

**LanRover™ VPN Gateway,
LanRover VPN Gateway PLUS, and
Intel® NetStructure™ 3110, 3120,
3125, 3130 VPN Gateway
Network Layout Reference Guide**

Disclaimer

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel Network System, Inc.'s Terms and Conditions of Sale for such products, Intel Network Systems, Inc. assumes no liability whatsoever, and Intel Network Systems, Inc. disclaims any express or implied warranty, relating to sale and/or use of Intel® products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel Network Systems, Inc. products are not intended for use in medical, life saving, or life sustaining applications.

Intel Network Systems, Inc. may make changes to specifications and product descriptions at any time, without notice.

This *LanRover™ VPN Gateway*, *LanRover VPN Gateway PLUS*, and *Intel® NetStructure™ 3110, 3120, 3125, 3130 VPN Gateway Network Layout Reference Guide*, as well as the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Network Systems, Inc. Intel Network Systems, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Network Systems, Inc.

Copyright © Intel Network Systems, Inc. 2000. *Other brands and names are the property of their respective owners.

Contents

Network Layout Reference Guide	1
Network Layout Reference Guide	1
Client Scenarios	1
LAN-to-LAN Scenarios	1
Client Scenarios	2
One-Armed Router Configuration With No Firewall	2
Inline Router Configuration	3
In Parallel With Firewall (Extranet or Intranet)	5
Bridge Configuration	7
Edge Router Configuration	9
Behind a Firewall With or Without NAT (One-Armed)	11
Behind a Firewall With or Without NAT (Inline)	13
The VPN Gateway as a Firewall	15
LAN-to-LAN Scenarios	18
In Parallel With a Firewall (Without NAT)	18
In Parallel With a Firewall (With NAT)	19
Behind a Firewall (One-Armed) With or Without NAT	21
Behind a Firewall That May or May Not Use NAT (Inline)	24
The VPN Gateway as a Firewall (With or Without NAT)	27

Network Layout Reference Guide

The purpose of this Network Layout Reference Guide is to help you install the LanRover™ VPN Gateway, the LanRover VPN Gateway PLUS, and the Intel® NetStructure™ 3110, 3120, 3125, and 3130 VPN Gateway devices in your network. The term VPN Gateway is used in this document to refer to all of these devices.

Here are some real-world examples of how the VPN Gateway can be incorporated into your network infrastructure. Skim through the following scenarios and find the ones most similar to your network configuration. Then, note the corresponding configuration options to help you quickly install the VPN Gateway into your network.

Scenarios are divided into client and LAN-to-LAN.

Client Scenarios

- One-armed router configuration (VPN server) with no firewall
- Inline router configuration
- In parallel with firewall (for extranet or intranet)
- Bridge configuration
- Edge router configuration
- Behind a firewall (one-armed) that may or may not use network address translation (NAT)
- Behind a firewall (inline) that may or may not use NAT
- VPN Gateway as a firewall

LAN-to-LAN Scenarios

- In parallel with a firewall and no NAT
- In parallel with a firewall with NAT
- Behind a firewall (one-armed) that may or may not use NAT
- Behind a firewall (inline) that may or may not use NAT
- VPN Gateway as a firewall (may or may not use NAT)

Client Scenarios

If you are using the VPN Gateway with the Intel NetStructure VPN Client, skim the following scenarios and find the ones most similar to your network configuration. Then, use the corresponding table of configuration parameters as a guideline when configuring your VPN Gateway and Intel NetStructure VPN Client.

If you are using the VPN Gateway in LAN-to-LAN configurations, skip to the next section “LAN-to-LAN Scenarios.”

One-Armed Router Configuration With No Firewall

This scenario shows the following:

- One-armed configuration uses only one of the VPN Gateway’s two interfaces.
- Firewall is not enabled.
- The VPN Gateway (VPNG) acts as a VPN server.

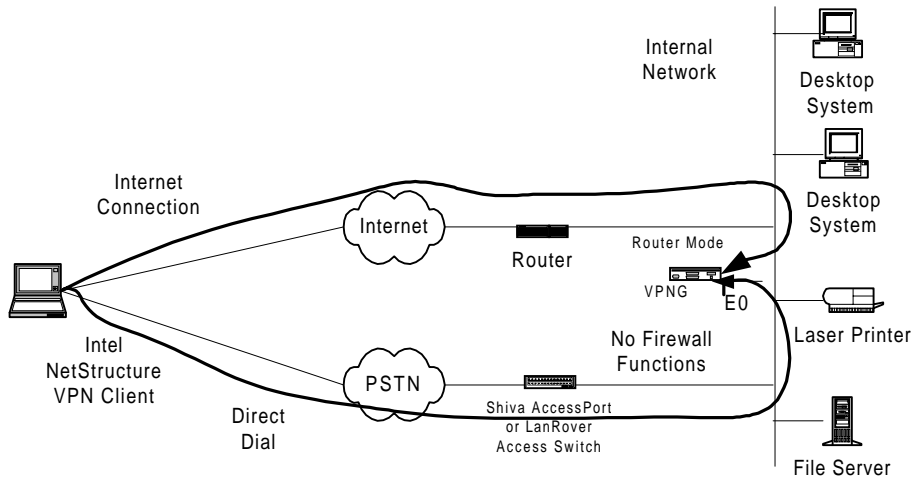


Figure: One-Armed Configuration With No Firewall

Configuring a One-Armed Router Configuration

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a one-armed router configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: One-Armed Router Configuration Parameters

NAT by Router/AccessPort	No NAT
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: (not used for one-armed) IP: NA Mode: NA	Interface E1: (not used for one-armed) IP: NA Mode: NA
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.2 255.255.255.255	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 john doe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

Inline Router Configuration

In this scenario, Intel NetStructure VPN Client traffic is handled either through a router (inline) or by directly dialing into the public-switched telephone network (PSTN).

- For inline router configurations:
 - The router accepts all incoming client traffic then transfers the traffic to the VPN Gateway.
 - The VPN Gateway then transfers the traffic on to the local network to which it is attached. The VPN Gateway may or may not perform firewall functions on the traffic.
- For direct dial into the PSTN:
 - Traffic may go through a Shiva® AccessPort or LanRover Access Switch, which may or may not perform NAT.
 - The traffic then goes through the VPN Gateway, which may or may not perform firewall functions on the traffic.

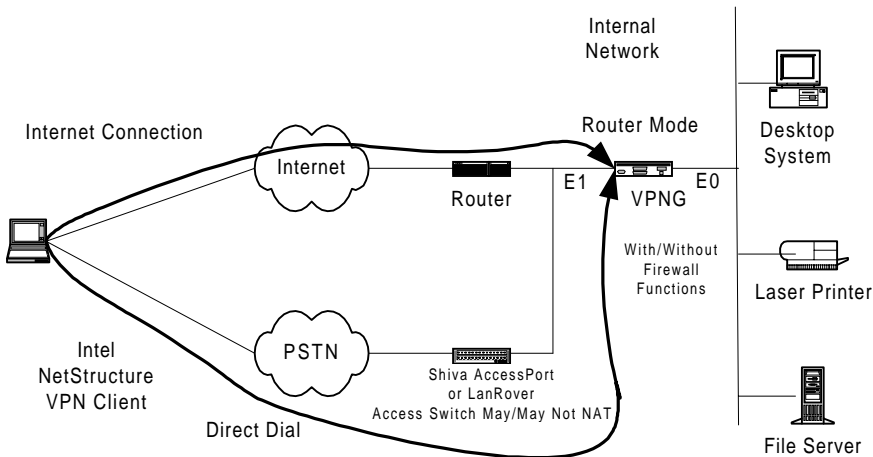


Figure: Inline Router Configuration

Configuring an Inline Router Configuration

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up an inline router configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Inline Router Configuration Parameters

NAT by Router/Shiva AccessPort	No NAT
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.3 255.255.255.255	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 john doe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

In Parallel With Firewall (Extranet or Intranet)

In this scenario, Intel NetStructure VPN Client traffic is handled either through a router (inline) or by directly dialing in to the PSTN. In addition, there is a third-party firewall on the network handling firewall functionality.

- For inline router configurations:
 - The router accepts all incoming client traffic, then transfers the traffic to the VPN Gateway.
 - The VPN Gateway then transfers the traffic to the local network to which it is attached.
 - The VPN Gateway is in router mode and does not perform firewall functions.

- Traffic is then handed to the third-party firewall, which performs firewall functions before handing the traffic onto the local network.
- For direct dial into the PSTN:
 - Traffic may go through a Shiva AccessPort or LanRover Access Switch, which may or may not perform NAT.
 - The traffic then goes through the VPN Gateway (VPNG), which passes the traffic to the local network.
 - The third-party firewall then performs firewall functions on the traffic before passing it to the local network.

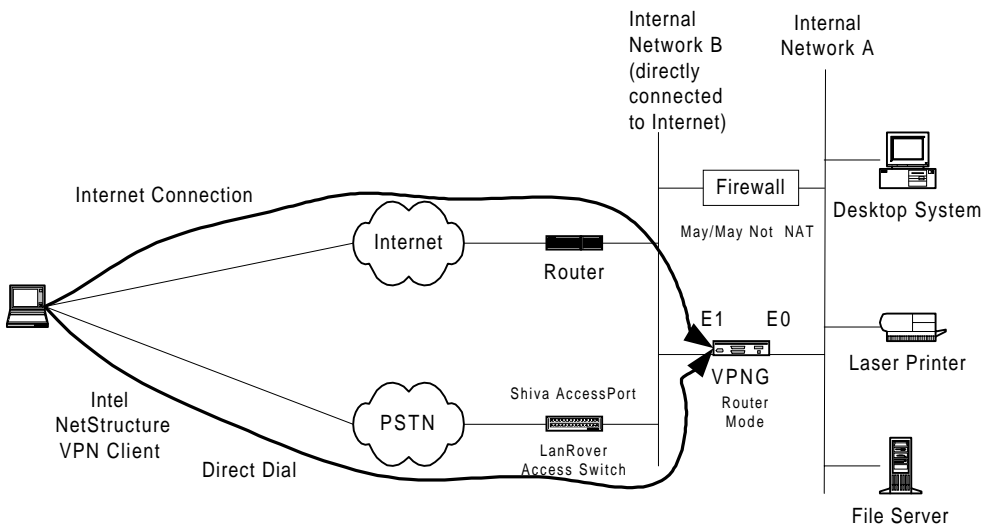


Figure: In Parallel With Firewall

Configuring an In Parallel With Firewall Configuration

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up an in parallel with firewall configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: In Parallel With Firewall Configuration Parameters

VPN Gateway (NAT by Router)	VPN Gateway (No NAT)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.3 255.255.255.255	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 johndoe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

Bridge Configuration

In this scenario, Intel NetStructure VPN Client traffic is handled either through a router/bridge or by directly dialing into the PSTN.

- For router/bridge configurations:
 - The router/bridge accepts all incoming client traffic then transfers the traffic to the VPN Gateway.
 - The VPN Gateway is set to bridge mode and transfers the traffic to the local network to which it is attached.
 - The VPN Gateway may or may not perform firewall functions on the traffic.
 - The bridge is installed on the internal side of the network with minimal changes to the network topology.
- For direct dial into the PSTN:
 - Traffic may go through a Shiva AccessPort or LanRover

Access Switch, which may or may not perform network address translation.

- The traffic then goes through the VPN Gateway, which is set to bridge mode. The VPN Gateway may or may not perform firewall functions on the traffic.

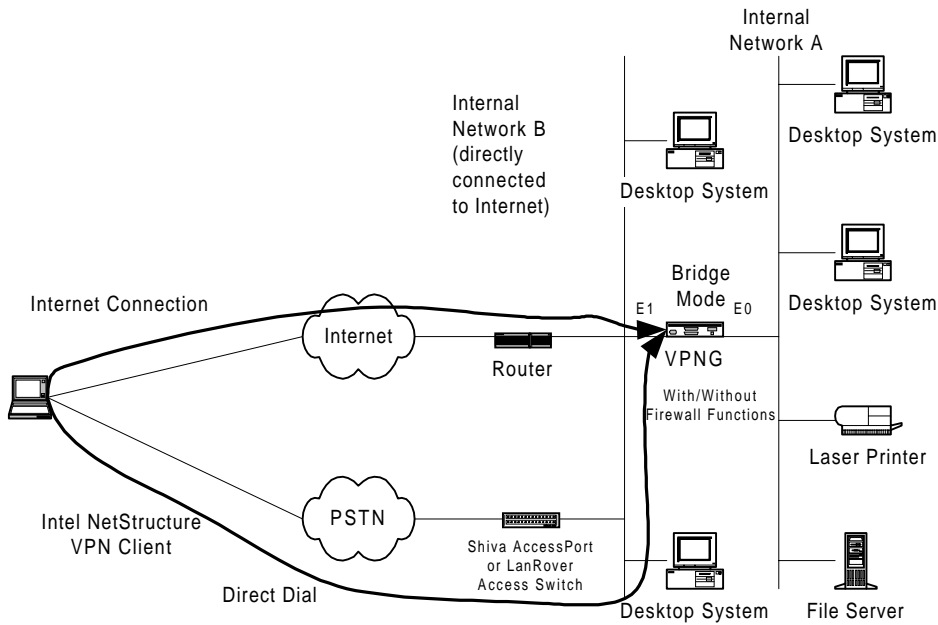


Figure: Bridge Configuration

Configuring a Bridge Configuration

When setting up a VPN Gateway, you must configure many global configuration. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a bridge configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Bridge Configuration Parameters

NAT by Router/Shiva AccessPort	InlineNo NAT
Interface E0: Mode: Red	Interface E0: Mode: Red
Interface E1: Mode: Red	Interface E1: Mode: Red
Bridge IP: 10.250.128.2	Bridge IP: 205.25.128.2 255.255.255.0
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

Edge Router Configuration

In this scenario, the VPN Gateway acts as an “edge” router; it is the only device between the Internet and the local network.

- The Intel NetStructure VPN Client makes a secure VPN connection through the Internet to the VPN Gateway.
- The VPN Gateway is configured to router mode.
- The VPN Gateway may or may not perform firewall functions on the traffic.
- The Intel NetStructure VPN Client has no means to perform direct dial to the local network; it must go through a VPN tunnel.

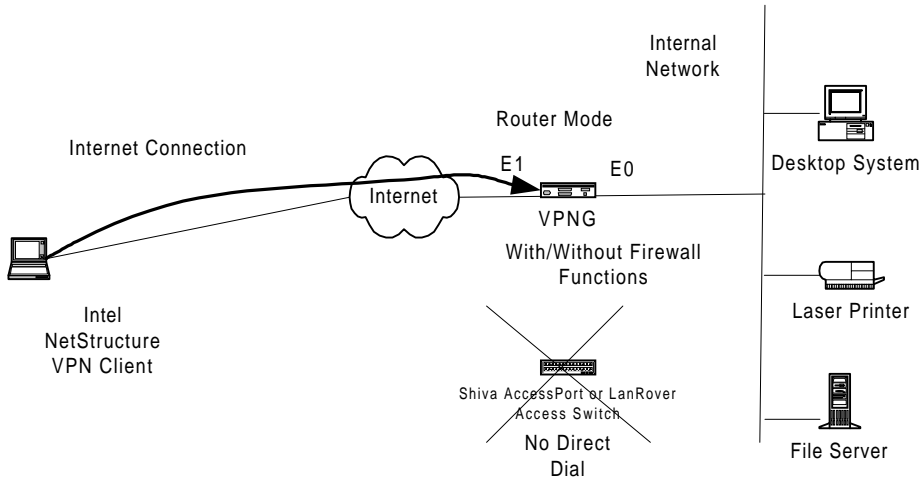


Figure: Edge Router Configuration

Configuring an Edge Router Configuration

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up an edge router configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Edge Router Configuration Parameters

VPN Gateway (NAT by Router)	VPN Gateway (No NAT)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Black	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red

VPN Gateway (NAT by Router)	VPN Gateway (No NAT)
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.3 255.255.255.255	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 johndoe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

Behind a Firewall With or Without NAT (One-Armed)

In this scenario, Intel NetStructure VPN Client traffic is handled either through a router (inline) or by directly dialing in to the PSTN. The traffic passes through a third-party firewall before passing through the VPN Gateway.

- For inline router configurations:
 - The router accepts all incoming client traffic, then transfers the traffic to the third-party firewall.
 - The third-party firewall performs firewall functionality on the traffic before passing it to the VPN Gateway.
 - The VPN Gateway takes the encrypted traffic and decrypts it before passing it to the local network.
- For direct dial into the PSTN:
 - Traffic may go through a Shiva AccessPort or LanRover Access Switch, which may or may not perform NAT.
 - The traffic then goes through a third-party firewall. The third-party firewall performs firewall functionality on the traffic before passing it to the VPN Gateway.
 - The VPN Gateway then decrypts the encrypted VPN traffic and passes it to the local network.

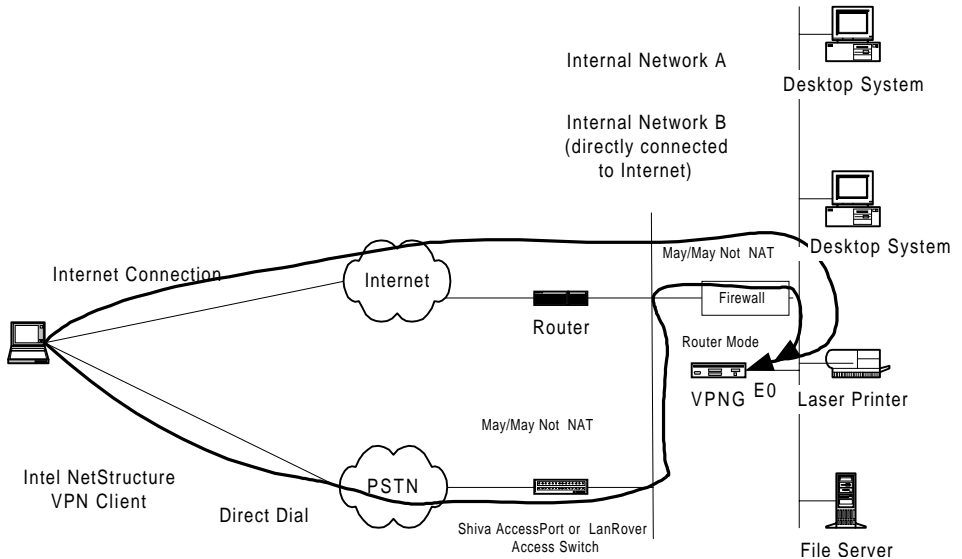


Figure: Behind a Firewall (One-Armed)

Configuring a Behind a Firewall (One-Armed) Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a behind a firewall (one-armed) configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Behind a Firewall (One-Armed) Configuration Parameters

VPN Gateway (NAT by Router)	VPN Gateway (No NAT)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: (Not used for one-armed) IP: NA Mode: NA	Interface E1: (Not used for one-armed) IP: NA Mode: NA
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.3 255.255.255.255	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 johndoe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

Behind a Firewall With or Without NAT (Inline)

In this scenario, Intel NetStructure VPN Client traffic is handled either through a router (inline) or by directly dialing in to the PSTN. The traffic passes through a third-party firewall that may or may not perform NAT before passing the traffic to the VPN Gateway.

- For inline router configurations:
 - The router accepts all incoming client traffic, then transfers the traffic to the third-party firewall.
 - The third-party firewall may or may not perform NAT before passing the traffic to the VPN Gateway.
 - The VPN Gateway then decrypts the encrypted VPN traffic and passes it to the local network.

- For direct dial into the PSTN:
 - Traffic may go through a Shiva AccessPort or LanRover Access Switch, which may or may not perform NAT.
 - The traffic then goes through the third-party firewall, which also may or may not perform NAT before being handed to the VPN Gateway.
 - The VPN Gateway then decrypts the encrypted VPN traffic and passes it to the local network.

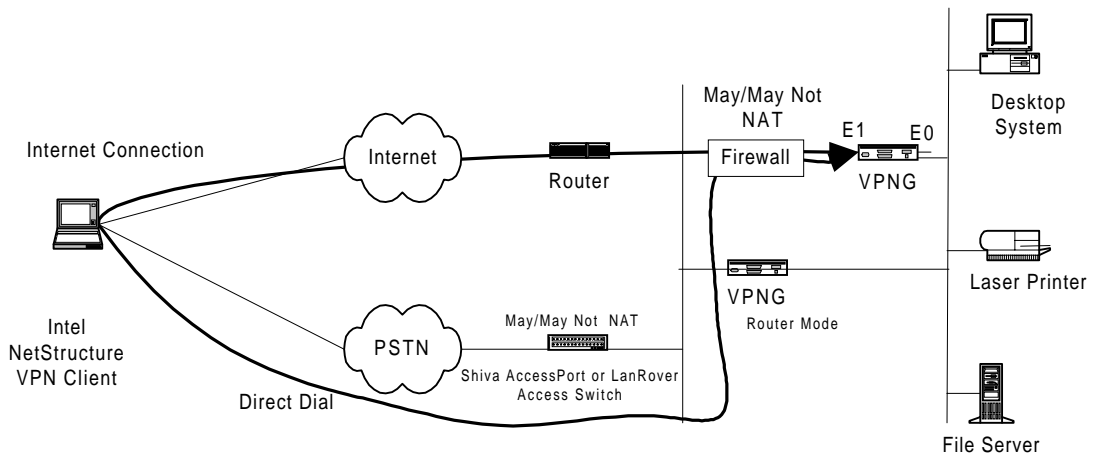


Figure: Behind a Firewall (Inline)

Configuring a Behind a Firewall (Inline) Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a behind a firewall (inline) configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Behind a Firewall (Inline) Configuration Parameters

VPN Gateway (NAT by Router)	VPN Gateway (No NAT)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red
Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.3 255.255.255.255	Configuration file entries/routing info: security profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 johndoe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

The VPN Gateway as a Firewall

In this scenario, Intel NetStructure VPN Client traffic is handled either through a router (inline) or by directly dialing in to the PSTN. The traffic passes through firewall functionality on the VPN Gateway. The VPN Gateway may or may not perform NAT before passing the traffic to the local network.

- For inline router configurations:
 - The router accepts all incoming client traffic, then transfers the traffic to the VPN Gateway.
 - The third-party firewall may or may not perform NAT before passing the traffic to the VPN Gateway.
 - The VPN Gateway then performs firewall functionality on the traffic and passes it to the local network.

- The VPN Gateway may or may not perform NAT.
- For direct dial into the PSTN:
 - Traffic may go through a Shiva AccessPort or LanRover Access Switch.
 - The traffic then goes through firewall functionality on the VPN Gateway.
 - The VPN Gateway may or may not perform NAT before being handed onto the local network.

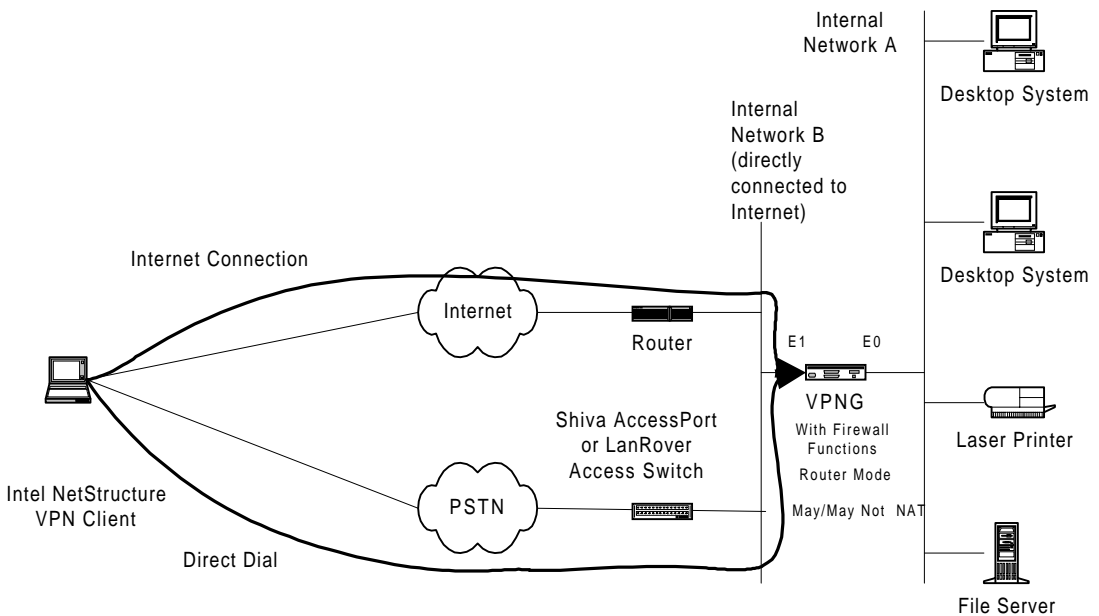


Figure: VPN Gateway as a Firewall

Configuring a VPN Gateway as a Firewall

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a VPN Gateway as a firewall configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: VPN Gateway as a Firewall Configuration Parameters

VPN Gateway (NAT by Router)	VPN Gateway (No NAT)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Black	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Black
Configuration file entries/routing info: security-profile remote user remote tunnel johndoe security-profile remote user client-ip 10.250.128.3 255.255.255.255	Configuration file entries/routing info: security-profile remote user remote tunnel johndoe security-profile remote user ip route 209.29.128.50 255.255.255.255 johndoe
Intel NetStructure VPN Client IP: 10.250.128.3	Intel NetStructure VPN Client IP: Uses ISP IP (no client IP)
Subnet: 10.250.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)
ISP IP: 209.29.128.50	ISP IP: 209.29.128.50

LAN-to-LAN Scenarios

In Parallel With a Firewall (Without NAT)

This scenario shows the following:

- A LAN-to-LAN connection between two VPN Gateway devices with no NAT.
- Each VPN Gateway is attached to a router. The routers connect through the Internet.
- Traffic travels from one local network, through the LAN-to-LAN connection, to the other local network.
- Traffic passes through the VPN Gateway, which is in router mode.
- The VPN Gateway passes the VPN traffic on to the local network.

Note: You must add a route to the third-party firewall for the network behind VPN Gateway B.

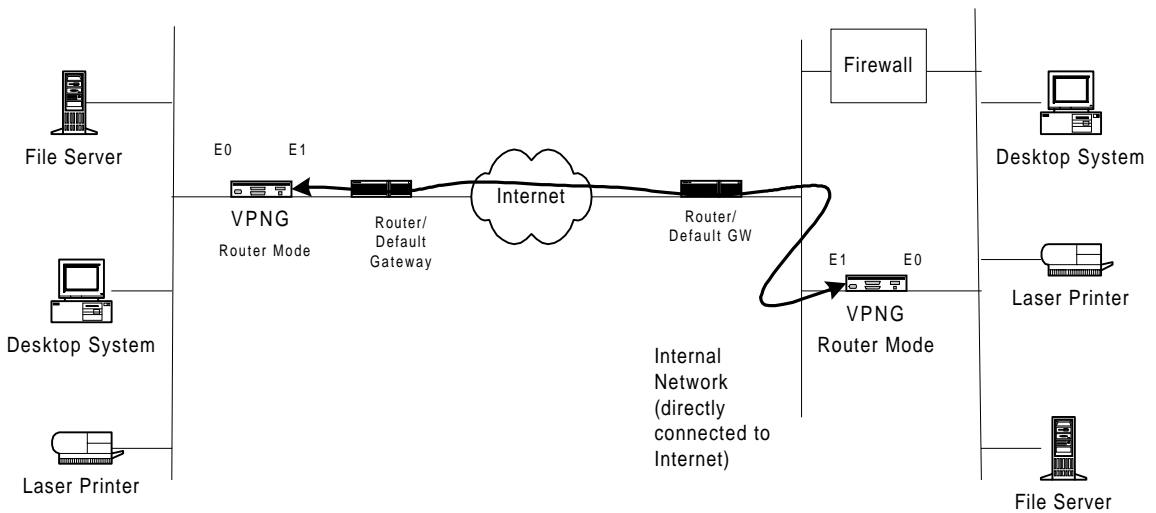


Figure: In Parallel With a Firewall (No NAT)

Configuring an In Parallel With a Firewall (No NAT) Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a parallel with a firewall (no NAT) configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: In Parallel With a Firewall (No NAT) Configuration Parameters

VPN Gateway A (No NAT)	VPN Gateway B (No NAT)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 10.250.130.2 255.255.255.0 Mode: Red
Interface E1: IP: 209.80.10.1 255.255.255.0 Default Gateway: 209.80.10.2 Mode: Red	Interface E1: IP: 209.80.20.1 255.255.255.0 Mode: Red
Config file entries/routing info: security-profile site-to-site tunnel SanFrancisco route 10.250.130.0 255.255.255.0 gateway 209.80.20.1	Config file entries/routing info: security-profile site-to-site tunnel Boston route 10.250.128.0 255.255.255.0 gateway 209.80.10.1

In Parallel With a Firewall (With NAT)

This scenario shows the following:

- A LAN-to-LAN connection between two VPN Gateway devices using NAT.
- Each VPN Gateway is attached to a router. The routers connect through the Internet and perform NAT.
- Traffic travels from one local network, through the LAN-to-LAN connection, to the other local network.
- Traffic passes through the VPN Gateway, which is in router mode.

- The LanRover VPN Gateway passes the VPN traffic to the third-party firewall (in parallel with the VPN Gateway).
- The third-party firewall performs firewall functionality on the traffic, then passes the traffic to the local network.

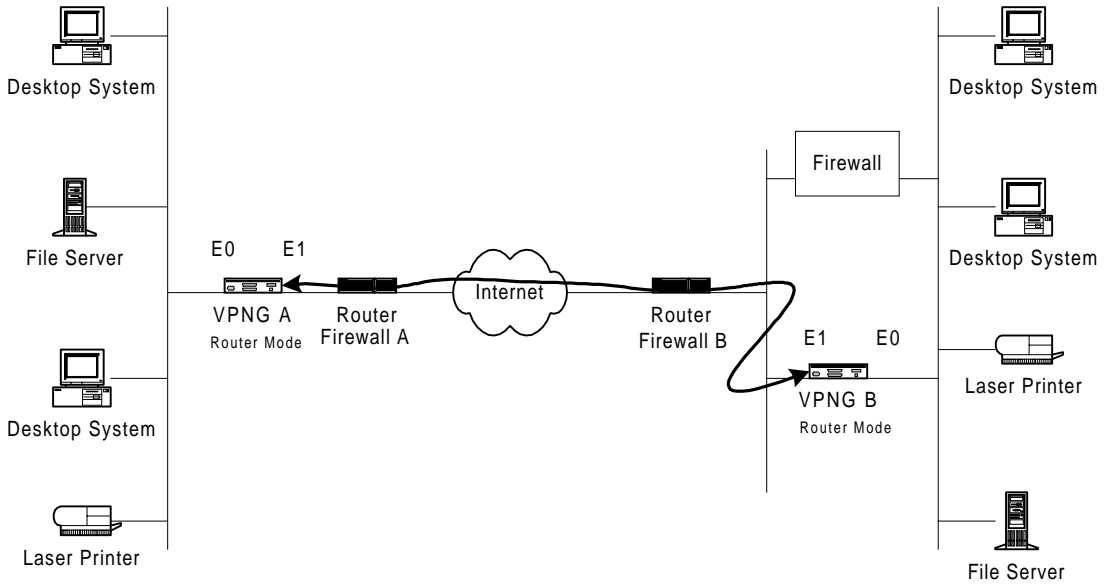


Figure: In Parallel With a Firewall (With NAT)

Configuring an In Parallel With a Firewall (With NAT) Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up an in parallel with a firewall (with NAT) configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: In Parallel With a Firewall (With NAT) Configuration Parameters

VPN Gateway A (NAT by Router)	VPN Gateway B (NAT by Router)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 10.250.130.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Default Gateway: 192.168.10.4 Mode: Red	Interface E1: IP: 192.168.12.2 255.255.255.0 Default Gateway: 192.168.12.4 Mode: Red
Configuration file entries/routing info: security-profile site-to-site tunnel Boston route 209.29.128.50 255.255.255.0	Configuration file entries/routing info: security-profile site-to-site tunnel SanFrancisco route 209.29.128.50 255.255.255.0

Behind a Firewall (One-Armed) With or Without NAT

This scenario shows the following:

- A LAN-to-LAN connection between two VPN Gateway devices.
- VPN Gateway A is attached to Router A. Router B is attached to the local network. The routers connect through the Internet.
- Traffic travels from one local network, through the LAN-to-LAN connection, to the other local network.
- Router B passes the traffic first to the third-party firewall, which resides in parallel to the VPN Gateway.
- The third-party firewall may or may not perform network address translation.
- The third-party firewall performs firewall functionality on the traffic, then passes the traffic to the VPN Gateway.
- The VPN Gateway decrypts the encrypted VPN traffic and passes it to the local network.

Note: You must add a route to the firewall for the network that is in front of VPN Gateway B (which routes to the VPN Gateway B interface for the subnet accessible through the tunnel). If you do not add

this route, local machines (with their default gateway pointing to the firewall) will not be able to route to the VPN Gateway A network.

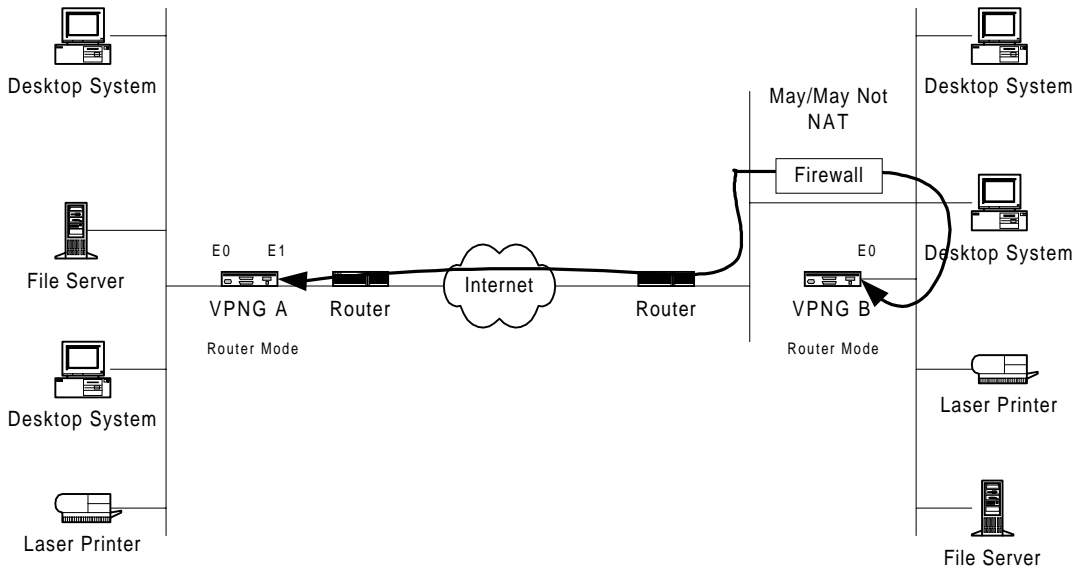


Figure: Behind a Firewall (One-Armed)

Configuring a Behind a Firewall (One-Armed) With NAT Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a behind a firewall (one-armed) with NAT configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Behind a Firewall (One-Armed) With NAT Configuration Parameters

VPN Gateway A (NAT by Router)	VPN Gateway B (NAT by Router)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 10.250.135.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red	Interface E1: (Not used for one-armed) IP: N/A Mode: N/A
Config file entries/routing info: security-profile site-to-site tunnel SanFrancisco security-profile site-to-site route 10.250.135.0 255.255.255.0	Config file entries/routing info: security-profile site-to-site tunnel Boston security-profile site-to-site route 209.29.128.50 255.255.255.255

Configuring a Behind a Firewall (One-Armed) Without NAT Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a behind a firewall (one-armed) without NAT configuration, use the configuration parameters in the following table. Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Behind a Firewall Without NAT

VPN Gateway A (No NAT)	VPN Gateway B (No NAT)
Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.135.2 255.255.255.0 Mode: Red
Interface E1: IP: 209.80.10.25 255.255.255.0 Default Gateway: 209.80.10.2 Mode: Red	Interface E1: (Not used for one-armed) IP: N/A Mode: N/A
Config file entries/routing info: security-profile site-to-site tunnel SanFrancisco security-profile site-to-site ip route 205.25.135.0 255.255.255.0 205.25.135.2	Config file entries/routing info: security-profile site-to-site tunnel Boston security-profile site-to-site route 205.25.128.0 255.255.255.0 209.80.10.25

Behind a Firewall That May or May Not Use NAT (Inline)

This scenario shows the following:

- A LAN-to-LAN connection between two VPN Gateways.
- VPN Gateway A is directly attached to Router A. Router B is directly attached to a third-party firewall. The routers connect through the Internet.
- Traffic travels from Router A to Router B. Router B passes traffic directly through the third-party firewall.
- The third-party firewall performs firewall functionality on the traffic and may or may not use NAT.
- The third-party firewall then passes the traffic to the VPN Gateway B, which is directly attached to it.
- The VPN Gateway B decrypts the VPN traffic before passing it to the local network.

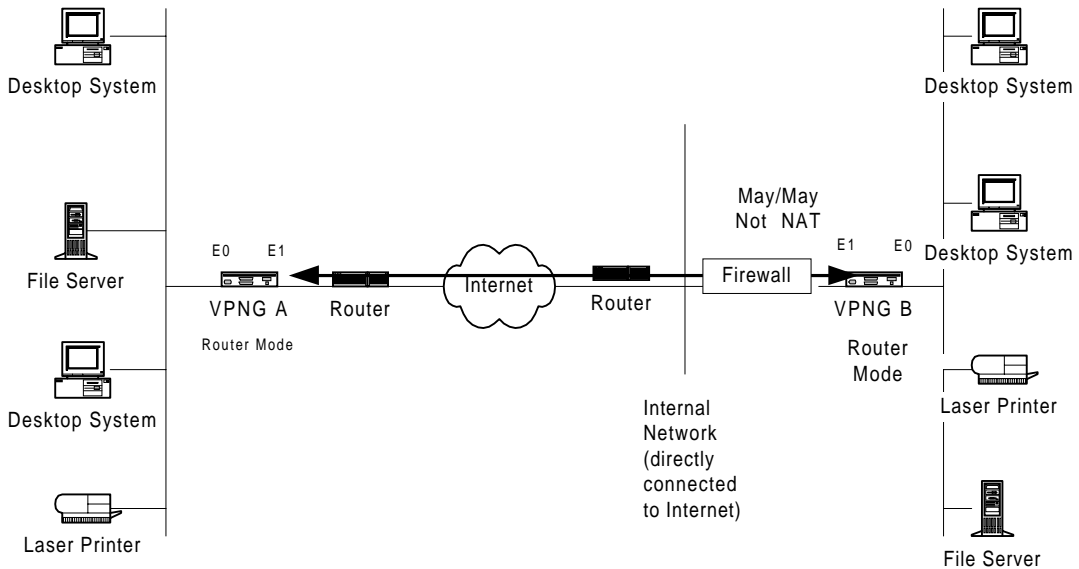


Figure: Behind a Firewall That May or May Not Use NAT (Inline)

Configuring a Behind a Firewall (Inline) Network Layout

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a behind a firewall (inline) configuration, use the configuration parameters in the following tables (with or without NAT). Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: Behind a Firewall With NAT (Inline) Configuration Parameters

VPN Gateway A (NAT by Router)	VPN Gateway B (NAT by Router)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red	Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red
Config file entries/routing info: security-profile site-to-site tunnel SanFrancisco ip route 10.250.135.0 255.255.255.0 205.25.135.1	Config file entries/routing info: security-profile site-to-site tunnel Boston ip route 10.250.128.0 255.255.255.0 209.80.10.1
Subnet: 10.250.128.0 (net-include)	Subnet: 10.250.128.0 (net-include)

Table: Behind a Firewall Without NAT (Inline)

VPN Gateway A (No NAT)	VPN Gateway B (No NAT)
Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 210.25.135.2 255.255.255.0 Mode: Red
Interface E1: IP: 205.35.129.2 255.255.255.0 Mode: Red	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red
Config file entries/routing info: security-profile site-to-site tunnel SanFrancisco ip route 210.25.129.0 255.255.255.0 205.25.128.2	Config file entries/routing info: security-profile site-to-site tunnel Boston ip route 205.35.129.0 255.255.255.0 210.25.135.2

The VPN Gateway as a Firewall (With or Without NAT)

This scenario shows the following:

- A LAN-to-LAN connection between two VPN Gateways.
- Each VPN Gateway is directly attached to a router. The routers connect through the Internet.
- Traffic travels from Router A to Router B. Router B passes traffic directly through the VPN Gateway.
- The VPN Gateway performs firewall functionality on the traffic and may or may not use NAT.
- The VPN Gateway B decrypts the VPN traffic before passing it to the local network.

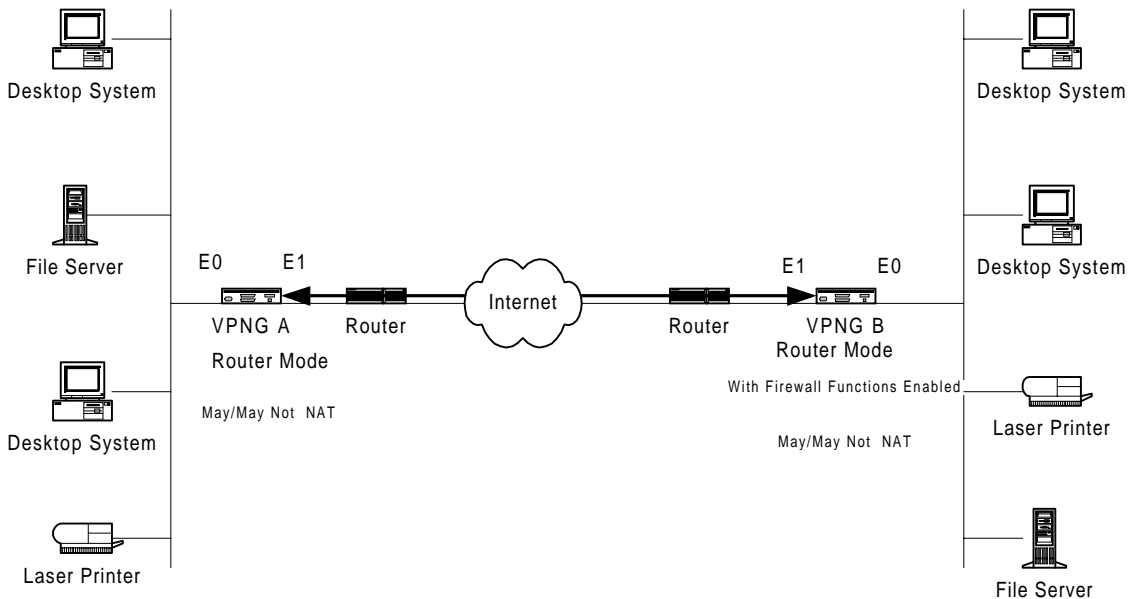


Figure: VPN Gateway as a Firewall

Configuring the VPN Gateway as a Firewall

When setting up a VPN Gateway, you must configure many global configuration settings. You configure the VPN Gateway through the Intel NetStructure VPN Manager or command shell.

To set up a VPN Gateway as a firewall configuration, use the configuration parameters in the following tables (with and without

NAT). Note that the values of these parameters are examples only; you must enter values specific to your network.

Table: VPN Gateway as a Firewall With NAT Configuration Parameters

VPN Gateway A (NAT by Router)	VPN Gateway B (NAT by Router)
Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 10.250.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red	Interface E1: IP: 192.168.10.2 255.255.255.0 Mode: Red
Config file entries/routing info: security-profile site-to-site site-to-site tunnel SanFrancisco security-profile site-to-site route 209.29.128.50 255.255.255.0	Config file entries/routing info: security-profile site-to-site site-to-site tunnel SanFrancisco security-profile site-to-site route 209.29.128.50 255.255.255.0
Subnet: 10.250.128.0 (net-include)	Subnet: 10.250.128.0 (net-include)

Table: VPN Gateway As a Firewall Without NAT Configuration Parameters

VPN Gateway A (No NAT)	VPN Gateway B (No NAT)
Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red	Interface E0: IP: 205.25.128.2 255.255.255.0 Mode: Red
Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red	Interface E1: IP: 210.35.129.2 255.255.255.0 Mode: Red
Config file entries/routing info: security-profile site-to-site site-to-site tunnel SanFrancisco security-profile site-to-site route 209.29.128.50 255.255.255.255	Config file entries/routing info: security-profile site-to-site site-to-site tunnel SanFrancisco security-profile site-to-site route 209.29.128.50 255.255.255.0
Subnet: 205.25.128.0 (net-include)	Subnet: 205.25.128.0 (net-include)

Index

- B**
- behind a firewall
 - inline, with or without NAT 13, 24
 - one-armed, with or without NAT 11, 21
 - bridge configuration 7
- C**
- client scenarios 2–17
 - behind a firewall with or without NAT (inline) 13
 - behind a firewall with or without NAT (one-armed) 11
 - bridge configuration 7
 - edge router configuration 9
 - in parallel with firewall (extranet or intranet) 5
 - inline router configuration 3
 - one-armed router configuration with no firewall 2
 - VPN Gateway as a firewall 15
 - configuring
 - behind a firewall (inline) network layout 14, 25
 - behind a firewall (one-armed) network layout 12
 - behind a firewall (one-armed) with NAT network layout 22
 - behind a firewall (one-armed) without NAT network layout 23
 - bridge configuration 8
 - edge router configuration 10
 - in parallel with a firewall (with NAT) network layout 20
 - in parallel with a firewall (without NAT) network layout 19
 - in parallel with firewall 6
 - inline router configuration 4
 - one-armed router configuration 3
 - VPN Gateway as a firewall 16, 27
- E**
- edge router configuration 9
- I**
- in parallel with a firewall
 - extranet or intranet 5
 - with NAT 19
 - without NAT 18
 - inline router configuration 3
- L**
- LAN-to-LAN scenarios 18–29
 - behind a firewall (one-armed) with or without NAT 21
 - behind a firewall that may or may not use NAT (inline) 24
 - in parallel with a firewall (with NAT) 19
 - in parallel with a firewall (without NAT) 18
 - VPN Gateway as a firewall (with or without NAT) 27
- N**
- NAT (network address translation) 1
- O**
- one-armed router configuration with no firewall 2
- P**
- PSTN (public-switched telephone network) 3
- V**
- VPN Gateway as a firewall 15, 27