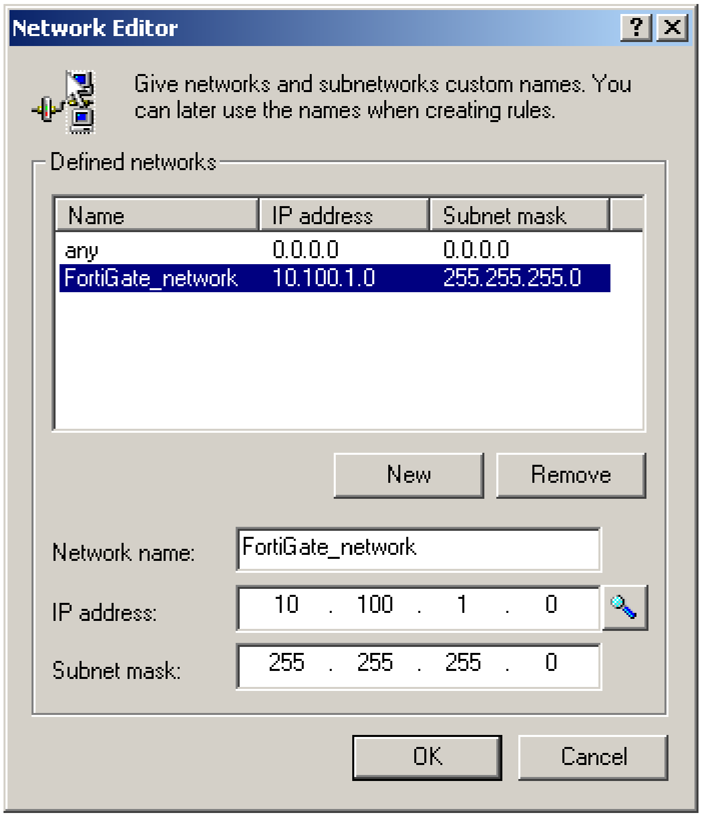
4 In the Add VPN Connection dialog box, select IP.

5 In the Gateway IP address box, enter 172.16.83.89.

6 Select … to add a new remote network.

7 In the Network Editor dialog box, select New.

Figure 11: Adding a remote network in the Network Editor



Network Editor

Give networks and subnetworks custom names. You can later use the names when creating rules.

Defined networks

Name	IP address	Subnet mask
any	0.0.0.0	0.0.0.0
FortiGate_network	10.100.1.0	255.255.255.0

Network name: FortiGate_network

IP address: 10 . 100 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

8 Enter the following information, then select OK.

Network name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

Enabling NAT traversal for the VPN connection

1 Go to **SSH Sentinel Policy Editor > Security Policy**.

2 Select 172.16.83.89.

This is the VPN Connection that you added in “Creating a new VPN connection” on page 10.

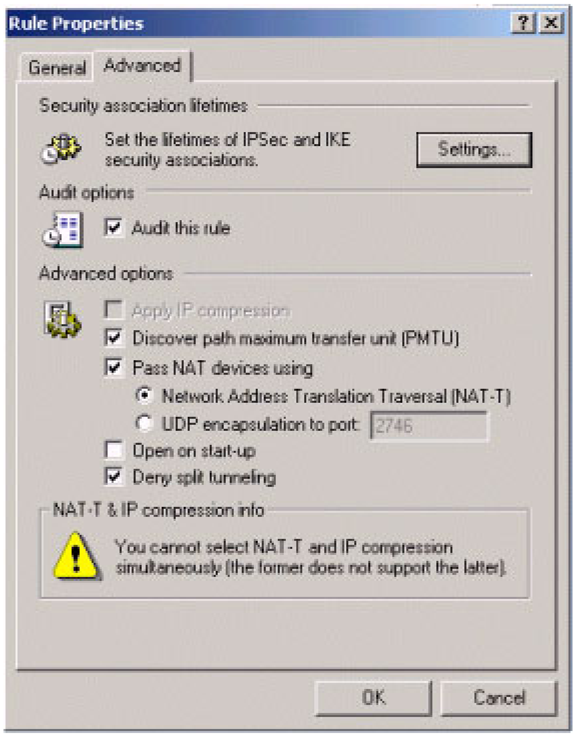
3 Select Properties.

4 Go to **Rule Properties > Advanced**.

5 For Advanced options, select this option: Pass NAT devices using: Network Address Translation Traversal (NAT-T).

6 Select OK.

Figure 12: Configuring Rule Properties > Advanced for NAT traversal



Rule Properties

General | Advanced

Security association lifetimes

Set the lifetimes of IPSec and IKE security associations. Settings...

Audit options

☑ Audit this rule

Advanced options

□ Apply IP compression

☑ Discover path maximum transfer unit (PMTU)

☑ Pass NAT devices using

● Network Address Translation Traversal (NAT-T)

○ UDP encapsulation to port: 2746

□ Open on start-up

☑ Deny split tunneling

NAT-T & IP compression info

You cannot select NAT-T and IP compression simultaneously (the former does not support the latter).

OK | Cancel

Adding the pre-shared key

Note: The SSH client pre-shared key must match the FortiGate authentication key.

1 Go to **SSH Sentinel Policy Editor > Key Management > My Keys**.

2 Select Add.

3 On the New Authentication Key wizard, select Create a pre-shared key.

4 Select Next.

5 In the Pre-Shared Key Information dialog box, enter the following information, then select Finish.

Name	test
Shared secret	12345678
Confirm shared secret	12345678

Applying the pre-shared key to the VPN policy

1 Go to **SSH Sentinel Policy Editor > Security Policy**.

2 Select the VPN Connection that you added in "Creating a new VPN connection" on page 10.

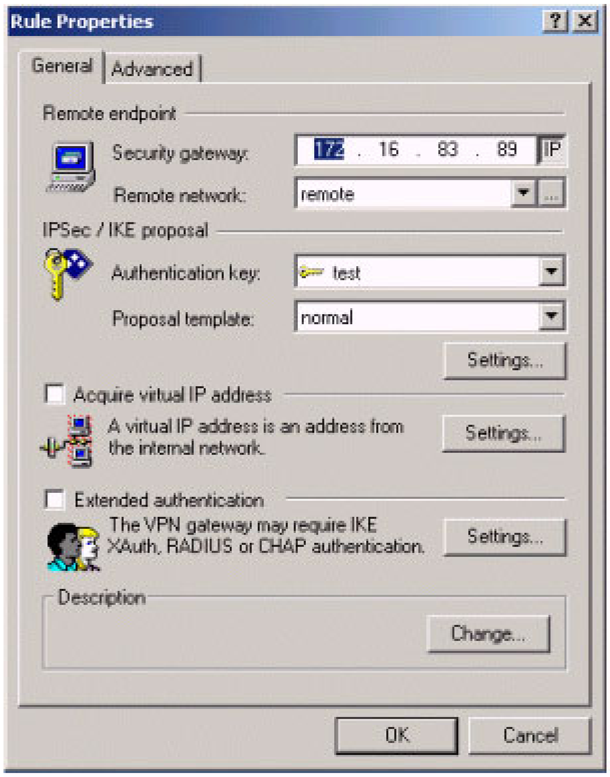
3 Select Properties.

4 In the Rule Properties dialog box, enter the following information:

Remote network	FortiGate_network
Authentication key	test

5 Under IPSec/IKE proposal, select Settings.

Figure 13: Selecting the new pre-shared key



Remote endpoint

Security gateway: 172 . 16 . 83 . 89 IP

Remote network: remote

IPSec / IKE proposal

Authentication key: test

Proposal template: normal

□ Acquire virtual IP address

A virtual IP address is an address from the internal network.

□ Extended authentication

The VPN gateway may require IKE XAuth, RADIUS or CHAP authentication.

Description

6 In the Proposal Parameters dialog box, select the following IKE proposal parameters:

Encryption algorithm	3DES
Integrity function	SHA-1
IKE mode	main mode
IKE group	MODP 1024 (group 2)

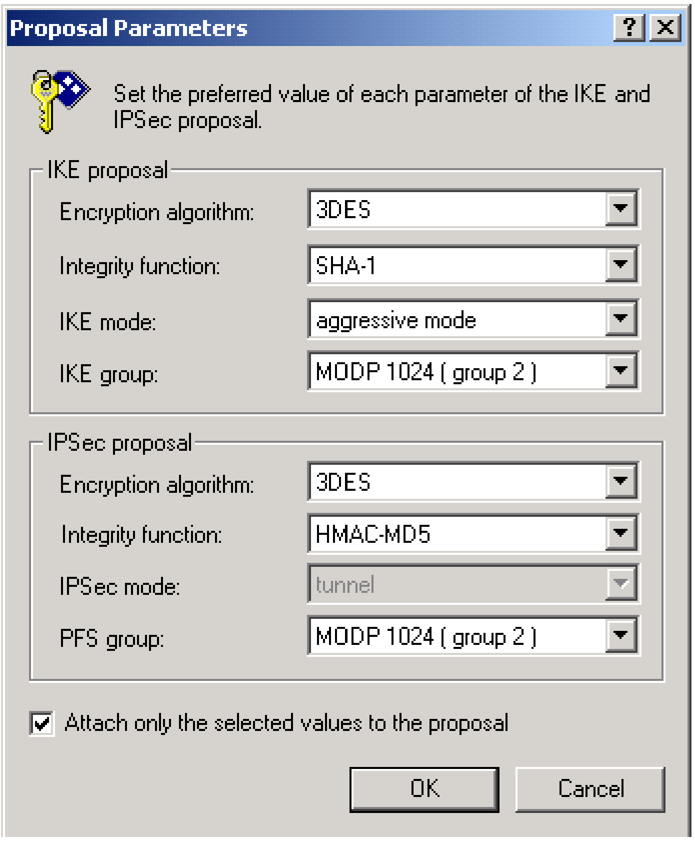
7 Select the following IPSec proposal parameters:

Encryption algorithm	3DES
Integrity function	HMAC-SHA-1
PFS group	MODP 1024 (group 2)

8 Select this option: Attach only selected values to the proposal.

9 Select OK.

Figure 14: Selecting IKE and IPSec proposal parameters



Proposal Parameters

Set the preferred value of each parameter of the IKE and IPSec proposal.

IKE proposal

Encryption algorithm: 3DES

Integrity function: SHA-1

IKE mode: aggressive mode

IKE group: MODP 1024 (group 2)

IPSec proposal

Encryption algorithm: 3DES

Integrity function: HMAC-MD5

IPSec mode: tunnel

PFS group: MODP 1024 (group 2)

☑ Attach only the selected values to the proposal

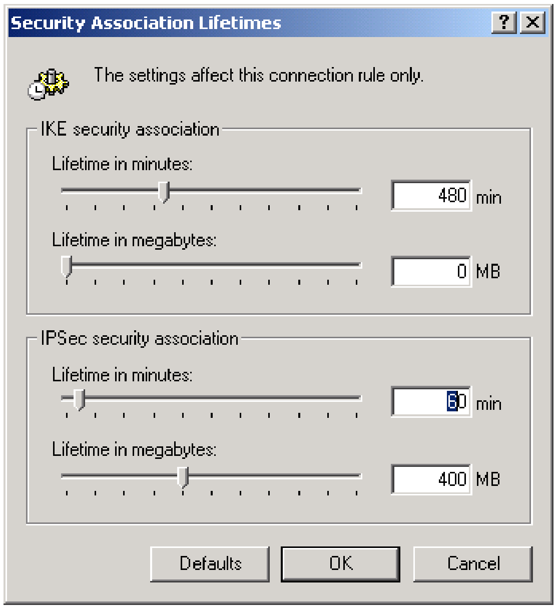
10 Go to **Rule Properties > Advanced**.

11 For Security association lifetimes, select Settings.

12 In the Security Associations dialog box, enter the following information, then select OK.

IKE security association: **Lifetime in minutes** **Lifetime in megabytes**	 480 0
IPSec security association: **Lifetime in minutes** **Lifetime in megabytes**	 60 400

Figure 15: Setting security association lifetimes for the VPN connection



Security Association Lifetimes

The settings affect this connection rule only.

IKE security association

Lifetime in minutes: 480 min

Lifetime in megabytes: 0 MB

IPSec security association

Lifetime in minutes: 60 min

Lifetime in megabytes: 400 MB

Testing the VPN connection

1. Go to **SSH Sentinel Policy Editor > Security Policy.**
2. Select the new VPN connection: 172.16.83.89.
3. Select Diagnostics.

   If the VPN connection is active, the Diagnostics screen appears with a confirmation message.

   Figure 9 shows the Diagnostics screen. In this case, the IKE SA Mode is aggressive and NAT-T is enabled.

Starting the dialup VPN connection

Note: To automatically open any VPN connection when the Policy Manager starts, select the VPN connection in the Policy Editor, go to **Properties > Advanced > Advanced options,** and select Open on start-up.

1. Right-click on the SSH icon ▦.
2. Go to **Select VPN** to select the dialup VPN connection to start: 172.16.83.89 (FortiGate_network).

Viewing VPN connection status on the FortiGate unit

On the FortiGate unit, you can use the dialup monitor to view the status of dialup VPNs. The dialup monitor lists the remote gateways and the active VPN tunnels for each gateway.

1 Go to **VPN > IPSec > Dialup**.

- The Lifetime column displays how long the connection has been up.
- 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.
- The Proxy ID Source column displays the actual IP address or subnet address of the remote peer.
- The Proxy ID Destination column displays the actual IP address or subnet address of the local peer.

FortiGate to SSH Sentinel VPN with certificates

This section describes how to configure and test a FortiGate to SSH Sentinel dialup VPN in main mode, for a network topology similar to that shown in Figure 1. The FortiGate unit is the dialup server and the SSH Sentinel is the dialup client with a dynamically assigned IP address. In this case, the VPN participants uses certificates, instead of the pre-shared keys.

General steps for certificate management

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, before an encrypted VPN tunnel is set up between the participants.

You require both a signed local certificate and a CA certificate. The local certificate is the digital certificate that the FortiGate unit uses to authenticate itself to other devices.The CA certificate is the certificate that the FortiGate unit uses to validate digital certificates received from other devices.

General configuration steps to obtain a signed local certificate

To obtain a signed local certificate, complete these steps:

1 Generate the certificate request.

This procedure creates a private and public key pair for the local FortiGate unit. The public key accompanies the certificate request. The private key remains confidential.

See “Generating the certificate request” on page 27.

2 Download the certificate request to the management computer.

See Downloading the certificate request.

3. Submit the certificate request to the CA.

   Copy the certificate request from the downloaded text file and paste it into a web page form controlled by the CA. The CA will notify you after it has signed the request. You must then go to the web server operated by the CA, copy the signed certificate and save it to your local computer.

   See "Requesting the signed local certificate" on page 28.

4. Import the signed certificate to the FortiGate unit.

   See "Importing the signed local certificate" on page 29.

General configuration steps to obtain a CA certificate

To obtain a CA certificate, complete these steps:

1. Retrieve the CA certificate.

   Connect to the web page controlled by the CA, copy the CA certificate and save it to your local computer. The CA certificate includes a certificate path which grants legitimacy to all certificates issued by the CA.

   See "Downloading a CA certificate" on page 29.

2. Import the CA certificate to the Fortigate unit.

   See "Importing a CA certificate" on page 29.

Obtaining a signed local certificate for the FortiGate unit

The signed local certificate provides the FortiGate unit with a means to authenticate itself to other devices.

Note: The VPN peers must use digital certificates that adhere to the X.509 standard.

Generating the certificate request

To generate the certificate request

1. Go to **VPN > Local Certificates**.
2. Select Generate.
3. Enter a Certificate Name.

   Typically, this is the name of the FortiGate unit being certified.

   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4. Configure the Subject Information that identifies the FortiGate unit being certified.

   Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an email address.

Host IP	For Host IP, enter the IP address of the FortiGate unit being certified.

Domain Name For Domain name, enter the fully qualified domain name of the FortiGate unit being certified. Do not include the protocol specification (http://) or any port number or path names.

E-Mail For E-mail, enter the email address of the owner of the FortiGate unit being certified. Typically, email addresses are entered only for clients, not gateways.

Note: If you specify a host IP or domain name, use the IP address or domain name associated with the interface on which IKE negotiations will take place (e.g. the external interface of the local FortiGate unit). If the IP address in the certificate does not match the IP address of the local interface (or if the domain name in the certificate does not match a DNS query of the FortiGate unit's IP), then some implementations of IKE may reject the connection. Enforcement of this rule varies for different IPSec products.

5. Configure the Optional Information to further identify the object being certified.

Organization Unit Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit.

Organization Enter the name of the organization that is requesting the certificate for the FortiGate unit.

Locality (City) Enter the name of the city, or town, where the person or organization certifying the FortiGate unit resides.

State/Province Enter the name of the state or province where the FortiGate unit is located.

Country Select the country where the FortiGate unit is located.

e-mail Enter a contact e-mail address for the FortiGate unit.

6. Configure the key.

Key Type Select RSA as the key encryption type. No other key type is supported.

Key Size Select one of 1024 Bit, 1536 Bit or 2048 Bit. If you do not specify a key size, 1024 Bit will be used. Larger keys are slower to generate but more secure.

7. Select OK to generate the private and public key pair and the certificate request.
   The certificate request will be displayed on the Local Certificates list with a status of Pending.

Downloading the certificate request

To download the certificate request

1. Go to **VPN > Local Certificates**.
2. Select Download to download the local certificate to the management computer.
   The File Download dialog will display.
3. Select Save.
4. Name the file and save it on the management computer.

Requesting the signed local certificate

To request the signed local certificate

1. On the management computer, open the certificate request file in a text editor.
2. Copy the certificate request.

3 Connect to the CA web server.

4 Request the signed local certificate.

Follow the CA web server instructions to:

- add a base64 encoded PKCS#10 certificate request to the CA web server,
- paste the certificate request to the CA web server,
- submit the certificate request to the CA web server.

The certificate request is submitted to the CA for it to sign.

5 After the certificate is signed, select Base 64 encoded, then select Download CA certificate. The File Download dialog will display.

6 Select Save.

7 Name the file and save it on the management computer.

Importing the signed local certificate

To import the signed local certificate

1 Go to **VPN > Local Certificates**.

2 Select Import.

3 Enter the path or browse to locate the file containing the signed local certificate.

4 Select OK.

The signed local certificate will be displayed on the Local Certificates list with a status of OK.

Obtaining a CA certificate

For the VPN peers to authenticate themselves to each other, they must both obtain a CA certificate from the same certificate authority.

Note: The CA certificate must adhere to the X.509 standard.

Downloading a CA certificate

To download the CA certificate

1 Connect to the CA web server.

2 Follow the CA web server instructions to download the CA certificate.

The File Download dialog will display.

3 Select Save.

4 Name the file and save it on the management computer.

Importing a CA certificate

To import the CA certificate

1 Go to **VPN > CA Certificates**.

2 Select Import.

3 Enter the path or browse to locate the file containing the CA certificate.

4 Select OK.
The CA certificate appears on the CA Certificates list.

Configuring the FortiGate unit for dialup VPN

General configuration steps

- Add a remote gateway with Dialup User.
- Add an AutoIKE key VPN tunnel.
- Add a source address to specify the address or address range on the FortiGate internal network that is part of the VPN.
- Add an internal to external encrypt policy that includes the source address, the destination address External_All, and the dialup VPN tunnel.
- Place the encrypt policy above the non-encrypt policies in the policy list.

To add the remote gateway

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

2 Select New.

3 Enter the following information, then select OK.

Gateway Name	Dialup_Clent
Remote Gateway	Dialup User
Mode	Main (ID Protection)
P1 Proposal	1-Encryption 3DES, Authentication SHA1
DH Group	2
Keylife	28800 (seconds)
Authentication Method	RSA Signature
Certificate Name	Select the signed local certificate that you want to use from the list.

To add the VPN tunnel

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

2 Select New.

3 Enter the following information and select OK.

Tunnel Name	Client_IKE
Remote Gateway	Dialup_Client
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	Enable
Concentrator	None
Quick Mode Identities	Use selectors from policy

To add the source address

1. Go to **Firewall > Address > Internal.**
2. Select New.
3. Enter the following information, then select OK.

Address Name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

To add the firewall policy

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

Source	FortiGate_network
Destination	External_All
Schedule	Always
Service	Any
Action	ENCRYPT
VPN Tunnel	Client_IKE
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 the firewall policy.

4 Place the policy in the policy list above non-encrypt policies. If there are more than one encrypt policies in the list, place the more specific ones above the more general ones with similar source and destination addresses.

Configuring SSH Sentinel

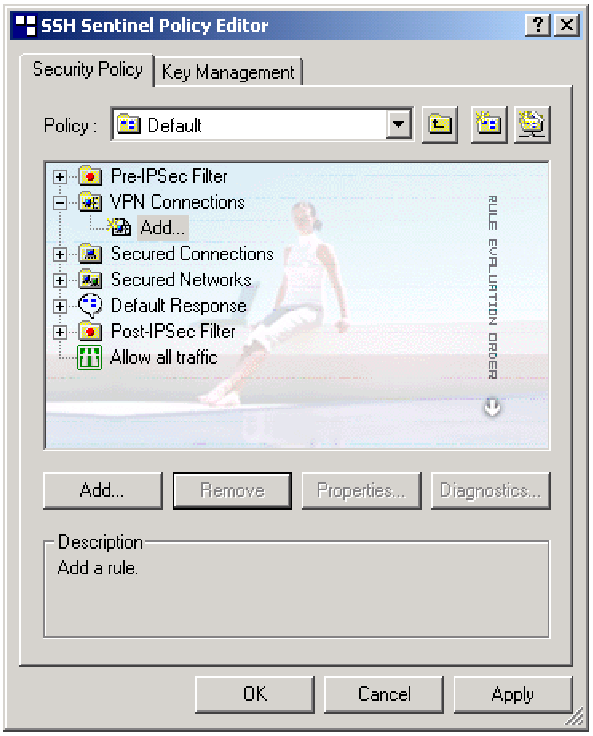
General configuration steps

- Add a VPN connection between the SSH Sentinel and the FortiGate dialup server.
- Add the FortiGate remote network.
- Add a signed local certificate.
- Apply the local certificate to the VPN policy.
- Add the CA certificate.
- Configure WINS and DNS server access.
- Test the VPN connection.
- Start the VPN tunnel between the SSH Sentinel and the FortiGate dialup server.

Creating a new VPN connection

1 Right-click the SSH icon ⊞ and select Run Policy Editor.

Figure 16: Policy Editor Security Policy menu



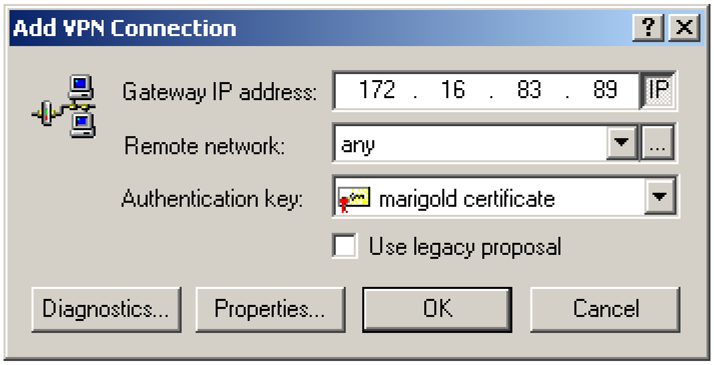
Policy : Default

Description
Add a rule.

2 Select the Security Policy tab.

3 Select VPN Connections and select Add.

Figure 17: Adding a VPN connection



Gateway IP address: 172 . 16 . 83 . 89

Remote network: any

Authentication key: marigold certificate

□ Use legacy proposal

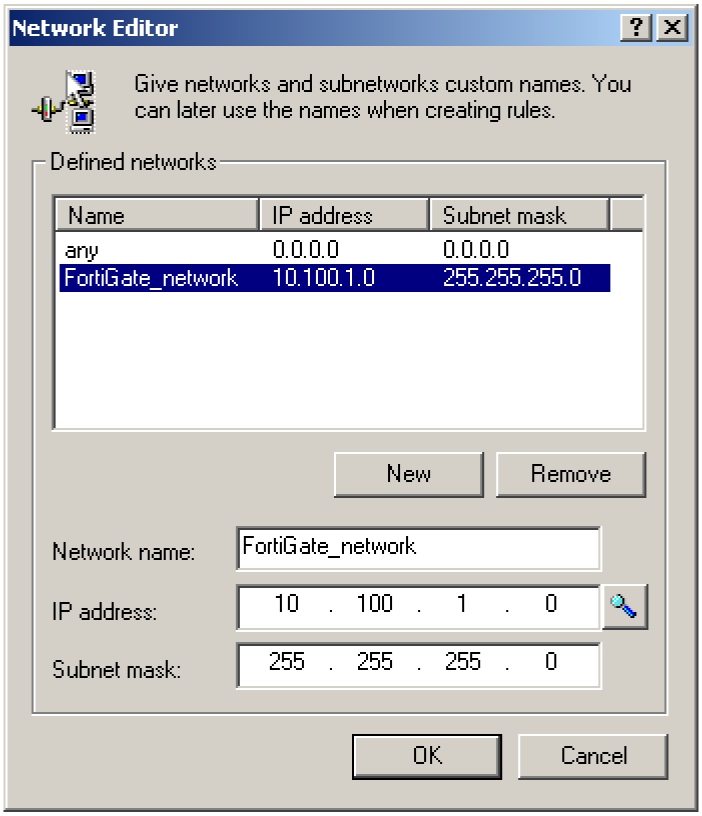
4 In the Add VPN Connection dialog box, select IP.

5 In the Gateway IP address box, enter 172.16.83.89.

6 Select ... to add a new remote network.

7 In the Network Editor dialog box, select New.

Figure 18: Adding a remote network in the Network Editor



Network Editor

Give networks and subnetworks custom names. You can later use the names when creating rules.

Defined networks

Name	IP address	Subnet mask
any	0.0.0.0	0.0.0.0
FortiGate_network	10.100.1.0	255.255.255.0

Network name: FortiGate_network

IP address: 10 . 100 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

8 Enter the following information, then select OK.

Network name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

Creating the certificate request

1 Go to **SSH Sentinel Policy Editor > Key Management > My Keys**.

2 Select Add.

3 In the New Authentication Key dialog box, select Create an authorized key pair and a certificate.

4 Follow the instructions to generate the key pair and then select Next.

5 In the Certificate Information dialog box, select and enter an identifier, then click Next.

6 In the Certificate Enrollment dialog box, select the option: Create a certification request and save it in a file for later enrollment.

7 In the Certification Request dialog box, save the file and click Finish.

Requesting and retrieving the signed local certificate

For detailed procedures, see “Requesting and retrieving the signed local certificate” on page 35 and “Importing the signed local certificate” on page 29.

Importing the signed local certificate

To import the signed local certificate

1 Right-click on the SSH icon ▦ and select Run Policy Editor.

2 Select the Key Management tab.

3 Right-click on My Keys.

4 From the popup menu, select Import.

5 Locate the signed local certificate that you obtained in “Requesting and retrieving the signed local certificate” on page 35, and select Open. The certificate will appear in the My Keys list.

Applying the local certificate to the VPN policy

1 Go to **SSH Sentinel Policy Editor > Security Policy**.

2 Select the VPN Connection that you added in “Creating a new VPN connection” on page 32.

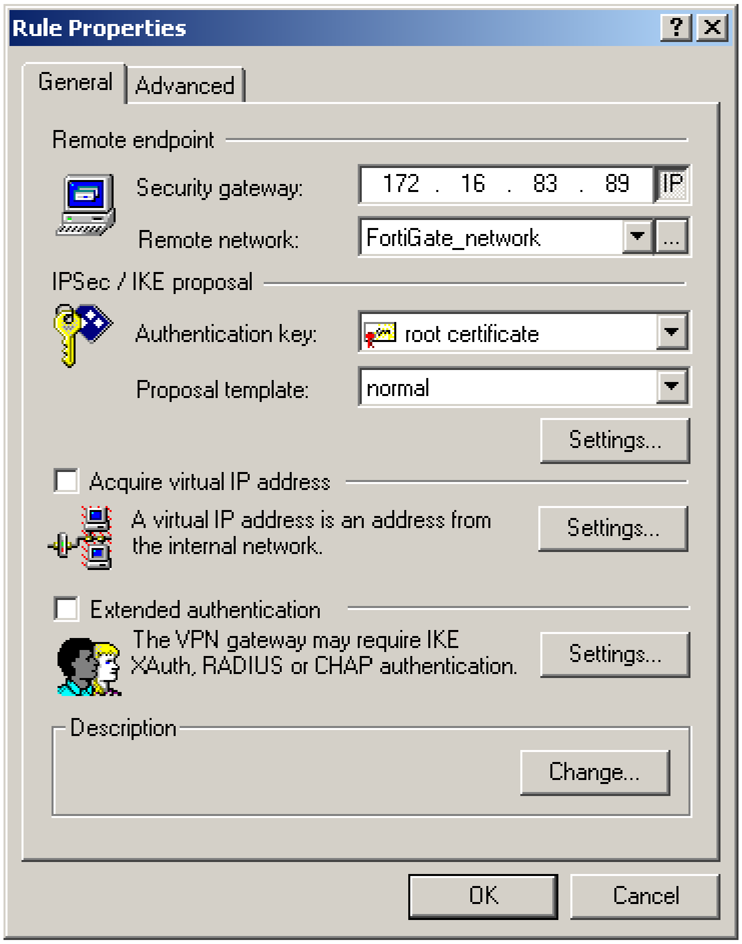
3 Select Properties.

4 In the Rule Properties dialog box, enter the following information:

Remote network	FortiGate_network
Authentication key	Root certificate

5 Under IPSec/IKE proposal, select Settings.

Figure 19: Selecting the new pre-shared key



Remote endpoint

Security gateway: 172 . 16 . 83 . 89 IP

Remote network: FortiGate_network

IPSec / IKE proposal

Authentication key: root certificate

Proposal template: normal

□ Acquire virtual IP address

A virtual IP address is an address from the internal network.

□ Extended authentication

The VPN gateway may require IKE XAuth, RADIUS or CHAP authentication.

Description

6 In the Proposal Parameters dialog box, select the following IKE proposal parameters:

Encryption algorithm	3DES
Integrity function	SHA-1
IKE mode	main mode
IKE group	MODP 1024 (group 2)

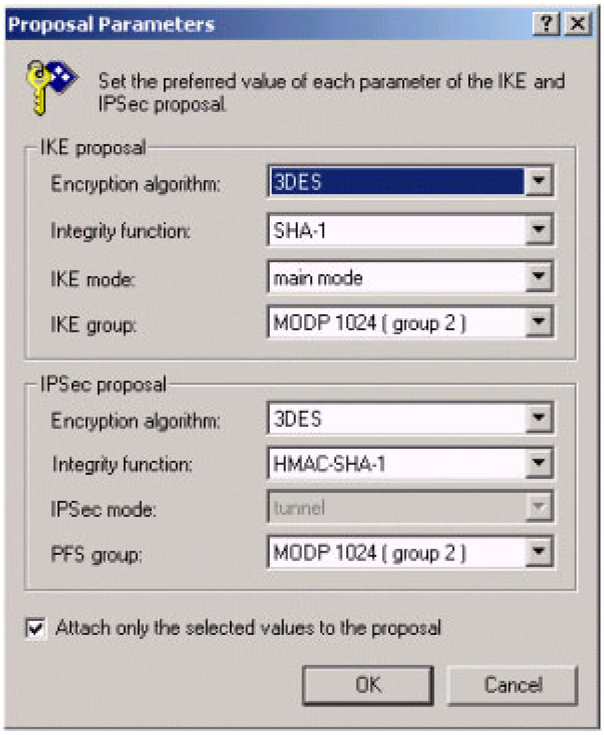
7 Select the following IPSec proposal parameters:

Encryption algorithm	3DES
Integrity function	HMAC-SHA-1
PFS group	MODP 1024 (group 2)

8 Select this option: Attach only selected values to the proposal.

9 Select OK.

Figure 20: Selecting IKE and IPSec proposal parameters



Proposal Parameters

Set the preferred value of each parameter of the IKE and IPSec proposal.

IKE proposal

Encryption algorithm: 3DES

Integrity function: SHA-1

IKE mode: main mode

IKE group: MODP 1024 (group 2)

IPSec proposal

Encryption algorithm: 3DES

Integrity function: HMAC-SHA-1

IPSec mode: tunnel

PFS group: MODP 1024 (group 2)

☑ Attach only the selected values to the proposal

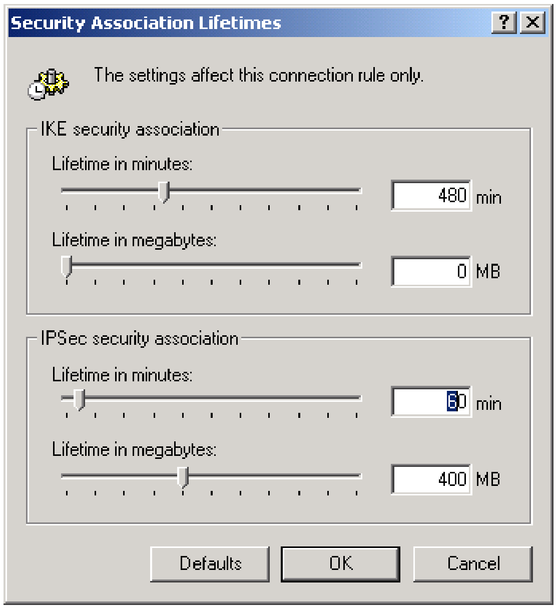
10 Go to **Rule Properties > Advanced**.

11 For Security association lifetimes, select Settings.

12 In the Security Associations dialog box, enter the following information, then select OK.

IKE security association: **Lifetime in minutes** **Lifetime in megabytes**	 480 0
IPSec security association: **Lifetime in minutes** **Lifetime in megabytes**	 60 400

Figure 21: Setting security association lifetimes for the VPN connection



Security Association Lifetimes

The settings affect this connection rule only.

IKE security association

Lifetime in minutes: 480 min

Lifetime in megabytes: 0 MB

IPSec security association

Lifetime in minutes: 60 min

Lifetime in megabytes: 400 MB

Obtaining a CA certificate

See “Downloading a CA certificate” on page 29.

Adding the CA certificate

1 Go to **SSH Sentinel Policy Editor > Key Management > Trusted Certificates > Certification Authorities.**

2 Select Add.

3 Locate the CA certificate you obtained, then select Open.

4 Select Apply.
The CA certificate is added to the Certification Authorities list.

Testing the VPN connection

1 Go to **SSH Sentinel Policy Editor > Security Policy.**

2 Select the new VPN connection: 172.16.83.89.

3 Select Diagnostics.
If the VPN connection is active, the Diagnostics screen appears with a confirmation message.

Starting the dialup VPN connection

Note: To automatically open any VPN connection when the Policy Manager starts, select the VPN connection in the Policy Editor, go to **Properties > Advanced > Advanced options,** and select Open on start-up.

1 Right-click on the SSH icon ▞.

2 Go to **Select VPN** to select the dialup VPN connection to start: 172.16.83.89 (FortiGate_network).

Viewing VPN connection status on the FortiGate unit

On the FortiGate unit, you can use the dialup monitor to view the status of dialup VPNs. The dialup monitor lists the remote gateways and the active VPN tunnels for each gateway.

1 Go to **VPN > IPSec > Dialup**.

- The Lifetime column displays how long the connection has been up.
- 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.
- The Proxy ID Source column displays the actual IP address or subnet address of the remote peer.
- The Proxy ID Destination column displays the actual IP address or subnet address of the local peer.

Managing SSH Sentinel policies

SSH Sentinel IPSec policies are either local policies or centrally managed policies. You can update your local policies. Only central management can update centrally managed policies.

This section describes:

- Exporting SSH Sentinel IPSec policies
- Importing SSH Sentinel IPSec pre-shared key policies
- Sharing policies
- Removing policies

Exporting SSH Sentinel IPSec policies

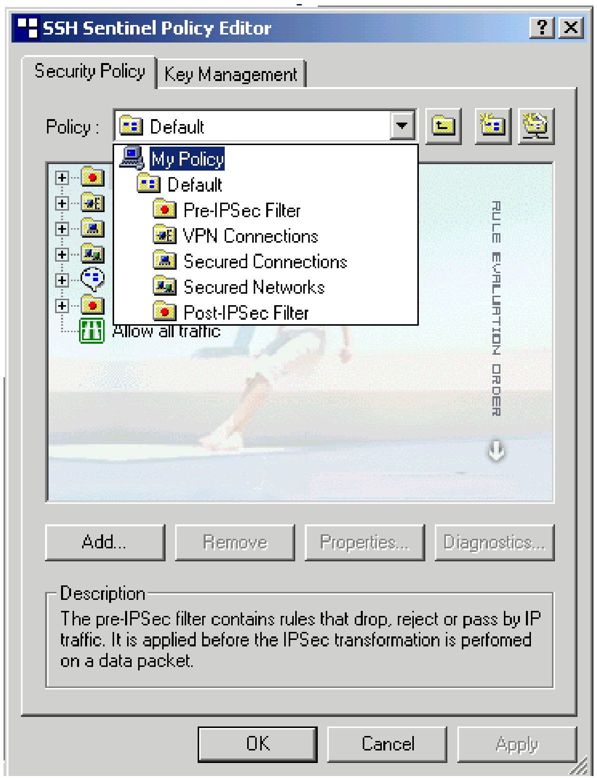
Export IPSec policies to make it easier to configure multiple SSH Sentinel VPN clients. If you configure one SSH Sentinel VPN client, you can export its configuration to a file and then import this configuration to other SSH Sentinel VPN clients (see “Importing SSH Sentinel IPSec pre-shared key policies” on page 41).

To export SSH Sentinel IPSec policies

1 Right-click on the SSH icon ⊞ and select Run Policy Editor to open the SSH Sentinel Security Policy Editor.

2 From the Policy list, select My Policy to list all policies.

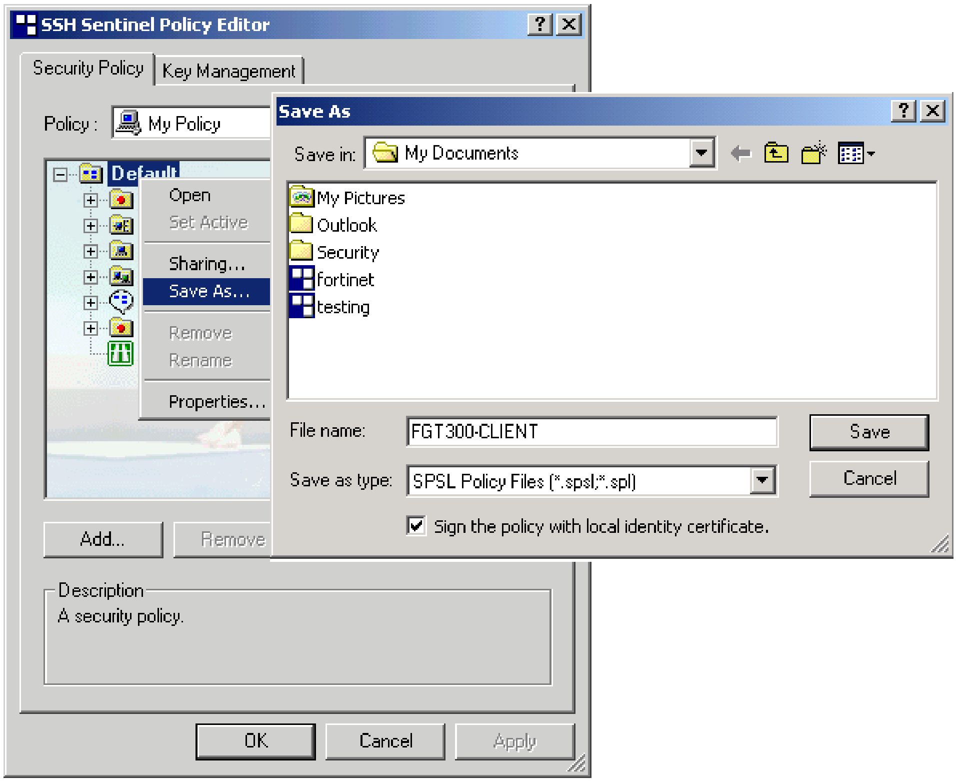
Figure 22: Selecting My Policy to list all policies



The pre-IPSec filter contains rules that drop, reject or pass by IP traffic. It is applied before the IPSec transformation is perfomed on a data packet.

3 Right-click on the policy to be exported and select Save As.
For example, right-click on Default to export the default policy (Figure 23).

Figure 23: Exporting the Default policy



Policy : My Policy

Save in: My Documents

File name: FGT300-CLIENT

Save as type: SPSL Policy Files (*.spsl;*.spl)

☑ Sign the policy with local identity certificate.

Description
A security policy.

4 Save the policy file to a diskette or hard disk.

5 SSH Sentinel saves the export file and displays a confirmation message.

Importing SSH Sentinel IPSec pre-shared key policies

When you export policies that contain pre-shared keys, for security reasons the SSH Sentinel does not export the pre-shared key. Importing pre-shared key policies requires:

- Importing the policy
- Adding the pre-shared key
- Activating the newly imported policy

Importing the policy

1 Right-click on the SSH icon ⊞ and select Run Policy Editor to open the SSH Sentinel Security Policy Editor.

2 Select Add to add a new policy.

3 Enter a Policy name.

4 In the Source type list, select Open file.

Note: If you are importing the policy from a remote host, select SSH Sentinel. Specify the IP address and policy name.

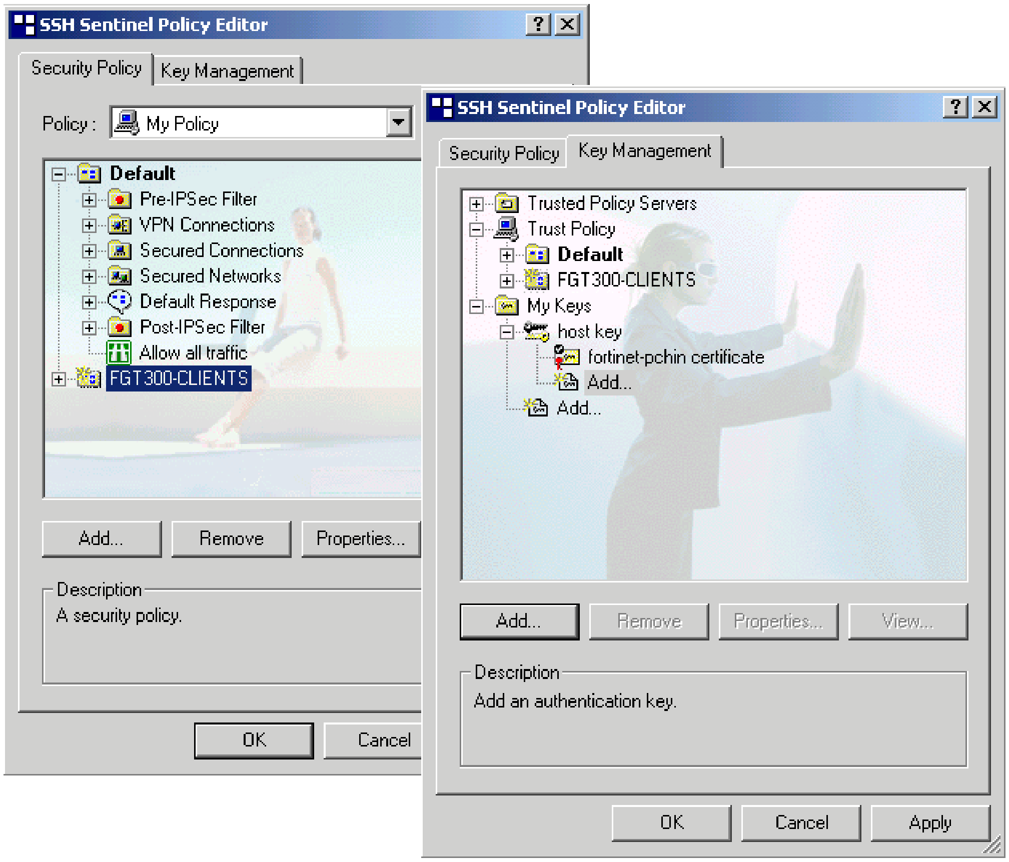
Note: If you are importing the policy from an LDAP server, select LDAP server. Specify the IP address, base object distinguished name (DN) (mandatory), and the policy name (optional) in the additional fields that appear.

5 Select the file to be imported.

6 Select OK to import the policy.

7 Select Yes to accept the certificate and add the policy.

Figure 24: New Policy added to Policy Editor and Key Management list



Policy : My Policy

Description
A security policy.

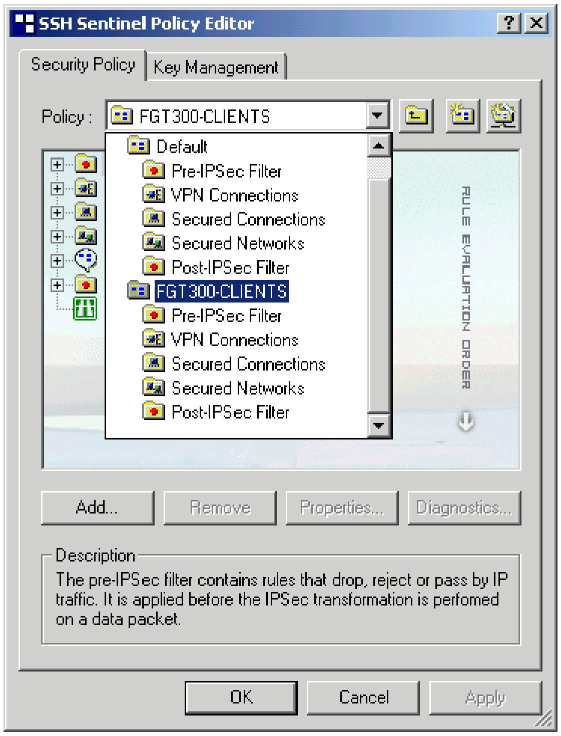
Description
Add an authentication key.

Adding the pre-shared key

To add a pre-shared key to an imported policy:

1 Select the newly imported policy from the Policy list.
For example, right-click on FGT300-CLIENTS (Figure 25).

Figure 25: New policy added to Key Management list

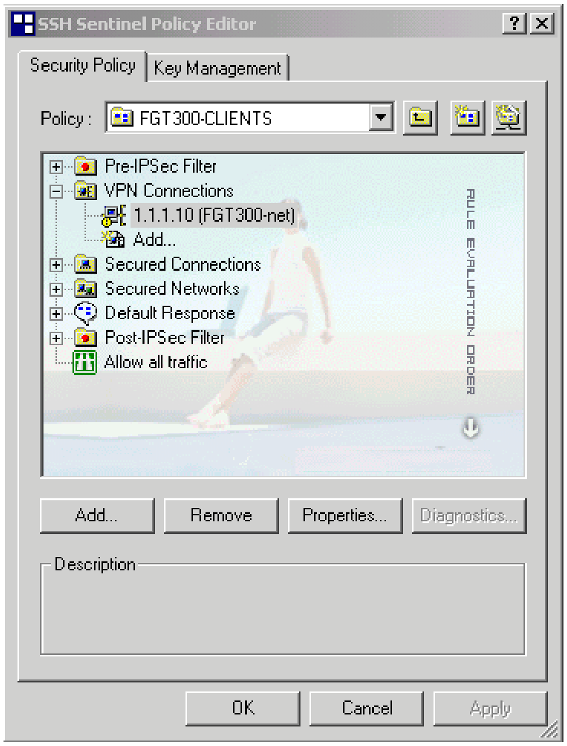


The pre-IPSec filter contains rules that drop, reject or pass by IP traffic. It is applied before the IPSec transformation is perfomed on a data packet.

2 Select VPN Connections and highlight the existing VPN settings.

3 Select Properties.

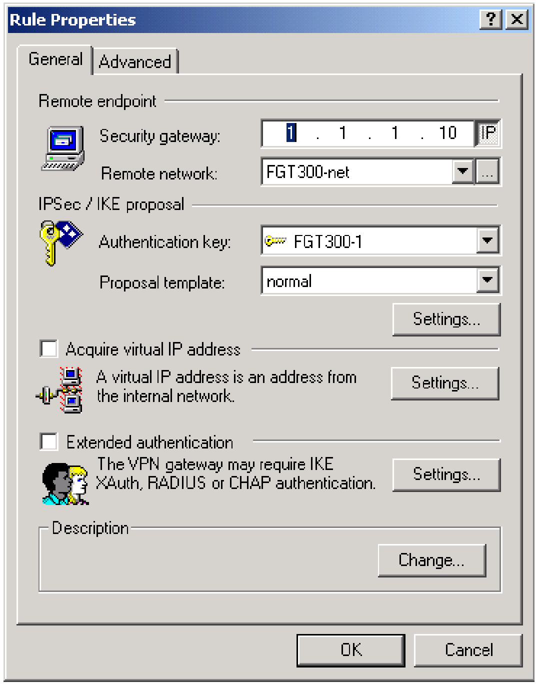
Figure 26: Selecting VPN settings



4 Select the new pre-shared key from the Authentication list.

5 Click OK twice to close Rule Properties and to close the Policy Editor.

Figure 27: Select the pre-shared key



Remote endpoint

Security gateway: 1 . 1 . 1 . 10 IP

Remote network: FGT300-net

IPSec / IKE proposal

Authentication key: FGT300-1

Proposal template: normal

☐ Acquire virtual IP address

A virtual IP address is an address from the internal network.

☐ Extended authentication

The VPN gateway may require IKE XAuth, RADIUS or CHAP authentication.

Description

Activating the newly imported policy

1. To activate the newly imported policy, right-click on the SSH icon ⊞. Choose Select Active policy and highlight the newly imported policy.
2. To run the newly imported policy, right-click on the SSH icon ⊞. Choose Select VPN and highlight the newly imported policy.

Sharing policies

Policy Properties > Sharing is available only if a local policy is in question. You can choose not to share the policy, share the policy on the local host, or publish it on a remote server.

Unsharing a local policy

Not shared is the default setting; if selected, other users cannot share this policy.

1. Right-click on the SSH icon ⊞ and select Run Policy Editor.
2. Go to **Security Policy** and highlight the policy to share.
3. Right-click on the highlighted policy and select Sharing.
4. Select Not shared.
5. Select OK.

Sharing a local policy

If Shared is selected, other users can share this policy. To fetch the policy, the remote end must support the Simple Policy Retrieval Protocol (SPRP). On the remote host, this policy appears as a centrally managed policy: it cannot be modified on the remote host and your changes to the policy will be reflected to it.

1. Right-click on the SSH icon and select Run Policy Editor.
2. Go to **Security Policy** and highlight the policy to share.
3. Right-click on the highlighted policy and select Sharing.
4. Select Shared.
5. Select OK.

Note: Alternatively, you can select Export to save this policy to a different location. See "Exporting SSH Sentinel IPSec policies" on page 39.

Publishing a local policy to an LDAP server

If Publish to a remote LDAP server is selected, you make this policy available for downloading on a remote LDAP server.

1. Right-click on the SSH icon and select Run Policy Editor.
2. Go to **Security Policy** and highlight the policy to share.
3. Right-click on the highlighted policy and select Sharing.
4. Select Publish to a remote LDAP server.
5. Select LDAP Properties.
6. Enter the server address (for example, ldap@mycompany.com).
7. Enter the base object distinguished name (DN) (for example, "cn=Policy Server, o=SSH, c=FI").

Note: The quotation marks are mandatory if there are any special characters in the string.

8. Select Submit login information to access if needed, and enter the user name and password.
9. Select OK.

Note: Alternatively, you can select Export to save this policy to a different location. See "Exporting SSH Sentinel IPSec policies" on page 39.

Removing policies

1. Right-click on the SSH icon and select Run Policy Editor.
2. Go to **Security Policy** and highlight the policy to remove.
3. Right-click on the highlighted policy and select Remove.
4. To make the removal permanent, select Apply.

   You cannot remove the active policy.