FortiGate to Netscreen-204 IPSec VPN Interoperability

Technical Note

FortiGate to Netscreen-204 IPSec VPN Interoperability Technical Note	
Document Version:	Version 1
Publication Date:	15 March 2005
Description:	This technical note demonstrates how to set up a policy based IPSec VPN tunnel between a FortiGate-800 Antivirus Firewall and a Juniper Networks Netscreen-204 appliance. In the configuration example, the two VPN peers use preshared keys to authenticate each other.
Product:	FortiGate v2.80 MR7 Netscreen-204 Version 5.1 and ScreenOS 4.0.0
Document Number:	01-280007-0147-20050315

Fortinet Inc.

FortiGate to Netscreen-204 IPSec VPN Interoperability Technical Note
FortiGate v2.80 MR7
15 March 2005
01-280007-0147-20050315

Table of Contents

Network topology 5
Infrastructure requirements 6
Configuring the FortiGate-800 6
Define the phase 1 parameters 6
Define the phase 2 parameters 7
Define the firewall encryption policy 8
Configuring the Netscreen-204 appliance 9
Monitoring and testing the VPN tunnel 10

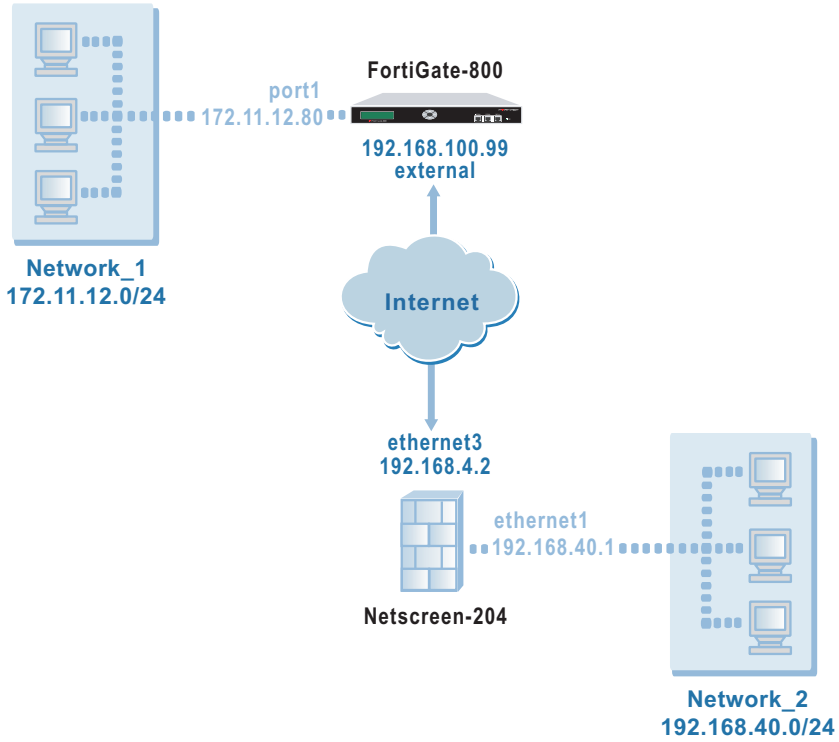
This technical note demonstrates how to set up a policy based IPSec VPN tunnel between a FortiGate-800 Antivirus Firewall and a Juniper Networks Netscreen-204 appliance. In the configuration example, the two VPN peers use preshared keys to authenticate each other. This technical note contains the following sections:

- Network topology
- Configuring the FortiGate-800
- Configuring the Netscreen-204 appliance
- Monitoring and testing the VPN tunnel

Network topology

Figure 1 shows an example network configuration. Computers on private Network_2 behind the Netscreen-204 appliance can access private Network_1 through the FortiGate-800 unit. All traffic generated by computers on Network_2 network is subject to a FortiGate firewall encryption policy.

Figure 1: FortiGate-800 to Netscreen-204 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.

Define the phase 1 parameters

The phase 1 configuration defines the parameters that the FortiGate unit will use to authenticate the Netscreen-204 appliance and establish a secure connection. For the purposes of this example, a preshared key will be used to authenticate the Netscreen-204 appliance. The same preshared key must be specified at the FortiGate-800 and the Netscreen-204 appliance.

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, and select OK:

Gateway Name	Type a name for the remote gateway (for example, `Netscreen-204`).
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	For DH Group, select 2 (the Netscreen default setting). The FortiGate setting must be identical to the current Netscreen setting.

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 and select OK:

Tunnel Name	Enter a name for the tunnel (for example, `ns_204`).
Remote Gateway	Select the gateway that you defined previously (for example, `Netscreen-204`).
Advanced	Select these Advanced options: • Clear Enable replay detection (by default, the Netscreen setting is off). The FortiGate setting must be identical to the current Netscreen setting. • Set DH Group to 2 (the Netscreen default setting). The FortiGate setting must be identical to the current Netscreen setting. • Set Keylife to 3600 seconds (the Netscreen default setting). The FortiGate setting must be identical to the current Netscreen setting. • Set Autokey Keep Alive to Enable (by default, the Netscreen setting is on). The FortiGate setting must be identical to the current Netscreen setting. • Under Quick Mode Identities, select Specify a selector. (A route-based configuration would need to have the Use wildcard selectors option selected instead.)

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 Netscreen-204 appliance.

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 Netscreen-204 appliance

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 Netscreen-204 appliance (for example, `192.168.40.0/24`).

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	`ns_204`

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

Configuring the Netscreen-204 appliance

Configuring a Netscreen-204 appliance is similar to configuring a FortiGate unit:

- Define the remote gateway and configure the AutoKey (phase 1 IPSec) parameters that the appliance needs to authenticate the FortiGate unit and establish a secure connection.
- Configure the AutoKey IKE (phase 2 IPSec) parameters that the appliance needs to create a VPN tunnel with the FortiGate unit.
- Completing the VPN configuration, which includes defining the IP source and destination addresses and creating bidirectional policies.

To define the remote gateway and the Netscreen-204 AutoKey parameters

1 Using a web browser, connect to the Netscreen-204 configuration interface.

2 Go to **VPNs > AutoKey Advanced > Gateway** and select New.

3 Enter the following information, and select OK:

Gateway Name	`FortiGate800`
Security Level	Custom
Remote Gateway Type	Select Static IP Address, and then in the IP Address/Hostname field, type `192.168.100.99`.
Preshared Key	Enter the preshared key. The value must be identical to the preshared key that you specified previously in the FortiGate-800 configuration.
Outgoing Interface	Select ethernet3.
Advanced	Select these Advanced options: • Under Security Level, set User Defined to Custom, and then from the first and second lists, select pre-g2-3des-sha and pre-g2-3des-md5. • Under Mode (Initiator), select Main (ID Protection).

To define the Netscreen-204 AutoKey IKE parameters

1 Go to **VPNs > AutoKey IKE** and select New.

2 Enter the following information, and select OK:

VPN Name	`Fortinet`
Security Level	Custom
Remote Gateway	Select Predefined, and then from the list, select FortiGate800.
Advanced	Select these Advanced options: • Under Security Level, set User Defined to Custom, and then from the first and second lists, select g2-esp-3des-md5 and g2-esp-3des-sha. • Under Bind to, select Tunnel Zone, and then from the list, select Untrust-Tunnel.

To complete the VPN configuration

Refer to your Netscreen ScreenOS 4.0.0 documentation for more information about how to configure a policy based LAN-to-LAN AutoKey IKE VPN. You must perform the following steps to complete the VPN configuration:

1 Assign IP addresses to the physical interfaces bound to the security zones.

2 Make address book entries for the local- and remote-end entities. In this case, the “end entities” are the private networks behind the FortiGate unit and the Netscreen-204 appliance.

3 Specify a default route to the external router to ensure that packets destined for Network_1 are delivered to Network_1.

4 Configure the policies needed for VPN traffic to pass bidirectionally through the tunnel.

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*.