# FortiGate IPSec VPN Subnet-address Translation

## Technical Note

| *FortiGate IPSec VPN Subnet-address Translation Technical Note* | |
|---|---|
| **Document Version:** | Version 1 |
| **Publication Date:** | 6 January 2005 |
| **Description:** | This technical note provides a detailed configuration example that enables bidirectional subnet-address translation inside an IPSec VPN tunnel. The `natip` attribute, when used with the outbound NAT feature, enables one-to-one subnet-address translation inside the tunnel. |
| **Product:** | FortiGate v2.80 MR7 |
| **Document Number:** | 01-280007-0148-20050106 |

**Fortinet Inc.**

*FortiGate IPSec VPN Subnet-address Translation Technical Note*
FortiGate v2.80 MR7
6 January 2005
01-280007-0148-20050106

# Table of Contents

FortiGate IPSec VPN Subnet-address Translation

This technical note provides a detailed configuration example that enables bidirectional subnet-address translation inside an IPSec VPN tunnel. The `natip` attribute, when used with the outbound NAT feature, enables one-to-one subnet-address translation inside the tunnel. This technical note contains the following sections:



## Enabling one-to-one subnet-address translation

When Outbound NAT is selected in a firewall encryption policy, you can configure a substitute address for Network Address Translation (NAT) through the CLI using the `set natip` attribute of the `config firewall policy` command. The setting enables one-to-one, subnet-address translation inside an IPSec VPN tunnel.

If you do not use the `set natip` attribute to translate IP addresses, the source addresses of outbound encrypted packets are translated to the IP address of the FortiGate external interface.

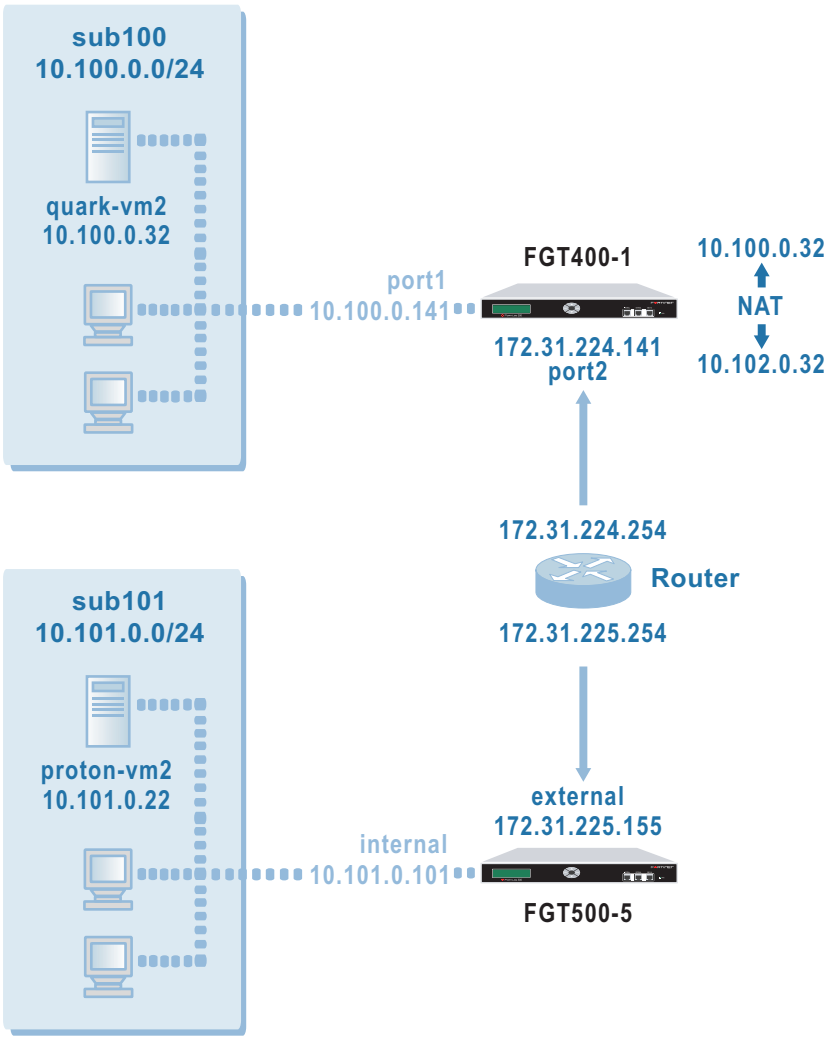
When you specify a `natip` value, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate the source addresses of encrypted packets into corresponding IP addresses on the subnetwork that you specify. For example, if the source address in the encryption policy is 192.168.1.0/24 and the `natip` value is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7.

You can specify a 32-bit subnet mask in the `natip` value to translate the source addresses of encrypted packets to a single IP address. For example, if the source address in the encryption policy is 192.168.1.0/24 and the `natip` value is 172.16.2.1/32, a source address of 192.168.1.7 will be translated to 172.16.2.1.

## Network topology

Figure 1 shows an example network configuration. In the examples throughout this technical note, the network devices are assigned IP addresses as shown in Figure 1.

**Figure 1: IPSec VPN configuration example**




In Figure 1, the Outbound NAT option is selected on FTG400-1. FTG400-1 intercepts outbound cleartext packets, encrypts them, performs NAT, and then forwards the packets. With Outbound NAT selected, the source addresses of outbound encrypted packets are translated to the IP address of the FTG400-1 port2 interface (172.31.224.141).

When `natip` is specified in conjunction with outbound NAT on the FTG400-1, the source addresses of outbound encrypted packets are translated to the specified `natip` address instead. For example, when `10.102.0.0/24` is specified as the `natip` value on FTG400-1, the source address 10.100.0.32 (which belongs to quark-vm2) is translated to 10.102.0.32. As a result, whenever quark-vm2 sends a packet beyond FTG400-1, the recipient of the packet uses the address modified by the `natip` value to reply to quark-vm2.

**Note:** Figure 1 does not show a subnet at address 10.102.0.0/24, which is the `natip` address. However, a virtual subnet called sub102 (at address 10.102.0.0/24) can be defined as the IP source address of FGT400-1 for phase 2 negotiations. Afterward, FTG500-5 will be able to reply to quark-vm2 using the `natip` address.

This technical note provides a detailed example of how to translate one subnet address into another subnet address in both directions—both the addresses of incoming and outgoing packets are translated—based on the network scenario shown in Figure 1. In the configuration example:

- Both VPN peers operate in NAT/Route mode and have static IP addresses.
- Encrypted packets from FTG400-1 are addressed to the external interface of FTG500-5. Encrypted packets from FTG500-5 are addressed to the port2 interface of FTG400-1.
- Outbound NAT is selected and a `natip` value of 10.102.0.0/24 is specified on FTG400-1.
- quark-vm2 can reach proton-vm2 using the destination IP address 10.101.0.22.
- proton-vm2 replies to quark-vm2 using a destination IP address of 10.102.0.32.

# Configuring FTG400-1

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 FTG400-1:

- Define the phase 1 parameters that FTG400-1 needs to authenticate FTG500-5 and establish a secure connection. See “Define the phase 1 parameters” on page 8.
- Define a virtual subnet address that corresponds to the `natip` value. The virtual subnet address is needed to define an IKE phase 2 selector for negotiating an outgoing IPSec security association prior to creating the tunnel. See “Define a virtual subnet address for IKE phase 2 negotiations” on page 8.
- Define the phase 2 parameters that FTG400-1 needs to create a VPN tunnel with FTG500-5. See “Define the phase 2 parameters” on page 9.
- Define the IP source and destination addresses needed for the firewall encryption policy. See “Specify the IP source and destination addresses” on page 9.
- Create a firewall encryption policy to control the permitted services and permitted direction of traffic between the IP source and destination addresses. See “Define the firewall encryption policy” on page 10.

## Define the phase 1 parameters

The phase 1 configuration defines the parameters that FTG400-1 will use to authenticate FTG500-5 and establish a secure connection. For the purposes of this example, a preshared key will be used to authenticate FTG500-5. The same preshared key must be specified at both FortiGate units.

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, `FGT500-5`). |
| **Remote Gateway** | Static IP Address |
| **IP Address** | `172.31.225.155` |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. |
| **Peer Options** | Accept any peer ID |

## Define a virtual subnet address for IKE phase 2 negotiations

After a secure channel has been established (in phase 1), quick mode establishes IPSec security associations at the beginning of phase 2. In order for FTG500-5 to reply to quark-vm2 using the `natip` address, you must define a virtual subnet address that quick mode can use to replace the port 2 IP address of FTG400-1 during IKE phase 2 negotiations. The quick mode source address must correspond to the subnet defined by the `natip` value.

### To define a virtual subnet address for IKE phase 2 negotiations

1. Go to **Firewall > Address**.
2. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `sub102`). |
| **IP Range/Subnet** | Enter the `natip` value that FTG400-1 will be using to replace the source address of outbound encrypted packets (for example, `10.102.0.0/24`). |

## 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.

### 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, `FGT500-5-tun`). |
| **Remote Gateway** | Select the gateway that you defined previously (for example, `FGT500-5`). |
| **Advanced** | Under Quick Mode Identities, select Specify a selector and then select the following values:<br>• From the Source address list, select `sub102`.<br>• From the Dest address list, select `sub101`. |

## Specify the IP source and destination addresses

In the example configuration:

- The source IP address for the firewall encryption policy corresponds to the private network behind FTG400-1.
- The destination IP address for the firewall encryption policy refers to the private network behind FTG500-5.

### To define the IP source address of the network behind FTG400-1

1 Go to **Firewall > Address**.

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

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `sub100`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind FTG400-1 (for example, `10.100.0.0/24`). |

### To specify the destination address of IP packets delivered to FTG500-5

1 Go to **Firewall > Address**.

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

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `sub101`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind FTG500-5 (for example, `10.101.0.0/24`). |

## 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.

**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<br>`port1`<br>Destination<br>`port2` |
| **Address Name** | Source<br>`sub100`<br>Destination<br>`sub101` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `FGT500-5-tun`<br>Select Outbound NAT. |

3. Place the policy in the policy list above any other policies having similar source and destination addresses.
4. Enter the following CLI command to set the `natip` attribute on FTG400-1:

```
config firewall policy
  edit 1
     set natip 10.102.0.0 255.255.255.0
     end
```

# Configuring FTG500-5

FTG500-5 has a basic IPSec VPN configuration. To configure FTG500-5, you must:

- Define the phase 1 parameters that FTG500-5 needs to authenticate FTG400-1 and establish a secure connection.
- Define the phase 2 parameters that FTG500-5 needs to create a VPN tunnel with FTG400-1.
- Create a firewall encryption policy and define the scope of permitted services between the IP source and destination addresses. In this case, the IP destination address must match the subnet defined by the `natip` value.

### 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, `FTG400-1`). |
| **Remote Gateway** | Static IP Address |
| **IP Address** | `172.31.224.141` |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. The value must be identical to the preshared key that you specified previously in the FTG400-1 configuration. |
| **Peer Options** | Accept any peer ID |

### 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, `FGT400-1-tun`). |
| **Remote Gateway** | Select the gateway that you defined previously (for example, `FTG400-1`). |

### To define the IP source address of the network behind FTG500-5

1 Go to **Firewall > Address**.

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

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `sub101`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind FTG500-5 (for example, `10.101.0.0/24`). |

### To specify the destination address of IP packets delivered to FTG400-1

1 Go to **Firewall > Address**.

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

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `sub100`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind FTG400-1 (for example, `10.102.0.0/24`). |

### 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<br>`internal`<br>Destination<br>`external` |
| **Address Name** | Source<br>`sub101`<br>Destination<br>`sub100` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `FGT400-1-tun` |

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

**Note:** If the tunnel goes down, you can re-establish the tunnel by configuring FTG500-5 to ping quark-vm2 at IP address 10.102.0.32.

## Sample tunnel traces

In the following tunnel-trace samples, FTG400-1 initiates the tunnel.

### FTG400-1 traces

```
Fortigate-400 # diag vpn tun up FGT500-5-tun

Fortigate-400 # Get sa_connect message...172.31.224.141->172.31.225.155:500, natt_mode=0
Using old connection...natt_mode=0
Tunnel 172.31.224.141 ---> 172.31.225.155:500,natt_en=1 is starting negotiation
Initiator:quick mode set pfs=1536...
Try to negotiate with 1800 life seconds.
Initiate an SA with selectors:
 10.102.0.0/255.255.255.0->10.101.0.0/255.255.255.0
Send IKE Packet(quick_outI1):172.31.224.141:500(if5) -> 172.31.225.155:500, len=396
Initiator: sent 172.31.225.155 quick mode message #1 (OK)
set retransmit: st=8, timeout=6.

Comes 172.31.225.155:500->172.31.224.141:500,ifindex=5, port2, vf_id=0....
Exchange Mode = 32, Message id = 0x5A1CB3D3, Len = 356
Received Payloads= HASH SA NONCE KE ID ID
Initiator:quick mode get 1st response
```

```
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Using tunnel mode.
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Replay protection enable.
Set sa life soft seconds=1775.
Set sa life hard seconds=1800.
dport = 500.Initializing sa OK.
Initiator: sent 172.31.225.155 quick mode message #2 (DONE)
expire: st=8, timeout=120.
Send IKE Packet(STF_REPLY):172.31.224.141:500(if5) -> 172.31.225.155:500, len=52

Fortigate-400 # diag vpn tun list
tunnel[4]:FGT500-5-tun, gateway:172.31.225.155:500, hub=, option=134
   eroute[2]:{[10.100.0.*]}->{[10.101.0.*]}
   channel[2]:172.31.224.141,natt=0,state=2,keepalive=0,oif=5
     sa[4]:mtu=1434, cur_bytes=0, timeout=1742
     itdb[1]:mtu=1434, cur_bytes=0, cur_packets=0, spi=db6f062c, replay=64
          3DES=48b19c10621cc7ea42b100dbf496c28f326ee48157fdda1b
          iv=0000000000000000
          SHA1_HMAC=deef1788bb00742a286e676e1acbf87c9fc70366
     otdb[1]:mtu=1434, cur_bytes=0, cur_packets=0, spi=832b2b1f, replay=64
          3DES=6889fc869678d9612124f2de3b3318ca1cb961037e76a637
          iv=5268bf9a744f53d2
          SHA1_HMAC=283905e5a0f44c8a6c4d67caf1b2c106dc4a0cb1
```

## FTG500-5 traces

```
Fortigate-500 # Comes 172.31.224.141:500->172.31.225.155:500,ifindex=3, external, vf_id=0....
Exchange Mode = 32, Message id = 0x5A1CB3D3, Len = 396
Received Payloads= HASH SA NONCE KE ID ID
Responder:quick mode get 1st message...
his proposal is: peer:10.102.0.0/255.255.255.0, me:10.101.0.0/255.255.255.0, ports=0/0,
                      protocol=0/0
my policy is: src:10.101.0.0/255.255.255.0, dst:10.102.0.0/255.255.255.0
Got it
Found FGT400-1:172.31.224.141.
Matched an IPsec tunnel(FGT400-1-tun), kernel_comm.c,689
Autokey FGT400-1-tun.
Negotiate Result
```

```
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
negotiate:set pfs=1536.
Using tunnel mode.
Responder:quick mode set pfs=1536.
quick mode:idci type=4, len=8, chunk=0a660000ffffff00
quick mode:idcr type=4, len=8, chunk=0a650000ffffff00
Responder: sent 172.31.224.141 quick mode message #1 (OK)
Send IKE Packet(STF_REPLY):172.31.225.155:500(if3) -> 172.31.224.141:500,
len=356
set retransmit: st=9, timeout=6.

Comes 172.31.224.141:500->172.31.225.155:500,ifindex=3, external, vf_id=0....
Exchange Mode = 32, Message id = 0x5A1CB3D3, Len = 52
Received Payloads= HASH
Replay protection enable.
Set sa life soft seconds=1750.
Set sa life hard seconds=1800.
dport = 500.Initializing sa OK.
Responder:quick mode done !

Responder: parsed 172.31.224.141 quick mode message #2 (DONE)
expire: st=9, timeout=120.

Fortigate-500 # diag vpn tun list
tunnel[4]:FGT400-1-tun, gateway:172.31.224.141:500, hub=, option=6
   eroute[2]:{[10.101.0.*]}->{[10.102.0.*]}
   channel[2]:172.31.225.155,natt=0,state=2,keepalive=0,oif=3
     sa[4]:mtu=1434, cur_bytes=0, timeout=1716
     itdb[1]:mtu=1434, cur_bytes=0, cur_packets=0, spi=832b2b1f, replay=64
          3DES=6889fc869678d9612124f2de3b3318ca1cb961037e76a637
          iv=0000000000000000
          SHA1_HMAC=283905e5a0f44c8a6c4d67caf1b2c106dc4a0cb1
     otdb[1]:mtu=1434, cur_bytes=0, cur_packets=0, spi=db6f062c, replay=64
          3DES=48b19c10621cc7ea42b100dbf496c28f326ee48157fdda1b
          iv=4d32dbdc42448e8c
          SHA1_HMAC=deef1788bb00742a286e676e1acbf87c9fc70366
```