Outbound NAT for IPSec VIP

Technical Note

Outbound NAT for IPSec VIP Technical Note	
Document Version:	Version 1
Publication Date:	5 August 2005
Description:	This technical note explains how to use the outbound NAT and IPSec virtual IP (VIP) features to circumvent ambiguous routing caused by combining two networks that use the same private address space.
Product:	FortiGate v2.80 MR10
Document Number:	01-28010-0079-20050805

Fortinet Inc.

Outbound NAT for IPSec VIP Technical Note
FortiGate v2.80 MR10
5 August 2005
01-28010-0079-20050805

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

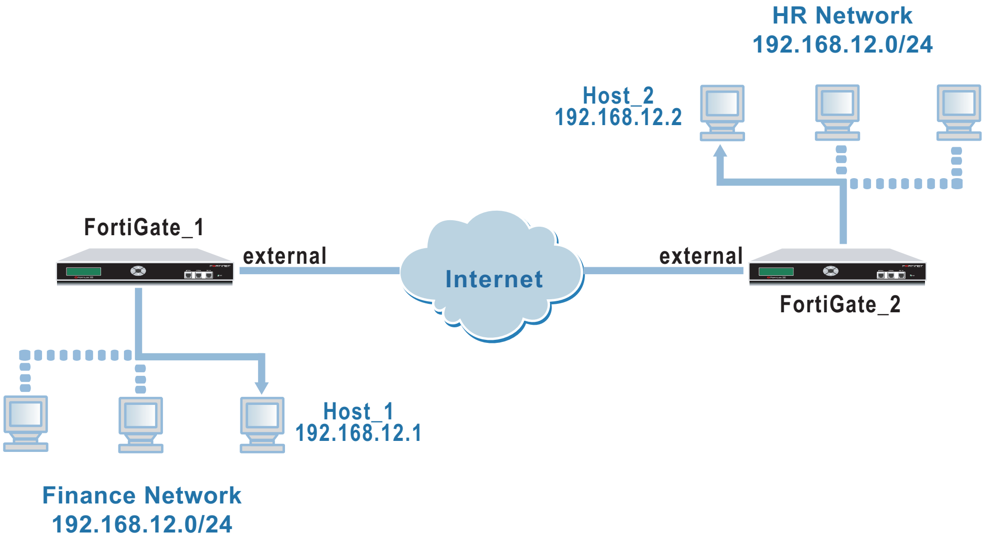
Outbound NAT for IPSec VIP

Ambiguous routing can happen accidentally when a VPN is set up between two physically separate private networks. This technical note explains how to use the outbound NAT and IPSec virtual IP (VIP) features to circumvent ambiguous routing caused by combining two networks that use the same private address space. This technical note contains the following sections:

How ambiguous routing happens

Ambiguous routing can happen when two physically separate networks that use the same private address space are connected through a VPN: a single private network would be created, but a packet destined for the remote network might not be forwarded to a computer on the other side of the VPN tunnel. An example of this type of network is shown in Figure 1 below.

Figure 1: The same private address space on physically separate networks



Working around ambiguous IP addresses

In cases where packets might not be forwarded to the remote network due to ambiguous IP addresses, you can use the IPSec VIP feature in conjunction with the outbound NAT feature to coordinate private IP addresses through a VPN:

- The IPsec VIP feature lets you specify which devices (for example, servers) are on the other side of the tunnel.
- Configuring outbound NAT through an encryption policy translates local IP addresses into an IP address that is valid on the other side of the tunnel.

For example, you can use the IPSec VIP and outbound NAT features to make a server on one network available to all of the devices on the other network. The server appears to be local to both networks.

To allow all devices on the local network to communicate with a remote server on the other side of the tunnel and enable the remote server to return traffic through the VPN tunnel, you add an IPSec VIP address for the remote server to the local FortiGate configuration and enable outbound NAT on the local FortiGate unit.

The configuration described in this technical note permits any device on the Finance network to communicate with Host_2 on the HR network (see Figure 1 on page 5). Whenever a connection is initiated from behind FortiGate_1, a VPN tunnel between FortiGate_1 and FortiGate_2 is activated.

About the IPSec VIP feature

A FortiGate unit can act as a proxy by answering ARP requests locally and forwarding the associated traffic to the intended destination host over an IPSec VPN tunnel. The IP addresses of both the source host and the destination host must be unique.

Use the `ipsec vip` CLI command to specify the IP addresses that need to be accessed at the remote end of the VPN tunnel. Adding an IPSec VIP entry to the VIP table enables a FortiGate unit to respond to ARP requests destined for remote servers and route traffic to the intended destinations automatically.

Each IPSec VIP entry is identified by an integer. Each entry identifies the local interface to the destination network and the IP address of the destination host on the destination network. Specify a VIP address for every host that needs to be accessed on the other side of the tunnel—you can define a maximum of 32 IPSec VIP addresses on the same interface.

About the outbound NAT feature

To enable the outbound NAT feature for an IPSec VPN, the Outbound NAT option must be selected in the firewall encryption policy. When the Outbound NAT option is selected, the FortiGate unit performs network address translation and assigns its own external IP address to outbound encrypted packets.

When outbound NAT is enabled, the FortiGate unit intercepts outbound cleartext packets, encrypts them, and then forwards them after performing network address translation. The source addresses of all outbound encrypted packets are translated into the IP address of the FortiGate external interface before the packets are routed to the remote network.

Defining the IPSec VIP address at FortiGate_1

Use the CLI to add IPSec VIP addresses to the VIP table on FortiGate_1. The web-based manager cannot be used to add the required entries.

The following example adds an IPSec VIP entry for a remote server that can be accessed by FortiGate_1 through its `external` interface.

```
config vpn ipsec vip
   edit 1
       set ip 192.168.12.2
       set out-interface external

end
```

Where:

- `set ip <address_ipv4>` provides the IP address of the destination host on the destination network (the default is `0.0.0.0`).
- `set out-interface <interface-name_str>` specifies the name of the local FortiGate interface to the destination network (the default is `null`).

Defining the firewall encryption policy at FortiGate_1

Firewall encryption policies control VPN traffic. A policy is needed to allow encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy. Before you define the policy, you must first specify the source and destination addresses.

Note: It is assumed that the required phase 1 authentication and phase 2 tunnel creation parameters have already been configured and tested at both VPN peers.

To define the source address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `Finance_Network`).
IP Range/Subnet	Enter the IP addresses and subnet mask (for example, `192.168.12.0/24`) from which VPN traffic may originate locally.

To define the destination address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `Host_2`).
IP Range/Subnet	Enter the individual IP address and subnet mask (for example, `192.168.12.2/32`) of Host_2. FortiGate_1 will compare this value to incoming source addresses to determine whether a connection is being initiated from Host_2 behind FortiGate_2.

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 network. Destination Select the interface to the external (remote) network.

Address Name	Source
	`Finance_Network`
	Destination
	`Host_2`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	Select the name of the phase 2 configuration that you created for the VPN tunnel. Select Allow inbound to allow traffic originating from Host_2 into the Finance network. Select Allow outbound to forward traffic originating from the Finance network to Host_2. Select Outbound NAT to translate the source addresses of outbound encrypted packets into the IP address of the FortiGate_1 external interface.
Advanced	As required.

3 To ensure that the encryption policy matches VPN connections, on the Policy tab, place the policy in the policy list above any other policies having similar source and destination addresses.

Defining the firewall encryption policy at FortiGate_2

Defining the firewall encryption policy at FortiGate_2 involves specifying the source and destination addresses and configuring the policy.

To define the source address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `Host_2`).
IP Range/Subnet	Enter the IP address and subnet mask (for example, `192.168.12.2/32`) of Host_2.

To define the destination address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `FortiGate_1`).
IP Range/Subnet	Enter the IP address of the FortiGate_1 external interface. FortiGate_2 will compare this value to incoming source addresses to determine whether a connection is being initiated from FortiGate_1.

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 network. Destination Select the interface to the external (remote) network.

Address Name	Source
	`Host_2`
	Destination
	`FortiGate_1`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	Select the name of the phase 2 configuration that you created for the VPN tunnel. Select Allow inbound to allow traffic originating from behind FortiGate_1 to reach Host_2. Select Allow outbound to forward traffic originating from Host_2 to FortiGate_1.
Advanced	As required.

3 On the Policy tab, place the policy in the policy list above any other policies having similar source and destination addresses.