AlliedWare^{TM} OS

How To | Create a VPN between an Allied Telesis and a NetScreen Router

Today's network managers often need to incorporate other vendors' equipment into their networks, as companies change and grow. To support this challenge, Allied Telesis routers are designed to inter-operate with a wide range of equipment.

This How To Note details one of the inter-operation solutions from Allied Telesis: creating virtual private networks between Allied Telesis and NetScreen routers. It shows you how to configure a VPN between a local Allied Telesis router and a remote NetScreen router, step-by-step. On the Allied Telesis router, it uses the Site-To-Site VPN wizard for the VPN configuration.

The wizard runs on selected AR400 Allied Telesis routers from the router's web-based GUI (graphical user interface). It asks you to enter a few details and from those it configures the following settings:

- encryption to protect traffic over the VPN
- ISAKMP with a preshared key to manage the VPN
- the firewall, to protect the LANs and to allow traffic to use the VPN
- Network Address Translation (NAT), so that you can access the Internet from the private LAN through a single public IP address. This Internet access does not interfere with the VPN solution.

You can use the command line to set up an equivalent configuration on AR700 and other AR400 Series routers. See "The router commands" on page 28 for a complete list of the commands the configuration uses.

What information will you find in this document?

This How To Note begins with the following information:

- "Related How To Notes" on page 2
- "Which products and software version does it apply to?" on page 2

Then it describes the configuration, in the following sections:

- "The network" on page 3
- "How to configure the Allied Telesis router" on page 4
- "How to configure the NetScreen router" on page 13
- "How to test the tunnel" on page 26
- "The router commands" on page 28

Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

Which products and software version does it apply to?

The VPN wizard is available on the following Allied Telesis routers, running Software Version 2.9.1 or later:

- AR415S
- AR440S, AR441S, AR442S

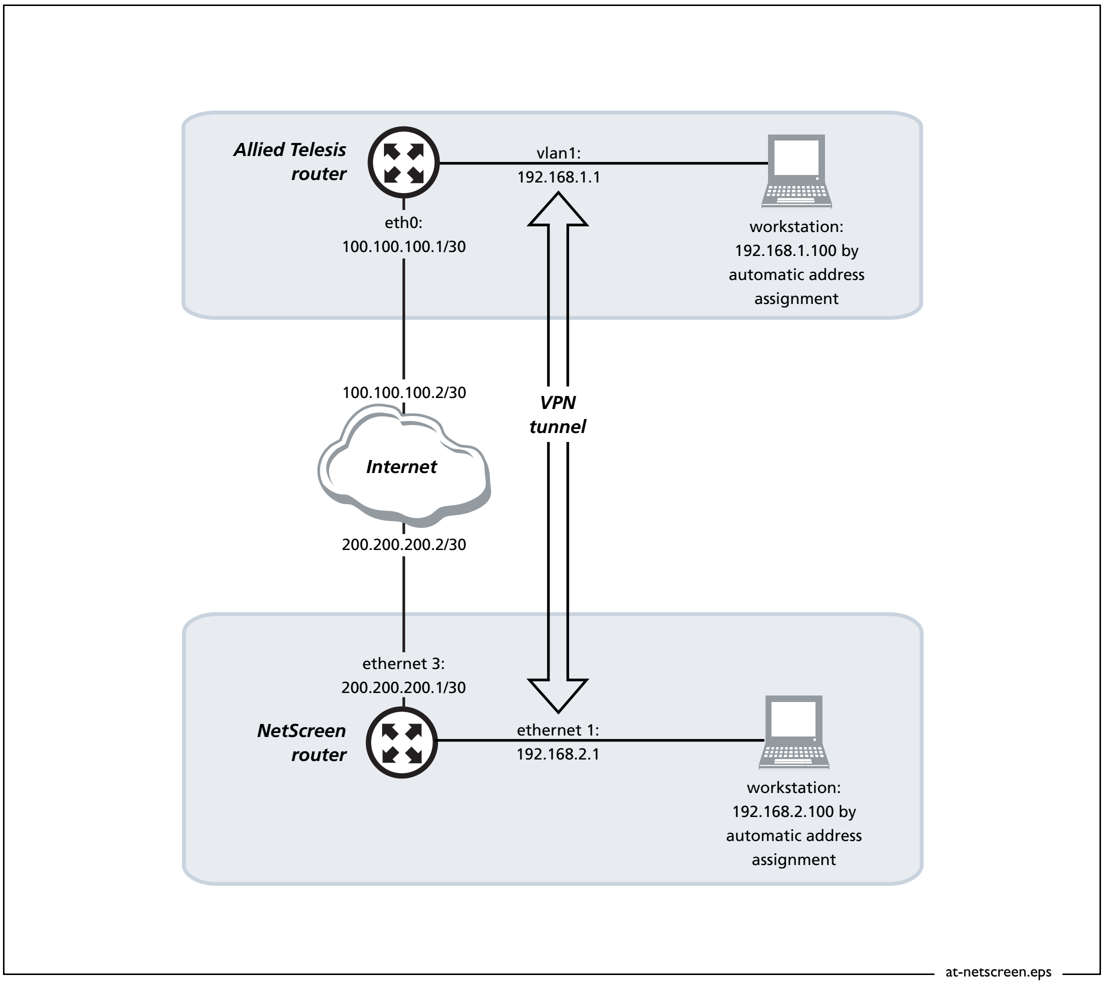
You can use the command line to set up an equivalent configuration on AR700 and other AR400 Series routers. See "The router commands" on page 28 for a complete list of the commands that the configuration uses.

We created this example with a NetScreen 25, running ScreenOS 4.0.3r4.0.

The screenshots in this Note are from an Internet Explorer 6.0 browser running on Windows XP and Windows 2000.

The network

The following diagram shows the LANs and their interfaces and addresses.



How to configure the Allied Telesis router

Before you start

1. Access the router via its GUI.
2. Customise the router and set up vlan1 as the LAN interface. The site-to-site VPN wizard always uses vlan1 as the local LAN for the VPN connection, so you must make sure an IP interface is configured on vlan1 before running the wizard.
3. Create a security officer. If you use the Basic Setup wizard to customise the router, this creates one security officer, with a username of "secoff".
4. Set up the WAN interface appropriately for your connection type. This example shows the steps for both a fixed IP address on the WAN interface (as in the figure above) and a PPPoE interface with a dynamically-assigned address.

The router setup of steps 1-4 is described in *How To Use the Allied Telesis GUI to Customise the Router and Set Up An Internet Connection*, which is available from www.alliedtelesis.com/resources/literature/howto.aspx.

In this example, the Allied Telesis router has the following settings:

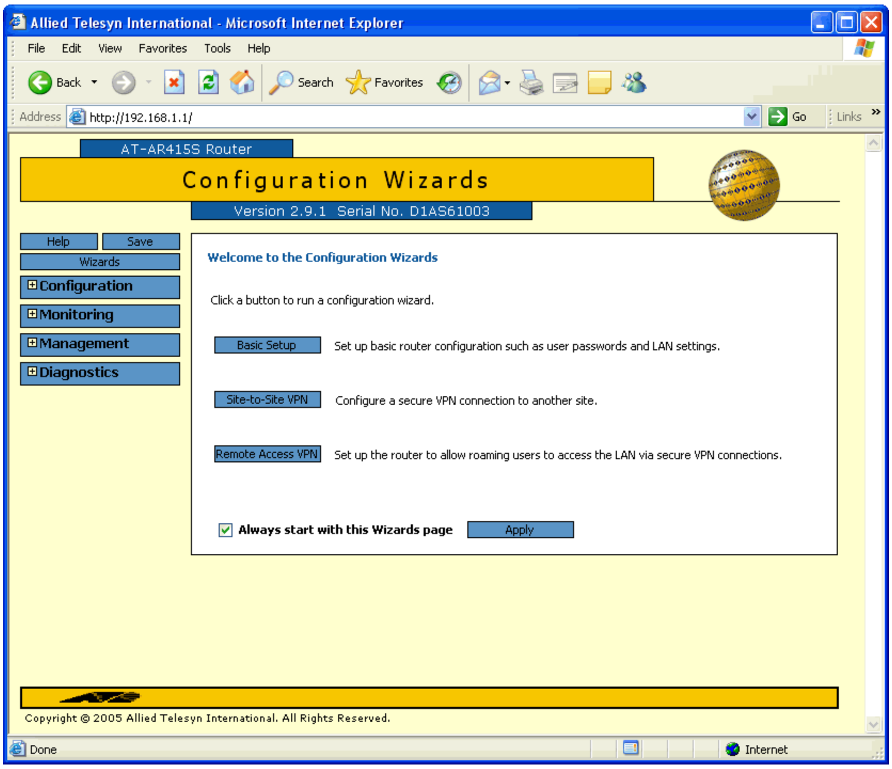
	Interface	Address	Mask
Allied Telesis router LAN	vlan1	192.168.1.1	255.255.255.0
Allied Telesis router WAN:			
if fixed IP address	eth0	100.100.100.1	255.255.255.252
if dynamic IP address	ppp0	0.0.0.0	0.0.0.0
Remote site's WAN settings		200.200.200.1	
Remote site's LAN settings		192.168.2.1	255.255.255.0

Create the VPN tunnel

1. Open the Configuration Wizards page

Log in as either the manager or the security officer. If you log in as the manager, the router changes to secure mode when you finish the VPN wizard and at that stage prompts you to log in again as the security officer.

The Site-To-Site VPN wizard is one of the options on the GUI's Configuration Wizards page. Make sure your browser's pop-up blocker is disabled—the wizard needs to open pop-ups. If you access the Internet through a proxy server, make sure your browser bypasses the proxy for this address.


Allied Telesyn International - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/
Go Links
AT-AR415S Router
Configuration Wizards
Version 2.9.1 Serial No. D1AS61003
Help Save
Wizards
⊞Configuration
⊞Monitoring
⊞Management
⊞Diagnostics
Done
Internet

Welcome to the Configuration Wizards

Click a button to run a configuration wizard.

Basic Setup — Set up basic router configuration such as user passwords and LAN settings.

Site-to-Site VPN — Configure a secure VPN connection to another site.

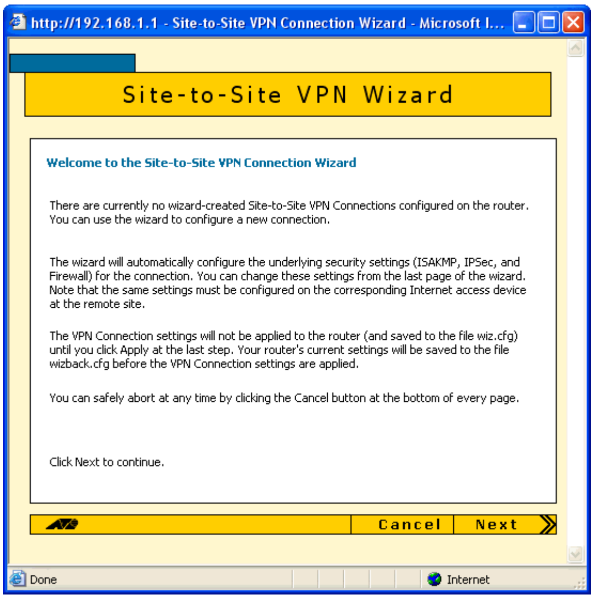
Remote Access VPN — Set up the router to allow roaming users to access the LAN via secure VPN connections.

☑ Always start with this Wizards page Apply

Copyright © 2005 Allied Telesyn International. All Rights Reserved.

The GUI opens at this page the first time you configure your router. After initial configuration it may open at the System Status page instead. If so, click on the Wizards button in the left-hand menu to open the Configuration Wizards page.

2. Start the Site-to-Site VPN wizard


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Next
Done
Internet

Welcome to the Site-to-Site VPN Connection Wizard

There are currently no wizard-created Site-to-Site VPN Connections configured on the router. You can use the wizard to configure a new connection.

The wizard will automatically configure the underlying security settings (ISAKMP, IPSec, and Firewall) for the connection. You can change these settings from the last page of the wizard. Note that the same settings must be configured on the corresponding Internet access device at the remote site.

The VPN Connection settings will not be applied to the router (and saved to the file wiz.cfg) until you click Apply at the last step. Your router's current settings will be saved to the file wizback.cfg before the VPN Connection settings are applied.

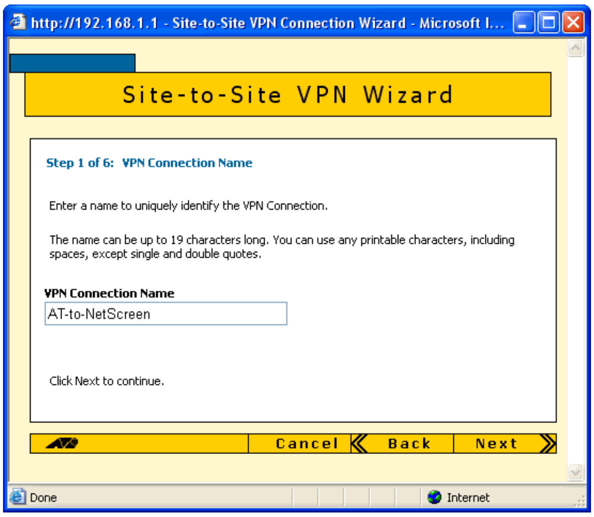
You can safely abort at any time by clicking the Cancel button at the bottom of every page.

Click Next to continue.

Click on the Site-to-Site VPN button. The wizard starts by displaying a welcome message.

Click the Next button.

3. Name the VPN connection


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Back
Next
Done
Internet

Step 1 of 6: VPN Connection Name

Enter a name to uniquely identify the VPN Connection.

The name can be up to 19 characters long. You can use any printable characters, including spaces, except single and double quotes.

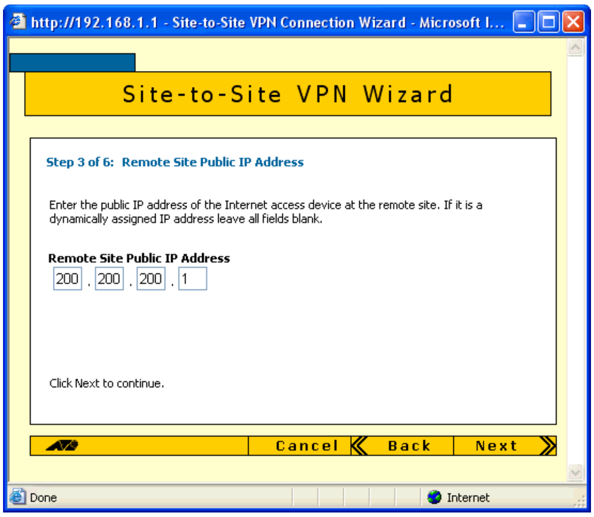
VPN Connection Name: AT-to-NetScreen

Click Next to continue.

Enter an appropriate VPN connection name.

Click the Next button. If you have multiple possible WAN interfaces configured on the router, the wizard next lets you select the appropriate interface. In this example there is only one WAN interface, so the wizard selects it automatically and moves directly to the remote site settings.

4. Enter the remote site's WAN IP address



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Back
Next
Done
Internet

Step 3 of 6: Remote Site Public IP Address

Enter the public IP address of the Internet access device at the remote site. If it is a dynamically assigned IP address leave all fields blank.

Remote Site Public IP Address
200 . 200 . 200 . 1

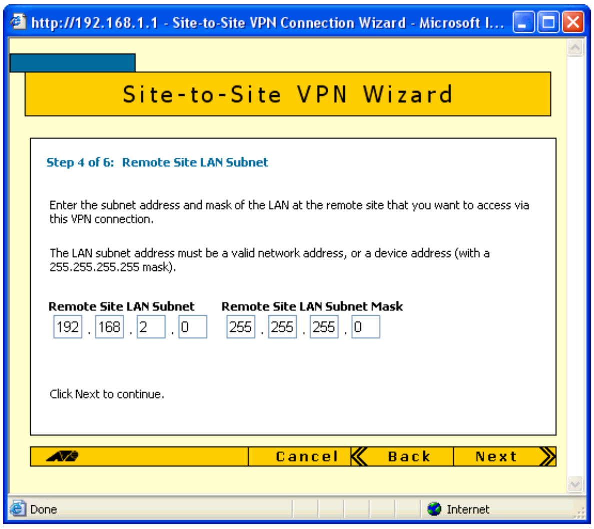
Click Next to continue.

Enter the public IP address of the other end of the tunnel. In this example, this is 200.200.200.1.

Note that you can use the Tab key to move between fields when entering the address, but should not use the . key (the period).

Click the Next button.

5. Enter the remote site's LAN IP address



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Back
Next
Done
Internet

Step 4 of 6: Remote Site LAN Subnet

Enter the subnet address and mask of the LAN at the remote site that you want to access via this VPN connection.

The LAN subnet address must be a valid network address, or a device address (with a 255.255.255.255 mask).

Remote Site LAN Subnet
192 . 168 . 2 . 0

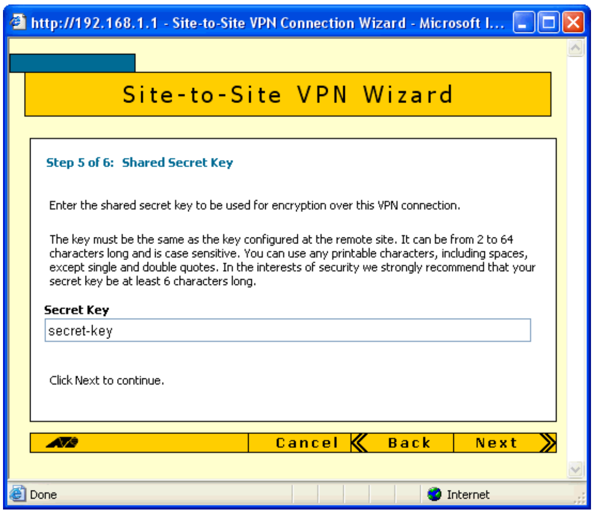
Remote Site LAN Subnet Mask
255 . 255 . 255 . 0

Click Next to continue.

Enter the NetScreen router's LAN subnet address and mask. In this example, this is 192.168.2.0 and a mask of 255.255.255.0.

Click the Next button.

6. Enter the shared secret key



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Back
Next
Done
Internet

Step 5 of 6: Shared Secret Key

Enter the shared secret key to be used for encryption over this VPN connection.

The key must be the same as the key configured at the remote site. It can be from 2 to 64 characters long and is case sensitive. You can use any printable characters, including spaces, except single and double quotes. In the interests of security we strongly recommend that your secret key be at least 6 characters long.

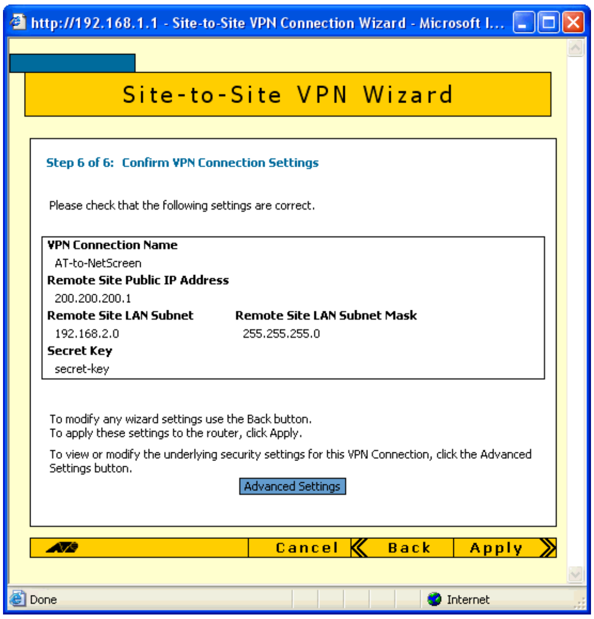
Secret Key: secret-key

Click Next to continue.

Enter the secret key, which is an alphanumeric string between 2 and 64 characters long. Both routers must use the same secret key. On the NetScreen router, this is the Preshared Secret.

Click the Next button.

7. Check the settings



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Advanced Settings
Cancel
Back
Apply
Done
Internet

Step 6 of 6: Confirm VPN Connection Settings

Please check that the following settings are correct.

VPN Connection Name
AT-to-NetScreen
Remote Site Public IP Address
200.200.200.1
Remote Site LAN Subnet 192.168.2.0 **Remote Site LAN Subnet Mask** 255.255.255.0
Secret Key
secret-key

To modify any wizard settings use the Back button.
To apply these settings to the router, click Apply.

To view or modify the underlying security settings for this VPN Connection, click the Advanced Settings button.

Check the summary. If necessary, use the wizard's Back button to return and correct any settings you want to change.

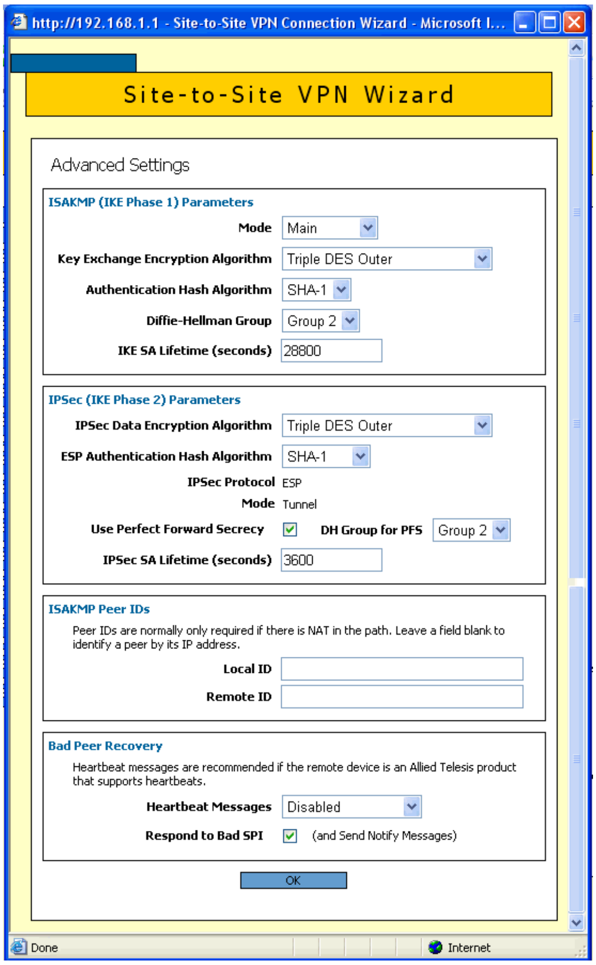
Once you are happy with the settings, click the Advanced Settings button to configure additional settings that allow interoperation with the NetScreen router.

8. Configure additional settings

This step has two alternatives:

- if your WAN connection has a static IP address, you need to configure Perfect Forward Secrecy. This is the first alternative
- if your WAN connection has a dynamic IP address, you need to use Aggressive Mode, configure Perfect Forward Secrecy, and give the peer a local ID. This is the second alternative, shown on the next page

Static address


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Done
Internet

Advanced Settings

ISAKMP (IKE Phase 1) Parameters

Mode	Main
Key Exchange Encryption Algorithm	Triple DES Outer
Authentication Hash Algorithm	SHA-1
Diffie-Hellman Group	Group 2
IKE SA Lifetime (seconds)	28800

IPSec (IKE Phase 2) Parameters

IPSec Data Encryption Algorithm	Triple DES Outer
ESP Authentication Hash Algorithm	SHA-1
IPSec Protocol	ESP
Mode	Tunnel
Use Perfect Forward Secrecy	☑ **DH Group for PFS** Group 2
IPSec SA Lifetime (seconds)	3600

ISAKMP Peer IDs

Peer IDs are normally only required if there is NAT in the path. Leave a field blank to identify a peer by its IP address.

Local ID	
Remote ID	

Bad Peer Recovery

Heartbeat messages are recommended if the remote device is an Allied Telesis product that supports heartbeats.

Heartbeat Messages	Disabled
Respond to Bad SPI	☑ (and Send Notify Messages)

OK

If you have a static address, then in the middle of the Advanced Settings page, select the Use Perfect Forward Secrecy checkbox and set the DH Group for PFS to Group 2.

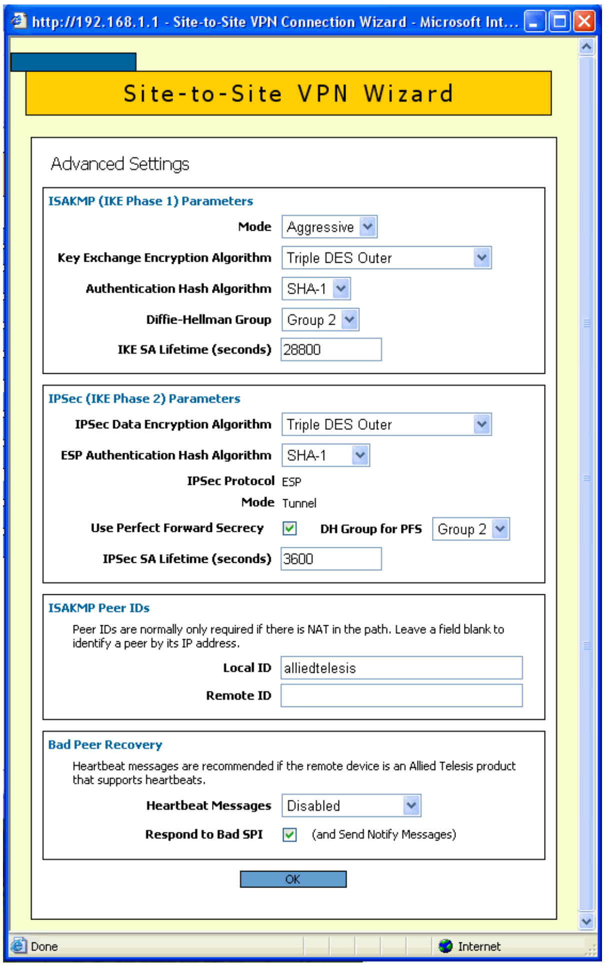
Then click the OK button.

Dynamic address

If you have a dynamic address, then on the Advanced Settings page:

- at the top, select Aggressive Mode
- in the middle, select the Use Perfect Forward Secrecy checkbox and set the DH Group for PFS to Group 2
- towards the bottom, enter a Local ID. This ID lets the NetScreen router validate the Allied Telesis router. Therefore, it must match the Remote User ID value that you enter on the NetScreen router

Then click the OK button.



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft Int...

Site-to-Site VPN Wizard

Advanced Settings

ISAKMP (IKE Phase 1) Parameters

Mode	Aggressive
Key Exchange Encryption Algorithm	Triple DES Outer
Authentication Hash Algorithm	SHA-1
Diffie-Hellman Group	Group 2
IKE SA Lifetime (seconds)	28800

IPSec (IKE Phase 2) Parameters

IPSec Data Encryption Algorithm	Triple DES Outer
ESP Authentication Hash Algorithm	SHA-1
IPSec Protocol	ESP
Mode	Tunnel
Use Perfect Forward Secrecy	☑ DH Group for PFS: Group 2
IPSec SA Lifetime (seconds)	3600

ISAKMP Peer IDs

Peer IDs are normally only required if there is NAT in the path. Leave a field blank to identify a peer by its IP address.

Local ID	alliedtelesis
Remote ID	

Bad Peer Recovery

Heartbeat messages are recommended if the remote device is an Allied Telesis product that supports heartbeats.

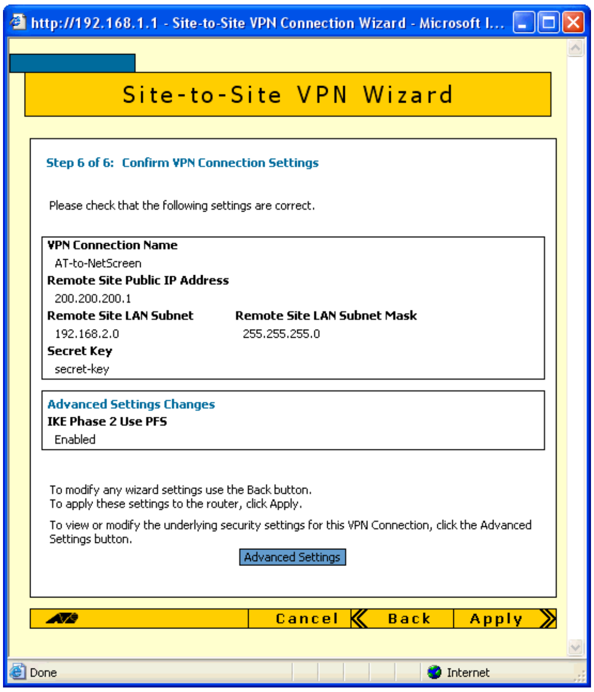
Heartbeat Messages	Disabled
Respond to Bad SPI	☑ (and Send Notify Messages)

9. Check the settings again

Static address

Check the summary.

If you have a static address, the summary now includes the Perfect Forward Secrecy setting.



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...

Site-to-Site VPN Wizard

Step 6 of 6: Confirm VPN Connection Settings

Please check that the following settings are correct.

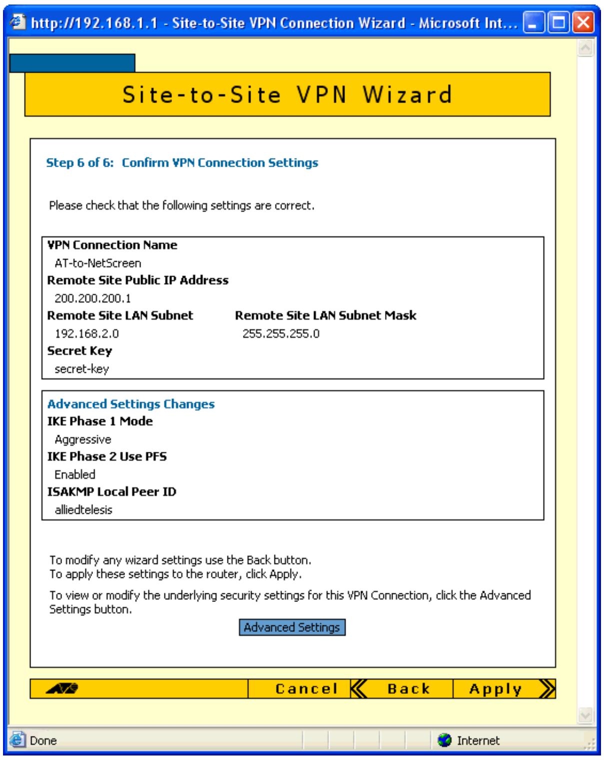
VPN Connection Name
AT-to-NetScreen
Remote Site Public IP Address
200.200.200.1
Remote Site LAN Subnet 192.168.2.0
Remote Site LAN Subnet Mask 255.255.255.0
Secret Key
secret-key

Advanced Settings Changes
IKE Phase 2 Use PFS
Enabled

To modify any wizard settings use the Back button.
To apply these settings to the router, click Apply.

To view or modify the underlying security settings for this VPN Connection, click the Advanced Settings button.

Dynamic address


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft Int...
Site-to-Site VPN Wizard

Step 6 of 6: Confirm VPN Connection Settings

Please check that the following settings are correct.

VPN Connection Name
AT-to-NetScreen
Remote Site Public IP Address
200.200.200.1
Remote Site LAN Subnet 192.168.2.0
Remote Site LAN Subnet Mask 255.255.255.0
Secret Key
secret-key

Advanced Settings Changes
IKE Phase 1 Mode
Aggressive
IKE Phase 2 Use PFS
Enabled
ISAKMP Local Peer ID
alliedtelesis

To modify any wizard settings use the Back button.
To apply these settings to the router, click Apply.

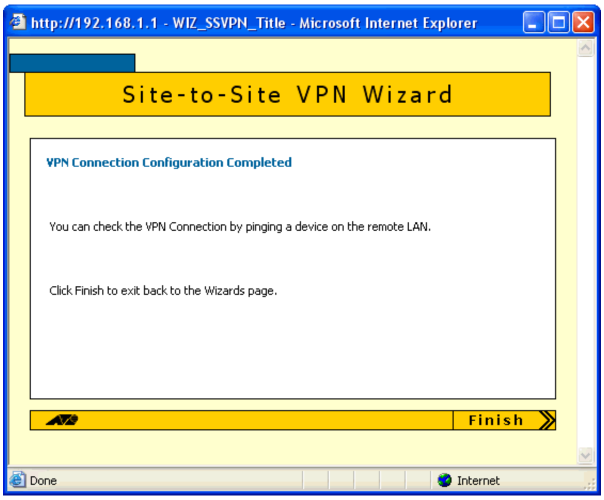
To view or modify the underlying security settings for this VPN Connection, click the Advanced Settings button.

If you have a dynamic address, the summary now includes Aggressive Mode, the Perfect Forward Secrecy settings, and the Local ID.

If necessary, correct any settings you want to change. When all the settings are correct, click the Apply button.

10. Finish the wizard

Security officer


http://192.168.1.1 - WIZ_SSVPN_Title - Microsoft Internet Explorer
Site-to-Site VPN Wizard

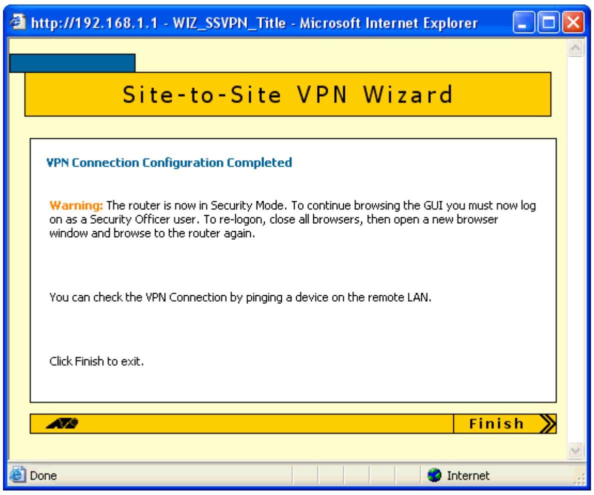
VPN Connection Configuration Completed

You can check the VPN Connection by pinging a device on the remote LAN.

Click Finish to exit back to the Wizards page.

If you are logged in as the security officer, the GUI displays a completion message. Click the Finish button to finish the Wizard and save the VPN settings.

Manager


http://192.168.1.1 - WIZ_SSVPN_Title - Microsoft Internet Explorer
Site-to-Site VPN Wizard
Finish
Done
Internet

VPN Connection Configuration Completed

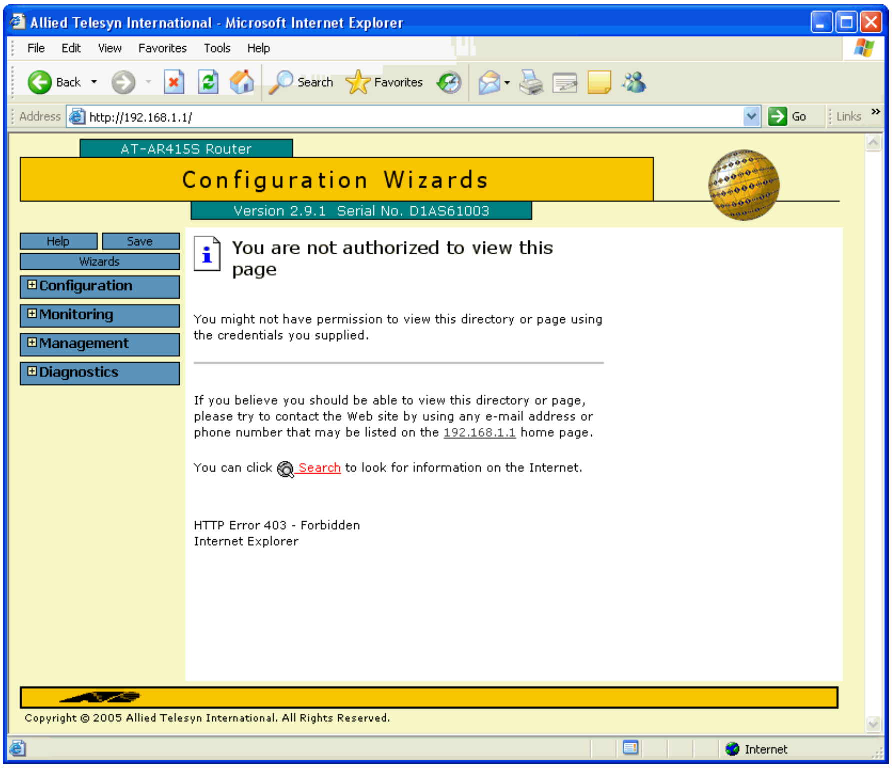
Warning: The router is now in Security Mode. To continue browsing the GUI you must now log on as a Security Officer user. To re-logon, close all browsers, then open a new browser window and browse to the router again.

You can check the VPN Connection by pinging a device on the remote LAN.

Click Finish to exit.

If you are logged in as manager, the GUI displays a message to warn you that you will need to close your browser and re-login as a security officer (see below) once you have finished the wizard.

Click the Finish button to finish the Wizard and save the VPN settings. The browser now indicates that you no longer have permission to view the GUI.


Allied Telesyn International - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/
Go Links
AT-AR415S Router
Configuration Wizards
Version 2.9.1 Serial No. D1AS61003
Help
Save
Wizards
Configuration
Monitoring
Management
Diagnostics
Internet

You are not authorized to view this page

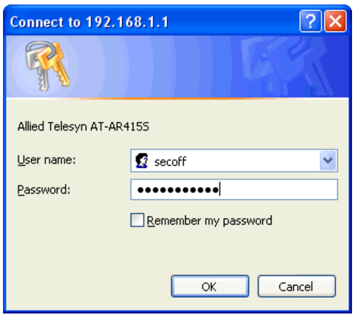
You might not have permission to view this directory or page using the credentials you supplied.

If you believe you should be able to view this directory or page, please try to contact the Web site by using any e-mail address or phone number that may be listed on the 192.168.1.1 home page.

You can click Search to look for information on the Internet.

HTTP Error 403 - Forbidden
Internet Explorer

Copyright © 2005 Allied Telesyn International. All Rights Reserved.



Allied Telesyn AT-AR415S

User name: secoff

Password: ••••••••••

The router configuration is now complete. If required, you can log in to the router again for further configuration or monitoring. To do this, close your browser, open it again, and browse to the router's IP address.

If you used the Basic Setup wizard to configure the LAN settings, the router will have one security officer, with a username of "secoff".

Login as the security officer.

How to configure the NetScreen router

To configure the NetScreen router, perform the steps in the following sections:

1. "Access the Router" on page 13
2. "Configure the interfaces" on page 15
3. "Configure routing" on page 18
4. "Configure the VPN" on page 21

Access the Router

By default, the NetScreen router starts up with a management IP address of 192.168.1.1 and mask of 255.255.255.0 on the ethernet1 port.

Resetting to factory defaults

If you have difficulty accessing your NetScreen router, you may need to reset it to its factory defaults. To do this:

1. Power up the NetScreen.
2. Press the Asset Recovery Pinhole button—beside the console port—with a paper clip or something similar. The Status1 LED flashes orange. Keep pressing the button for 6 seconds until the LED flashes green.
3. Release the button, then press it again. The LED flashes red (if it does not flash red, keep trying until it does). Keep pressing the button for another 6 seconds until the LED turns off.

1. Connect a PC to the router

Select a standalone PC to configure the router from—a PC that is not connected into any existing LAN.

Connect a NIC card on the PC to the ethernet1 port.

2. Set the PC's IP address

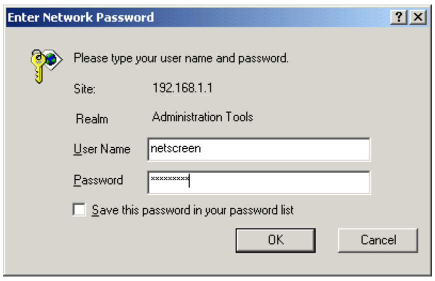
Give your PC an address in the 192.168.1.0 subnet.

3. Browse to the router's management GUI

Browse to 192.168.1.1. If you are using a pop-up blocker, disable it for this address. If you access the Internet through a proxy server, set your browser to bypass the proxy for this address.

The login dialog box opens.

4. Log on


Enter Network Password

Please type your user name and password.

Site:	192.168.1.1
Realm	Administration Tools
User Name	netscreen
Password	*********

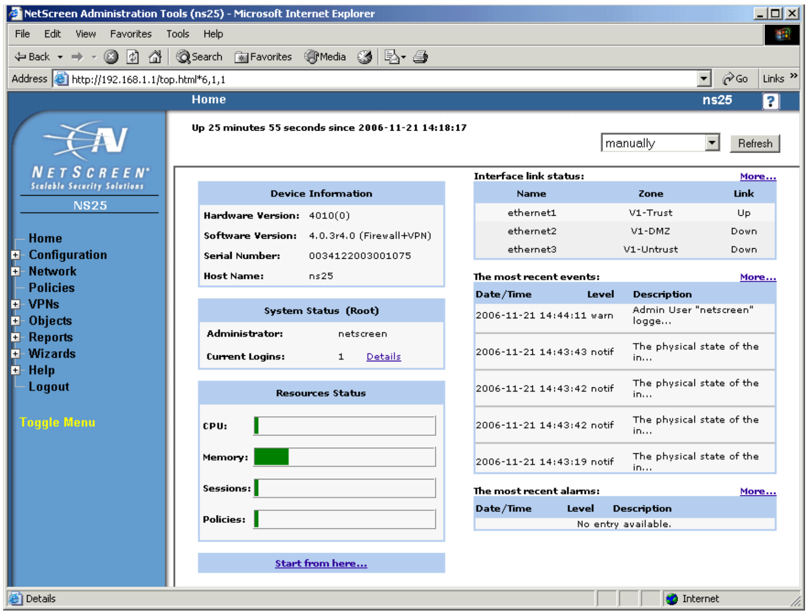
□ Save this password in your password list

The defaults are

username: netscreen

password: netscreen

The router opens at its Home page.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer

Up 25 minutes 55 seconds since 2006-11-21 14:18:17

Device Information	
Hardware Version:	4010(0)
Software Version:	4.0.3r4.0 (Firewall+VPN)
Serial Number:	0034122003001075
Host Name:	ns25

System Status (Root)		
Administrator:	netscreen	
Current Logins:	1	Details

Resources Status

CPU:
Memory:
Sessions:
Policies:

Interface link status: More...

Name	Zone	Link
ethernet1	V1-Trust	Up
ethernet2	V1-DMZ	Down
ethernet3	V1-Untrust	Down

The most recent events: More...

Date/Time	Level	Description
2006-11-21 14:44:11	warn	Admin User "netscreen" logge...
2006-11-21 14:43:43	notif	The physical state of the in...
2006-11-21 14:43:42	notif	The physical state of the in...
2006-11-21 14:43:42	notif	The physical state of the in...
2006-11-21 14:43:19	notif	The physical state of the in...

The most recent alarms: More...

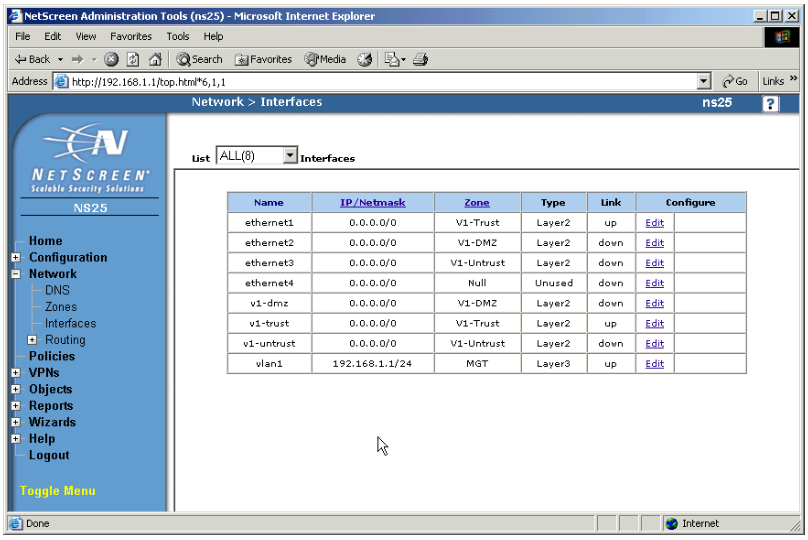
Date/Time	Level	Description
No entry available.		

Configure the interfaces

The following steps configure ethernet1 as the interface to the LAN and ethernet3 as the interface to the WAN.

1. Display the interfaces

From the left-hand menu on the Home page, select Network, then Interfaces. The GUI displays the Interfaces Table page.



NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/top.html*6,1,1
Go Links
Network > Interfaces
ns25
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Done
Internet

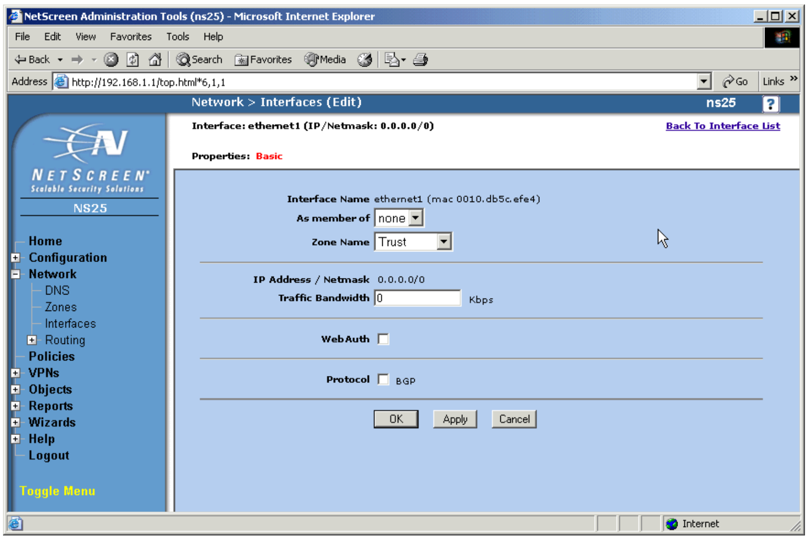
List ALL(8) Interfaces

Name	IP/Netmask	Zone	Type	Link	Configure	
ethernet1	0.0.0.0/0	V1-Trust	Layer2	up	Edit	
ethernet2	0.0.0.0/0	V1-DMZ	Layer2	down	Edit	
ethernet3	0.0.0.0/0	V1-Untrust	Layer2	down	Edit	
ethernet4	0.0.0.0/0	Null	Unused	down	Edit	
v1-dmz	0.0.0.0/0	V1-DMZ	Layer2	down	Edit	
v1-trust	0.0.0.0/0	V1-Trust	Layer2	up	Edit	
v1-untrust	0.0.0.0/0	V1-Untrust	Layer2	down	Edit	
vlan1	192.168.1.1/24	MGT	Layer3	up	Edit	

On the ethernet1 row, click Edit.

2. Set the Zone Name for ethernet1

Select a Zone Name of Trust.



NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/top.html*6,1,1
Go Links
Network > Interfaces (Edit)
ns25
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Internet
Back To Interface List
OK
Apply
Cancel

Interface: ethernet1 (IP/Netmask: 0.0.0.0/0)

Properties: Basic

Interface Name ethernet1 (mac 0010.db5c.efe4)

As member of none

Zone Name Trust

IP Address / Netmask 0.0.0.0/0

Traffic Bandwidth 0 Kbps

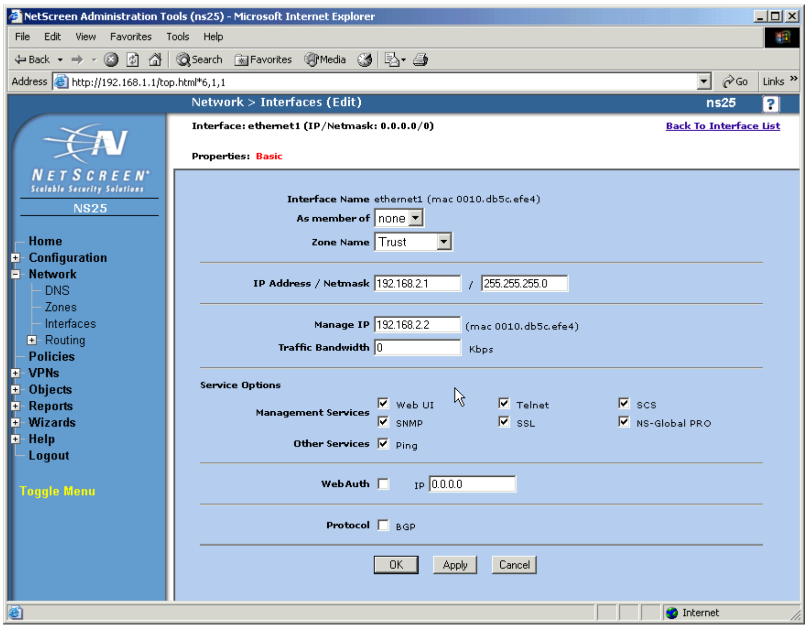
WebAuth □

Protocol □ BGP

Click the Apply button. The page refreshes with more settings available.

3. Change the IP address for ethernet1, if necessary

Change the IP address if you need to. In this example, the address is 192.168.2.1. If you change the subnet (as we did) you must also change the management IP address for the interface.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/top.html*6,1,1
Go Links
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Internet

Network > Interfaces (Edit) ns25

Interface: ethernet1 (IP/Netmask: 0.0.0.0/0) Back To Interface List

Properties: Basic

Interface Name ethernet1 (mac 0010.db5c.efe4)

As member of none

Zone Name Trust

IP Address / Netmask 192.168.2.1 / 255.255.255.0

Manage IP 192.168.2.2 (mac 0010.db5c.efe4)

Traffic Bandwidth 0 Kbps

Service Options

Management Services ☑ Web UI ☑ Telnet ☑ SCS ☑ SNMP ☑ SSL ☑ NS-Global PRO

Other Services ☑ Ping

WebAuth □ IP 0.0.0.0

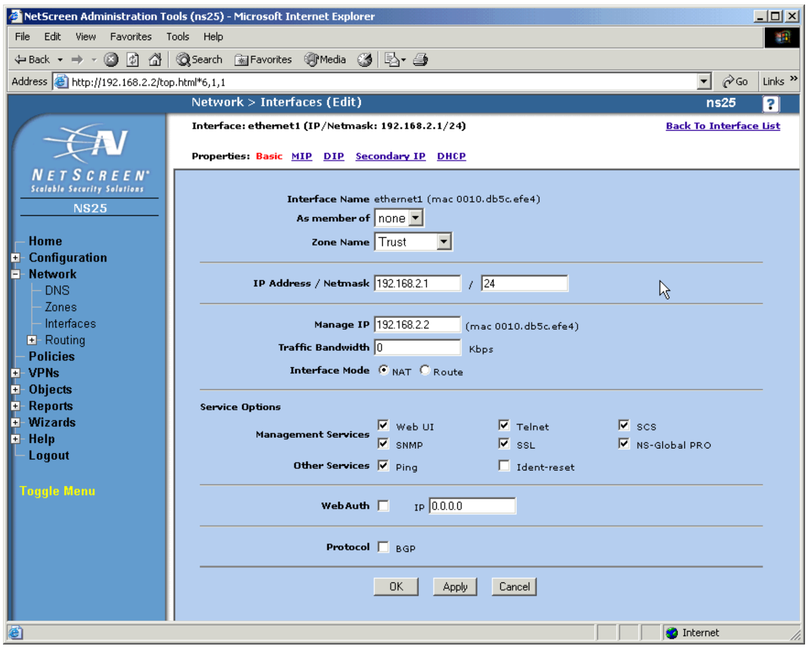
Protocol □ BGP

OK Apply Cancel

Click the Apply button. The page refreshes with even more settings available.

4. Check the interface mode for ethernet1

Check that the Interface Mode is set to NAT, so that the router translates addresses of packets from your private LAN to your public address.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Internet

Network > Interfaces (Edit) ns25

Interface: ethernet1 (IP/Netmask: 192.168.2.1/24) Back To Interface List

Properties: Basic MIP DIP Secondary IP DHCP

Interface Name ethernet1 (mac 0010.db5c.efe4)

As member of none

Zone Name Trust

IP Address / Netmask 192.168.2.1 / 24

Manage IP 192.168.2.2 (mac 0010.db5c.efe4)

Traffic Bandwidth 0 Kbps

Interface Mode ● NAT ○ Route

Service Options

Management Services ☑ Web UI ☑ Telnet ☑ SCS ☑ SNMP ☑ SSL ☑ NS-Global PRO

Other Services ☑ Ping □ Ident-reset

WebAuth □ IP 0.0.0.0

Protocol □ BGP

OK Apply Cancel

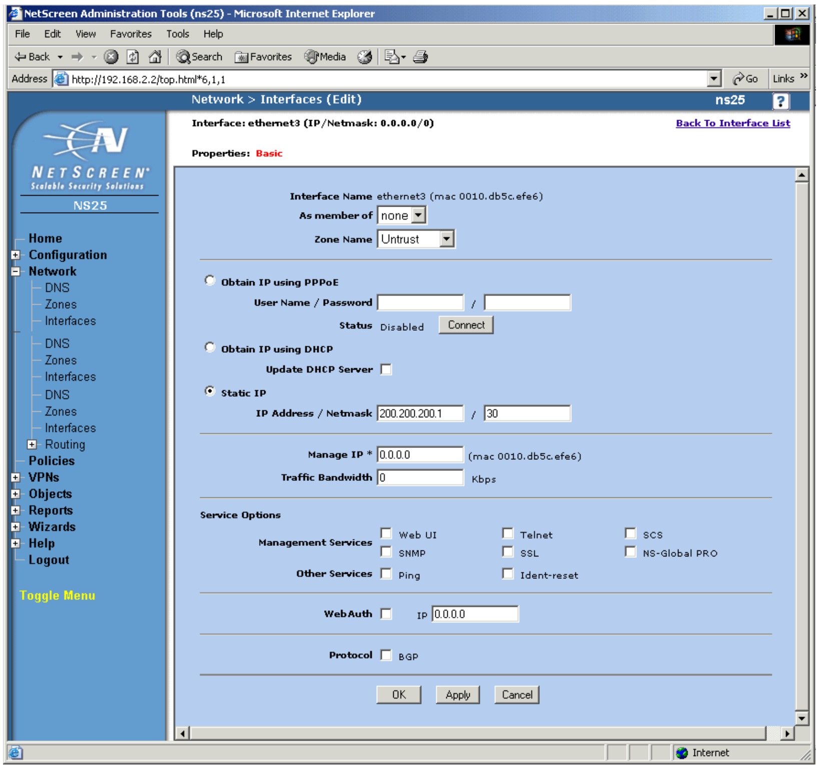
Click the OK button. If you changed the management IP address in step 3, this stops your browser from accessing the GUI. Change the IP address on your PC if necessary, and browse to the new management address.

You have now finished configuring ethernet1. The next steps configure ethernet3, which is the public WAN interface.

If necessary, browse to Network, then Interfaces again. On the ethernet3 row, click Edit.

5. Set the IP address for ethernet3

Check that the Zone Name is set to Untrust, and specify the appropriate IP address. In this example, the address is a Static IP of 200.200.200.1 and a mask of 30.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
NETSCREEN
Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
DNS
Zones
Interfaces
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Internet

Network > Interfaces (Edit) ns25

Interface: ethernet3 (IP/Netmask: 0.0.0.0/0) Back To Interface List

Properties: Basic

Interface Name ethernet3 (mac 0010.db5c.efe6)
As member of none
Zone Name Untrust

○ Obtain IP using PPPoE
User Name / Password ______ / ______
Status Disabled [Connect]

○ Obtain IP using DHCP
Update DHCP Server □

● Static IP
IP Address / Netmask 200.200.200.1 / 30

Manage IP * 0.0.0.0 (mac 0010.db5c.efe6)
Traffic Bandwidth 0 Kbps

Service Options
Management Services □ Web UI □ Telnet □ SCS □ SNMP □ SSL □ NS-Global PRO
Other Services □ Ping □ Ident-reset

WebAuth □ IP 0.0.0.0

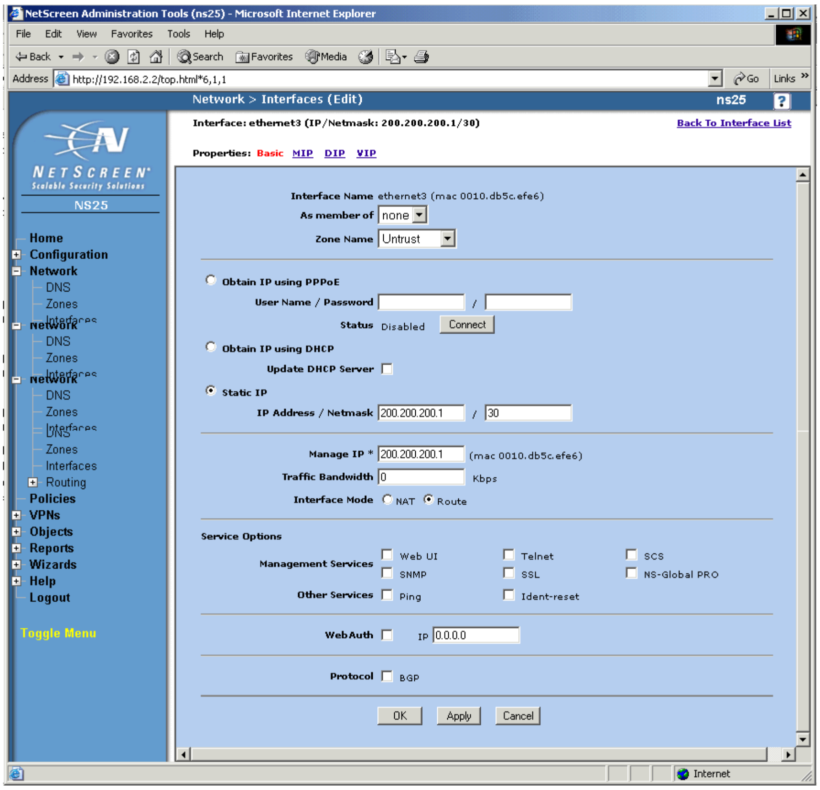
Protocol □ BGP

[OK] [Apply] [Cancel]

Click the Apply button. The page refreshes with more settings available.

6. Set the interface mode for ethernet3

Check that the Interface Mode is set to Route.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.2/top.html*6,1,1
Network > Interfaces (Edit)
ns25
NETSCREEN
Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Back To Interface List
Properties: Basic MIP DIP VIP
OK
Apply
Cancel

Interface: ethernet3 (IP/Netmask: 200.200.200.1/30)

Interface Name ethernet3 (mac 0010.db5c.efe6)

As member of none

Zone Name Untrust

○ Obtain IP using PPPoE

User Name / Password /

Status Disabled Connect

○ Obtain IP using DHCP

Update DHCP Server □

● Static IP

IP Address / Netmask 200.200.200.1 / 30

Manage IP * 200.200.200.1 (mac 0010.db5c.efe6)

Traffic Bandwidth 0 Kbps

Interface Mode ○ NAT ● Route

Service Options

Management Services □ Web UI □ Telnet □ SCS □ SNMP □ SSL □ NS-Global PRO

Other Services □ Ping □ Ident-reset

WebAuth □ IP 0.0.0.0

Protocol □ BGP

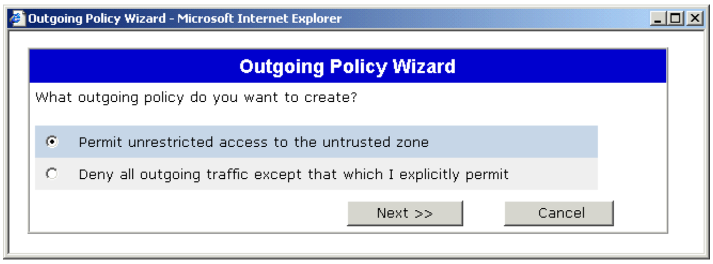
Click the OK button. You have now finished configuring ethernet3.

Configure routing

By default, the NetScreen router blocks all LAN traffic from accessing the WAN. The following steps change this, and also configure a default route.

1. Start the Outgoing Policy Wizard

From the left-hand menu on the Home page, select Wizards, then Outgoing Policy. The GUI displays the first page of the wizard. Select “Permit unrestricted access to the untrusted zone”.



Outgoing Policy Wizard

What outgoing policy do you want to create?

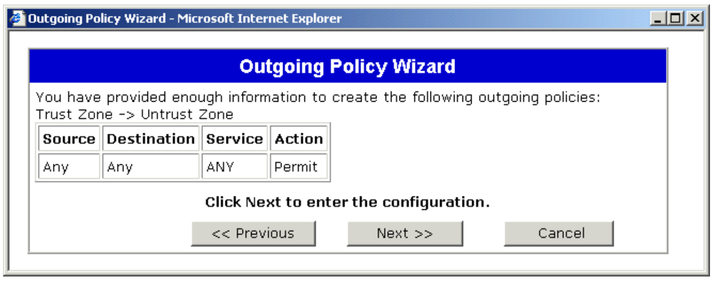
● Permit unrestricted access to the untrusted zone

○ Deny all outgoing traffic except that which I explicitly permit

Click the Next button.

2. Check the policy settings

The wizard displays a summary of the settings for you to confirm.



Outgoing Policy Wizard

You have provided enough information to create the following outgoing policies:
Trust Zone -> Untrust Zone

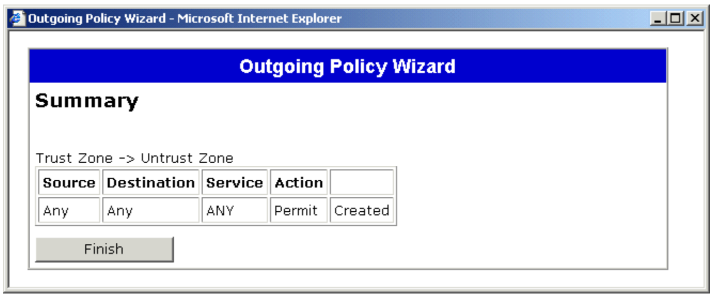
Source	Destination	Service	Action
Any	Any	ANY	Permit

Click Next to enter the configuration.

Click the Next button.

3. End the wizard

The wizard displays a summary of the settings.



Outgoing Policy Wizard

Summary

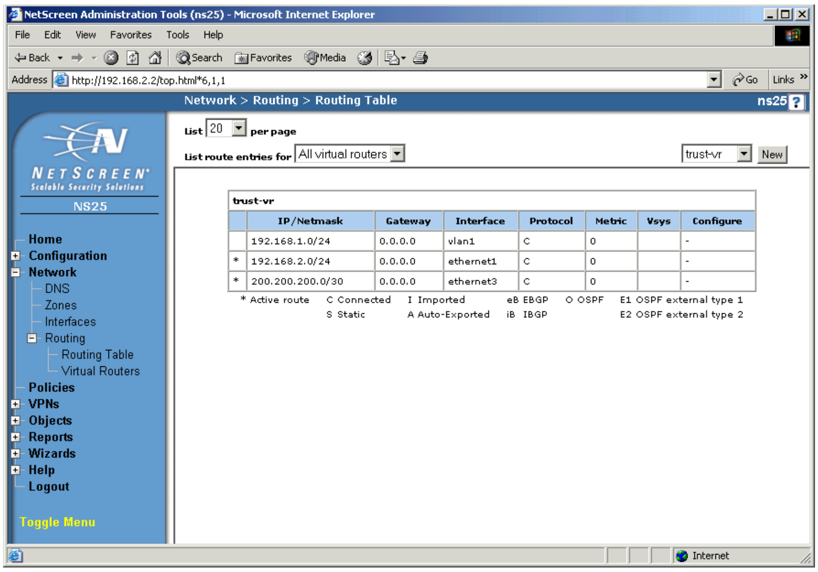
Trust Zone -> Untrust Zone

Source	Destination	Service	Action	
Any	Any	ANY	Permit	Created

Click the Finish button. The GUI displays the Interface Table page again.

4. Display the routes

From the left-hand menu on the Home page, select Network, then Routing, then Routing Table. The GUI displays the Routing Table page.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
Network > Routing > Routing Table
ns25
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Routing Table
Virtual Routers
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Internet

List 20 per page

List route entries for All virtual routers — trust-vr — New

trust-vr

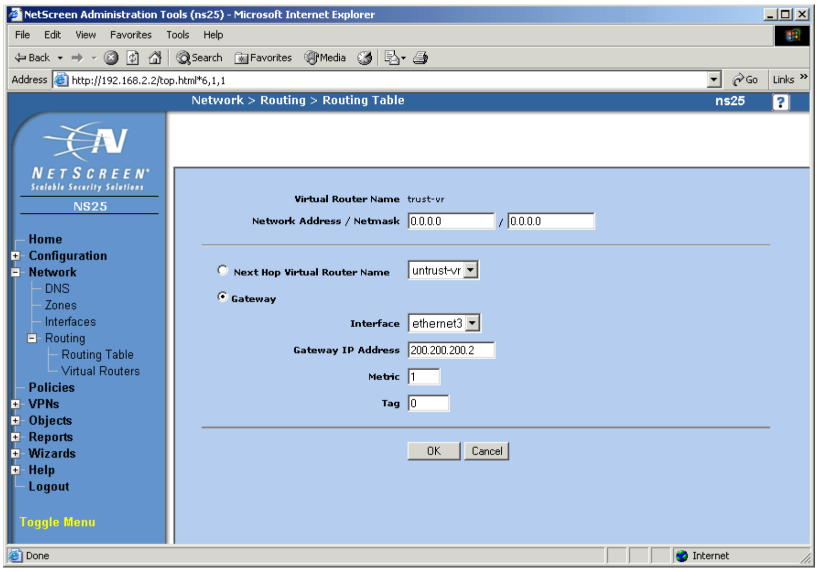
	IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure
	192.168.1.0/24	0.0.0.0	vlan1	C	0		-
*	192.168.2.0/24	0.0.0.0	ethernet1	C	0		-
*	200.200.200.0/30	0.0.0.0	ethernet3	C	0		-

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1
S Static A Auto-Exported iB IBGP E2 OSPF external type 2

Click the New button.

5. Configure the default route

Enter a Network Address and Netmask of 0.0.0.0. Select the Gateway option, with an Interface of ethernet3 and your ISP's address as the Gateway IP Address. In this example, the gateway address is 200.200.200.2.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
Network > Routing > Routing Table
ns25
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Routing Table
Virtual Routers
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
OK
Cancel
Done
Internet

Virtual Router Name trust-vr

Network Address / Netmask 0.0.0.0 / 0.0.0.0

○ Next Hop Virtual Router Name untrust-vr

● Gateway

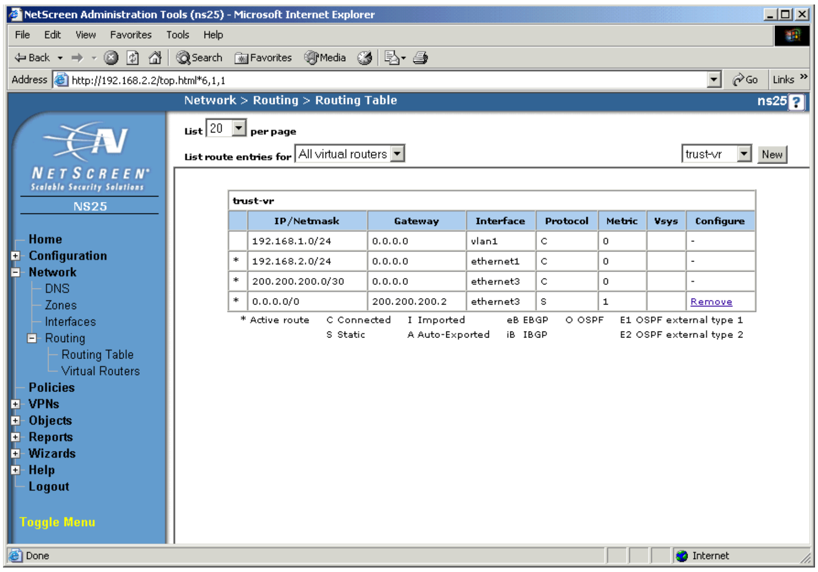
Interface ethernet3

Gateway IP Address 200.200.200.2

Metric 1

Tag 0

Click the OK button. The GUI displays the Routing Table page again. Check that your route is correct.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.2/top.html*6,1,1
Network > Routing > Routing Table
ns25
NS25
Home
Configuration
Network
DNS
Zones
Interfaces
Routing
Routing Table
Virtual Routers
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
New
Done
Internet

List 20 per page

List route entries for All virtual routers

trust-vr

trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure
	192.168.1.0/24	0.0.0.0	vlan1	C	0		-
*	192.168.2.0/24	0.0.0.0	ethernet1	C	0		-
*	200.200.200.0/30	0.0.0.0	ethernet3	C	0		-
*	0.0.0.0/0	200.200.200.2	ethernet3	S	1		Remove

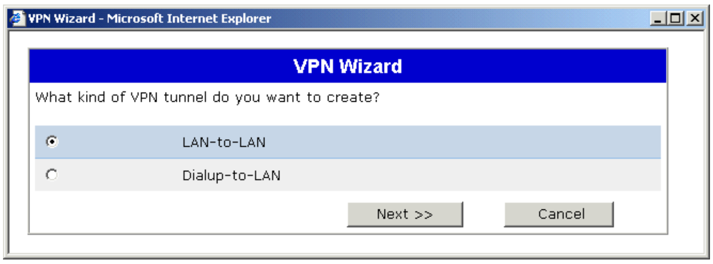
* Active route   C Connected   I Imported   eB EBGP   O OSPF   E1 OSPF external type 1
S Static   A Auto-Exported   iB IBGP   E2 OSPF external type 2

Configure the VPN

The following steps create the VPN.

1. Start the VPN Wizard

From the left-hand menu on the Home page, select Wizards, then VPN. The GUI displays the first page of the wizard. Select LAN-to-LAN.



What kind of VPN tunnel do you want to create?

● LAN-to-LAN

○ Dialup-to-LAN

Click the Next button.

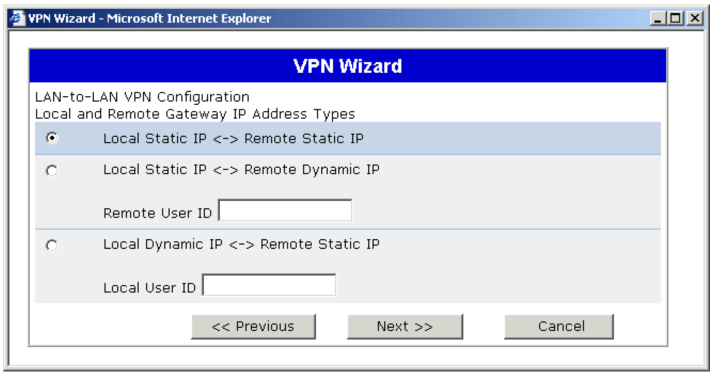
2. Select the type of address

Select the appropriate option. This example shows the options for when:

- both the Allied Telesis and the NetScreen routers have static IP addresses
- the Allied Telesis router has a dynamic address

Static remote address

If both ends of the VPN have fixed IP addresses, select Local Static to Remote Static and click the Next button.


VPN Wizard - Microsoft Internet Explorer

VPN Wizard

LAN-to-LAN VPN Configuration
Local and Remote Gateway IP Address Types

● Local Static IP <-> Remote Static IP

○ Local Static IP <-> Remote Dynamic IP

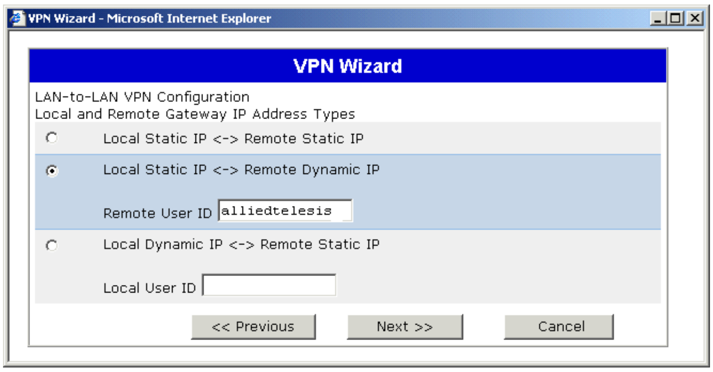
Remote User ID

○ Local Dynamic IP <-> Remote Static IP

Local User ID

Dynamic remote address

If the Allied Telesis router has a dynamic IP address, select Local Static IP to Remote Dynamic IP. In the Remote User ID field, enter the Local ID that you specified on the Allied Telesis router Advanced page. Then click the Next button.


VPN Wizard - Microsoft Internet Explorer

VPN Wizard

LAN-to-LAN VPN Configuration
Local and Remote Gateway IP Address Types

○ Local Static IP <-> Remote Static IP

● Local Static IP <-> Remote Dynamic IP

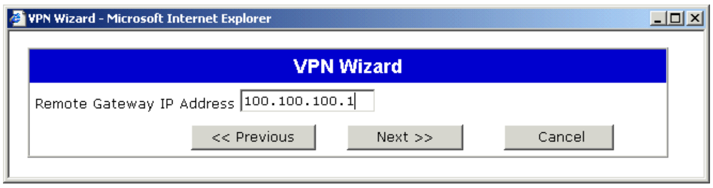
Remote User ID alliedtelesis

○ Local Dynamic IP <-> Remote Static IP

Local User ID

3. Specify the remote address, if it is static

If you chose the Local Static to Remote Static option at the step before, enter the Allied Telesis router's public IP address, 100.100.100.1 in this example. If you chose the Remote Dynamic IP option, you do not see this step.

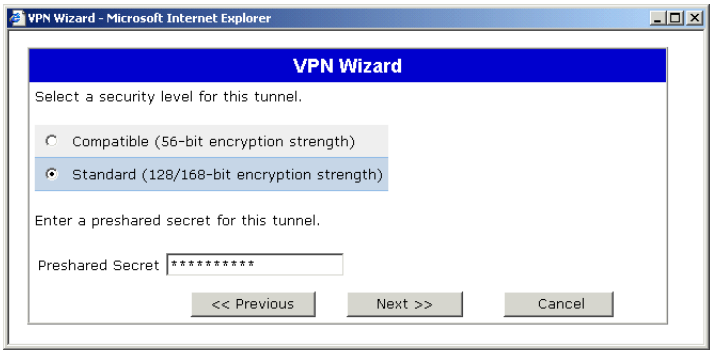


Remote Gateway IP Address 100.100.100.1

Click the Next button.

4. Specify the encryption strength and key

Select Standard encryption and enter the preshared key. The key must be the same as the Allied Telesis router's secret key.



Select a security level for this tunnel.

○ Compatible (56-bit encryption strength)

● Standard (128/168-bit encryption strength)

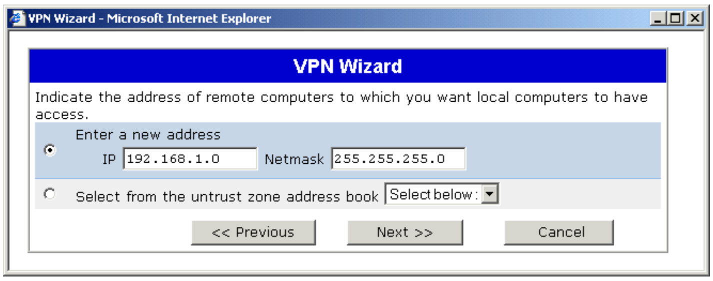
Enter a preshared secret for this tunnel.

Preshared Secret **********

Click the Next button.

5. Specify the remote LAN

Enter the IP subnet of the LAN at the Allied Telesis router's end of the tunnel. In this example, the address is 192.168.1.0 and the netmask is 255.255.255.0.



Indicate the address of remote computers to which you want local computers to have access.

● Enter a new address

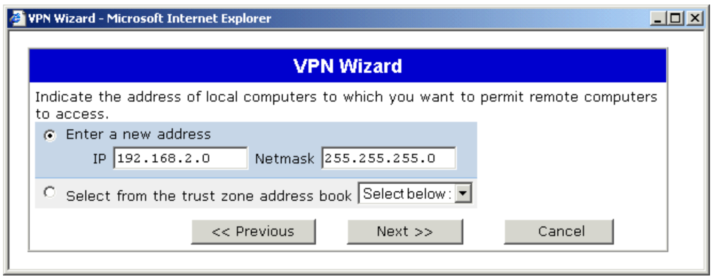
IP 192.168.1.0 Netmask 255.255.255.0

○ Select from the untrust zone address book Select below:

Click the Next button.

6. Specify the local LAN

Enter the IP subnet of the LAN at the NetScreen router's end of the tunnel. In this example, the address is 192.168.2.0 and the netmask is 255.255.255.0.



Indicate the address of local computers to which you want to permit remote computers to access.

● Enter a new address

IP 192.168.2.0 Netmask 255.255.255.0

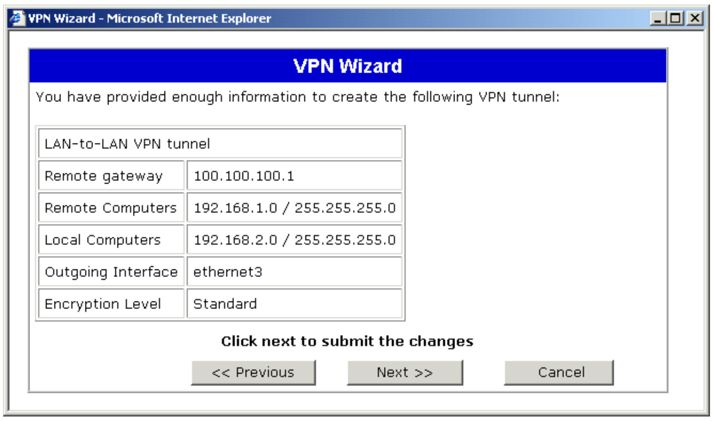
○ Select from the trust zone address book Select below :

Click the Next button.

7. Check the policy settings

The wizard displays a summary of the settings for you to confirm. Check that the settings are correct, and if necessary use the Previous button to return and correct them.

Static remote address

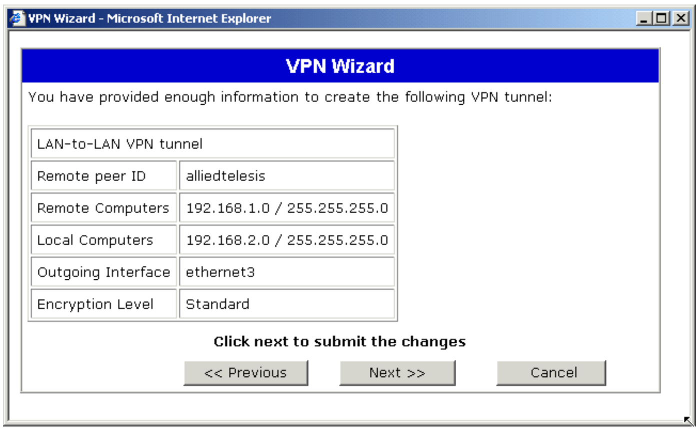


You have provided enough information to create the following VPN tunnel:

LAN-to-LAN VPN tunnel	
Remote gateway	100.100.100.1
Remote Computers	192.168.1.0 / 255.255.255.0
Local Computers	192.168.2.0 / 255.255.255.0
Outgoing Interface	ethernet3
Encryption Level	Standard

Click next to submit the changes

Dynamic remote address



You have provided enough information to create the following VPN tunnel:

LAN-to-LAN VPN tunnel	
Remote peer ID	alliedtelesis
Remote Computers	192.168.1.0 / 255.255.255.0
Local Computers	192.168.2.0 / 255.255.255.0
Outgoing Interface	ethernet3
Encryption Level	Standard

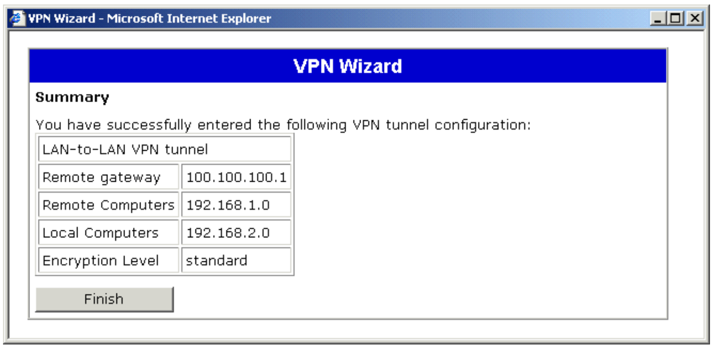
Click next to submit the changes

Once the settings are correct, click the Next button.

8. End the wizard

The wizard displays a summary of the settings.

Static remote address



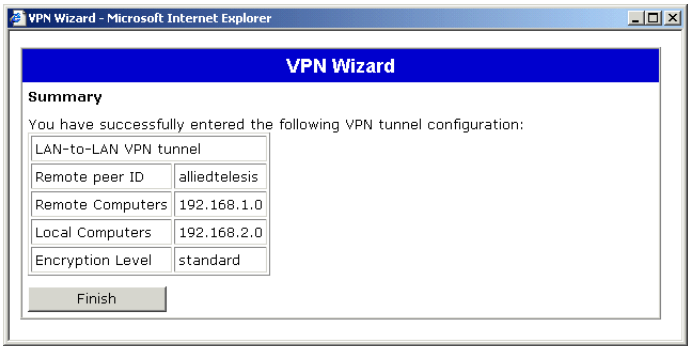
VPN Wizard

Summary

You have successfully entered the following VPN tunnel configuration:

LAN-to-LAN VPN tunnel	
Remote gateway	100.100.100.1
Remote Computers	192.168.1.0
Local Computers	192.168.2.0
Encryption Level	standard

Dynamic remote address



VPN Wizard

Summary

You have successfully entered the following VPN tunnel configuration:

LAN-to-LAN VPN tunnel	
Remote peer ID	alliedtelesis
Remote Computers	192.168.1.0
Local Computers	192.168.2.0
Encryption Level	standard

Click the Finish button. This completes the configuration.

How to test the tunnel

There are several options for testing the tunnel. If these checks show that your tunnel is not working, see the How To Note *How To Troubleshoot A Virtual Private Network (VPN)*.

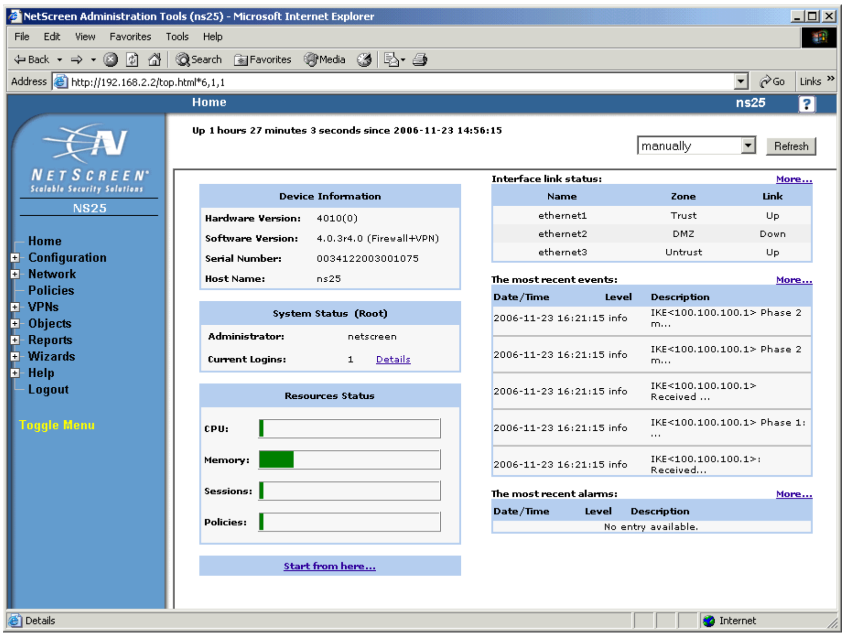
1. Ping the LAN

The simplest way to test the tunnel is to ping from one LAN to the other. For example, from the PC attached to the Allied Telesis router, ping the PC attached to the NetScreen router.

If the Allied Telesis router has a dynamic IP address, note that you must initiate the tunnel from the Allied Telesis end. This means pinging from a PC attached to the Allied Telesis router, not from a PC attached to the NetScreen router.

2. Check the events

On the Home page of the NetScreen router, you can look at the list of events while (or after) attempting to ping from one LAN to the other. You should see entries for successful Phase 1 and Phase 2 negotiations. Click on the More link to display the events in full.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
Home
ns25
NETSCREEN
Scalable Security Solutions
NS25
Home
Configuration
Network
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
manually
Refresh
Start from here...
Details
Internet

Up 1 hours 27 minutes 3 seconds since 2006-11-23 14:56:15

Device Information

Hardware Version: 4010(0)
Software Version: 4.0.3r4.0 (Firewall+VPN)
Serial Number: 0034122003001075
Host Name: ns25

System Status (Root)

Administrator: netscreen
Current Logins: 1 Details

Resources Status

CPU:
Memory:
Sessions:
Policies:

Interface link status: More...

Name	Zone	Link
ethernet1	Trust	Up
ethernet2	DMZ	Down
ethernet3	Untrust	Up

The most recent events: More...

Date/Time	Level	Description
2006-11-23 16:21:15	info	IKE<100.100.100.1> Phase 2 m...
2006-11-23 16:21:15	info	IKE<100.100.100.1> Phase 2 m...
2006-11-23 16:21:15	info	IKE<100.100.100.1> Received ...
2006-11-23 16:21:15	info	IKE<100.100.100.1> Phase 1: ...
2006-11-23 16:21:15	info	IKE<100.100.100.1>: Received...

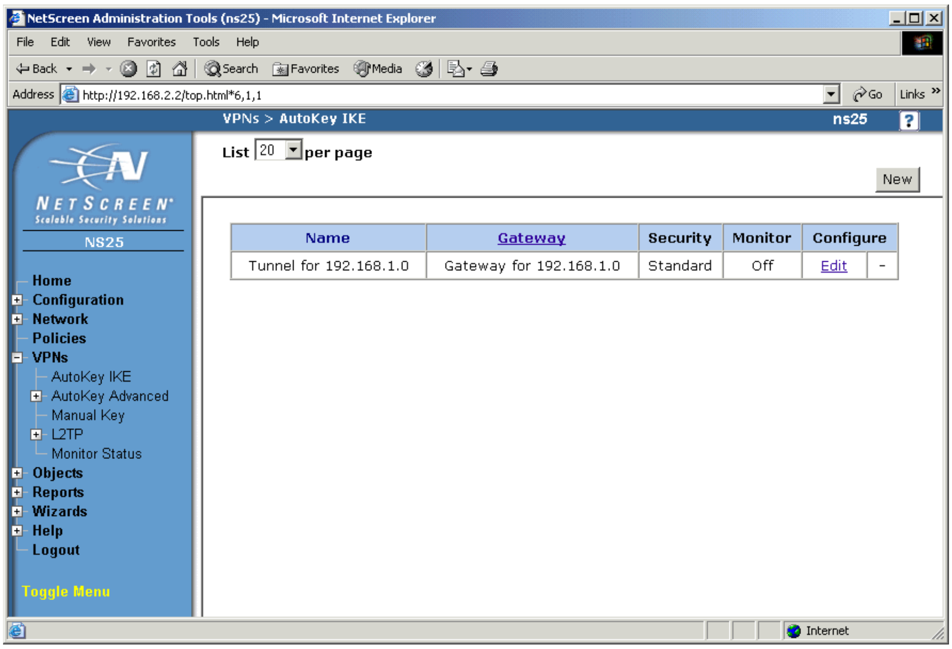
The most recent alarms: More...

Date/Time	Level	Description
No entry available.		

3. Check the tunnel settings

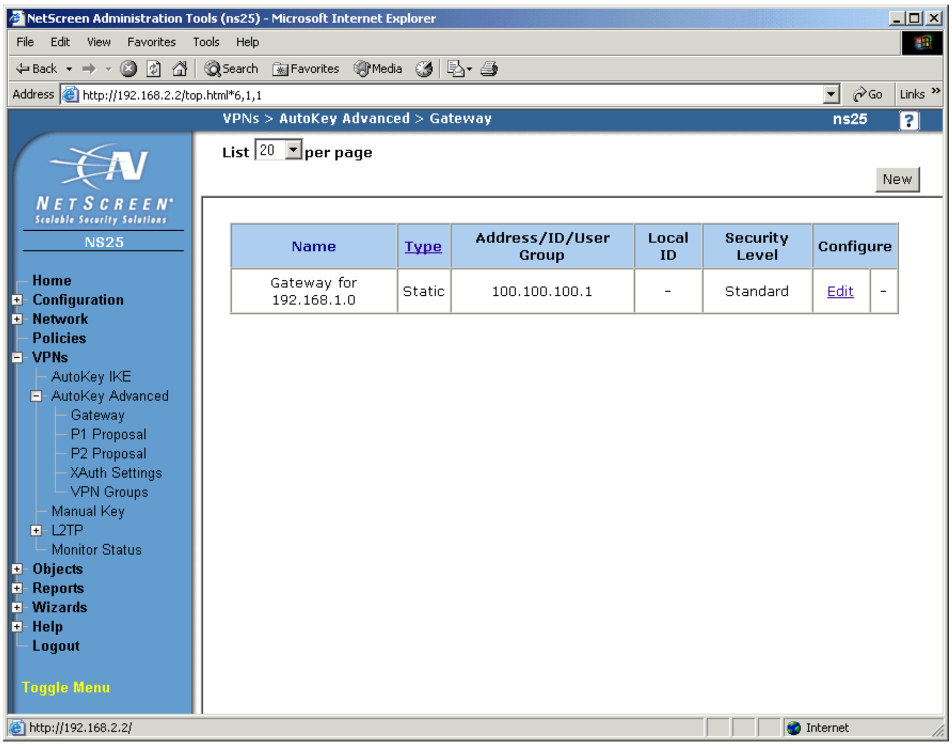
On the NetScreen router, two pages are particularly useful for checking the VPN: Autokey IKE and Autokey Advanced. To access these pages, select VPNs from the left-hand menu on the Home page, then the desired option.

Autokey IKE shows some of the tunnel settings and lets you edit it by clicking on Edit.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
VPNs > AutoKey IKE
ns25
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Network
Policies
VPNs
AutoKey IKE
AutoKey Advanced
Manual Key
L2TP
Monitor Status
Objects
Reports
Wizards
Help
Logout
Toggle Menu
List 20 per page
New
Internet

Name	Gateway	Security	Monitor	Configure	
Tunnel for 192.168.1.0	Gateway for 192.168.1.0	Standard	Off	Edit	-

Autokey Advanced shows information about the tunnel gateway and lets you edit it by clicking on Edit.



Name	Type	Address/ID/User Group	Local ID	Security Level	Configure	
Gateway for 192.168.1.0	Static	100.100.100.1	-	Standard	Edit	-

The router commands

This section lists the configuration commands that result from the GUI on each router. You can compare your router configuration against these commands to help with troubleshooting.

Allied Telesis router

To display the router configuration, log into its CLI and enter the following command:

```
show config dynamic
```

Static address on Allied Telesis router

The configuration is:

```
# System configuration
set system name="AlliedTelesis"

# User configuration
set user=manager pass=your-password priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
add user=secoff pass=your-password priv=securityOfficer lo=yes
set user=secoff telnet=no netmask=255.255.255.255

# IP configuration
enable ip
ena ip dnsrelay
add ip int=vlan1 ip=192.168.1.1
add ip int=eth0 ip=100.100.100.1 mask=255.255.255.252
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=100.100.100.2
add ip dns prim=150.150.150.1 seco=150.150.150.2

# Firewall configuration
enable firewall
create firewall policy="guilan"
enable firewall policy="guilan" icmp_f=ping
add firewall policy="guilan" int=vlan1 type=private
add firewall policy="guilan" int=eth0 type=public
add firewall poli="guilan" nat=enhanced int=vlan1 gblin=eth0
add firewall poli="guilan" ru=1 ac=allo int=eth0 prot=udp po=500
  ip=100.100.100.1 gblip=100.100.100.1 gblp=500
add firewall poli="guilan" ru=2 ac=allo int=eth0 prot=udp po=4500
  ip=100.100.100.1 gblip=100.100.100.1 gblp=4500
add firewall poli="guilan" ru=3 ac=non int=eth0 prot=ALL enc=ips
add firewall poli="guilan" ru=4 ac=non int=vlan1 prot=ALL
  ip=192.168.1.1-192.168.1.254
set firewall poli="guilan" ru=4 rem=192.168.2.1-192.168.2.254

# DHCP (Post IP) configuration
enable dhcp
create dhcp poli="lan-dhcp" lease=259200
add dhcp poli="lan-dhcp" subn=255.255.255.0
add dhcp poli="lan-dhcp" rou=192.168.1.1
add dhcp poli="lan-dhcp" dnss=192.168.1.1
create dhcp ran="standard" poli="lan-dhcp" ip=192.168.1.100 num=50
```

```
# IPSEC configuration
create ipsec sas=0 key=isakmp prot=esp enc=3desouter hasha=sha
set ipsec sas=0 antir=true
create ipsec bund=0 key=isakmp string="0" expirys=3600
create ipsec pol="eth0allowISAKMP" int=eth0 ac=permit
set ipsec pol="eth0allowISAKMP" lp=500 tra=UDP
create ipsec pol="eth0allowISAKMPF" int=eth0 ac=permit
set ipsec pol="eth0allowISAKMPF" lp=4500
create ipsec pol="wiz_AT-to-NetScreen" int=eth0 ac=ipsec key=isakmp bund=0
  peer=200.200.200.1 isa="wiz_AT-to-NetScreen"
set ipsec pol="wiz_AT-to-NetScreen" lad=192.168.1.0 lma=255.255.255.0
  rad=192.168.2.0 rma=255.255.255.0
set ipsec pol="wiz_AT-to-NetScreen" usepfsk=TRUE gro=2
create ipsec pol="eth0allow" int=eth0 ac=permit
enable ipsec

# ISAKMP configuration
create isakmp pol="wiz_AT-to-NetScreen" pe=200.200.200.1 enc=3desouter key=0
  natt=true
set isakmp pol="wiz_AT-to-NetScreen" expirys=28800 gro=2
set isakmp pol="wiz_AT-to-NetScreen" sendd=true sendn=true
enable isakmp
```

Dynamic address on Allied Telesis router

The configuration is:

```
# System configuration
set system name="AlliedTelesis"

# User configuration
set user  securedelay=600
set user=manager pass=your-password priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
add user=secoff pass=your-password priv=securityOfficer lo=yes
set user=secoff telnet=no netmask=255.255.255.255

# PPP configuration
create ppp=0 description="Link to ISP" idle=3600 over=eth0-any
set ppp=0 iprequest=on username="pppoe_user" password="alliedtelesis"

# IP configuration
enable ip
enable ip remote
ena ip dnsrelay
add ip int=vlan1 ip=192.168.1.1
add ip int=ppp0 ip=0.0.0.0 mask=0.0.0.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

# Firewall configuration
enable firewall
create firewall policy="guilan"
enable firewall policy="guilan" icmp_f=ping
add firewall policy="guilan" int=vlan1 type=private
add firewall policy="guilan" int=ppp0 type=public
add firewall poli="guilan" nat=enhanced int=vlan1 gblin=ppp0
add firewall poli="guilan" ru=1 ac=allo int=ppp0 prot=udp po=500
  ip=100.100.100.1 gblip=100.100.100.1 gblp=500
add firewall poli="guilan" ru=2 ac=allo int=ppp0 prot=udp po=4500
  ip=100.100.100.1 gblip=100.100.100.1 gblp=4500
add firewall poli="guilan" ru=3 ac=non int=ppp0 prot=ALL enc=ips
add firewall poli="guilan" ru=4 ac=non int=vlan1 prot=ALL
  ip=192.168.1.1-192.168.1.254
set firewall poli="guilan" ru=4 rem=192.168.2.1-192.168.2.254
```

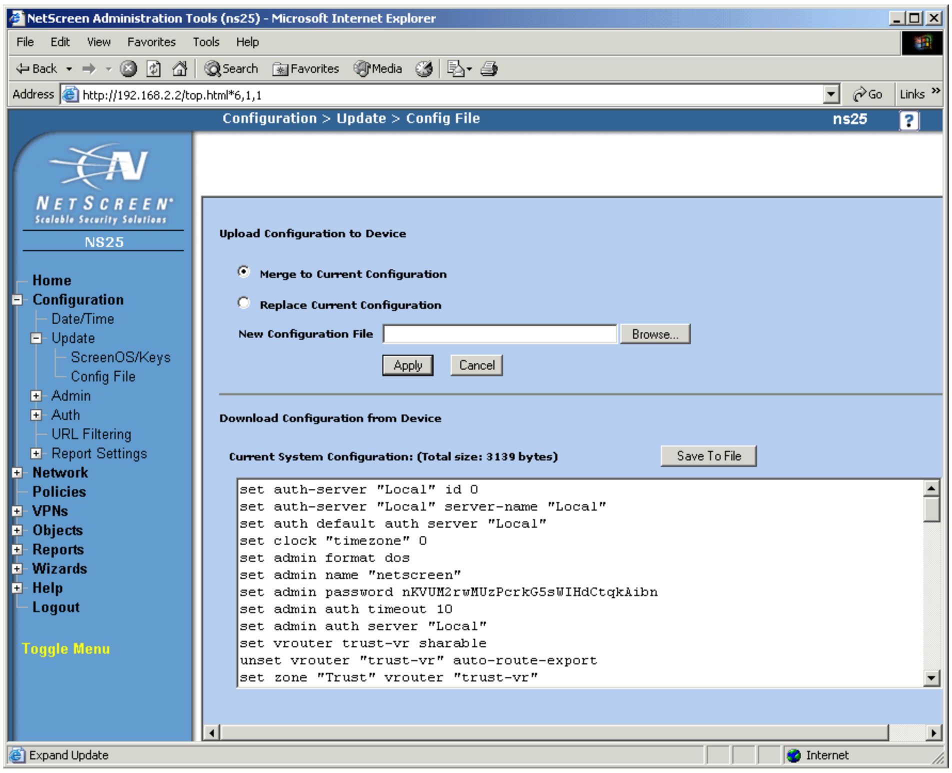
```
# DHCP (Post IP) configuration
enable dhcp
create dhcp poli="lan-dhcp" lease=259200
add dhcp poli="lan-dhcp" subn=255.255.255.0
add dhcp poli="lan-dhcp" rou=192.168.1.1
add dhcp poli="lan-dhcp" dnss=192.168.1.1
create dhcp ran="standard" poli="lan-dhcp" ip=192.168.1.100 num=50

# IPSEC configuration
create ipsec sas=0 key=isakmp prot=esp enc=3desouter hasha=sha
set ipsec sas=0 antir=true
create ipsec bund=0 key=isakmp string="0" expirys=3600
create ipsec pol="ppp0allowISAKMP" int=ppp0 ac=permit
set ipsec pol="ppp0allowISAKMP" lp=500 tra=UDP
create ipsec pol="ppp0allowISAKMPF" int=ppp0 ac=permit
set ipsec pol="ppp0allowISAKMPF" lp=4500
create ipsec pol="wiz_AT-to-NetScreen" int=ppp0 ac=ipsec key=isakmp bund=0
  peer=200.200.200.1 isa="wiz_AT-to-NetScreen"
set ipsec pol="wiz_AT-to-NetScreen" lad=192.168.1.0 lma=255.255.255.0
  rad=192.168.2.0 rma=255.255.255.0
set ipsec pol="wiz_AT-to-NetScreen" usepfsk=TRUE gro=2
create ipsec pol="ppp0allow" int=ppp0 ac=permit
enable ipsec

# ISAKMP configuration
create isakmp pol="wiz_AT-to-NetScreen" pe=200.200.200.1 mod=aggressive
  enc=3des
outer key=1 natt=true
set isakmp pol="wiz_AT-to-NetScreen" expirys=28800 gro=2
set isakmp pol="wiz_AT-to-NetScreen" sendd=true sendn=true
set isakmp pol="wiz_AT-to-NetScreen" localid="alliedtelesis"
enable isakmp
```

NetScreen router

To display the router configuration, in the left-hand menu select Configuration, then Update, then Config File. Use the Save to File option to save the configuration.


NetScreen Administration Tools (ns25) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.2/top.html*6,1,1
Go Links
Configuration > Update > Config File
ns25
NETSCREEN Scalable Security Solutions
NS25
Home
Configuration
Date/Time
Update
ScreenOS/Keys
Config File
Admin
Auth
URL Filtering
Report Settings
Network
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Expand Update
Internet

Upload Configuration to Device

● Merge to Current Configuration

○ Replace Current Configuration

New Configuration File ______ Browse...

Apply Cancel

Download Configuration from Device

Current System Configuration: (Total size: 3139 bytes) Save To File

```
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set clock "timezone" 0
set admin format dos
set admin name "netscreen"
set admin password nKVUM2rwMUzPcrkG5sWIHdCtqkAibn
set admin auth timeout 10
set admin auth server "Local"
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set zone "Trust" vrouter "trust-vr"
```

Static address on NetScreen router

The configuration is:

```
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set clock "timezone" 0
set admin format dos
set admin name "netscreen"
set admin password nKVUM2rwMUzPcrkG5sWIHdCtqkAibn
set admin auth timeout 10
set admin auth server "Local"
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "DMZ" tcp-rst
set zone "MGT" block
set zone "MGT" tcp-rst
set zone Untrust screen tear-drop
set zone Untrust screen syn-flood
set zone Untrust screen ping-death
set zone Untrust screen ip-filter-src
set zone Untrust screen land
set zone V1-Untrust screen tear-drop
set zone V1-Untrust screen syn-flood
set zone V1-Untrust screen ping-death
set zone V1-Untrust screen ip-filter-src
set zone V1-Untrust screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface vlan1 ip 192.168.1.1/24
set interface ethernet1 ip 192.168.2.1/24
set interface ethernet1 nat
set interface ethernet3 ip 200.200.200.1/30
set interface ethernet3 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 manage-ip 192.168.2.2
set interface vlan1 ip manageable
unset interface ethernet1 ip manageable
set interface ethernet2 ip manageable
set interface ethernet3 ip manageable
set hostname ns25
set address "Trust" "192.168.2.0" 192.168.2.0 255.255.255.0
  "Created by vpn wizard"
set address "Untrust" "192.168.1.0" 192.168.1.0 255.255.255.0
  "Created by vpn wizard"
set snmp name "ns25"
set ike gateway "Gateway for 192.168.1.0" address 100.100.100.1 Main
  outgoing-interface "ethernet3" preshare "secret-key" sec-level standard
set ike gateway  "Gateway for 192.168.1.0" nat-traversal
set ike gateway "Gateway for 192.168.1.0" nat-traversal udp-checksum
set ike gateway "Gateway for 192.168.1.0" nat-traversal keepalive-frequency 5
set ike policy-checking
set ike respond-bad-spi 1
set vpn "Tunnel for 192.168.1.0" id 1 gateway "Gateway for 192.168.1.0"
  no-replay tunnel idletime 0 sec-level standard
set ike id-mode subnet
set xauth lifetime 480
set xauth default auth server Local
set policy id 2 from "Trust" to "Untrust"  "192.168.2.0" "192.168.1.0" "ANY"
  Tunnel vpn "Tunnel for 192.168.1.0" id 2 pair-policy 1
set policy id 1 from "Untrust" to "Trust"  "192.168.1.0" "192.168.2.0" "ANY"
  Tunnel vpn "Tunnel for 192.168.1.0" id 2 pair-policy 2
set policy id 0 name "Created by policy wizard" from "Trust" to "Untrust"  "Any"
  "Any" "ANY" Permit
unset global-pro policy-manager primary outgoing-interface
unset global-pro policy-manager secondary outgoing-interface
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route  0.0.0.0/0 interface ethernet3 gateway 200.200.200.2
exit
```

Dynamic address on NetScreen router

The configuration is:

```
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set clock "timezone" 0
set admin format dos
set admin name "netscreen"
set admin password nKVUM2rwMUzPcrkG5sWIHdCtqkAibn
set admin auth timeout 10
set admin auth server "Local"
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "DMZ" tcp-rst
set zone "MGT" block
set zone "MGT" tcp-rst
set zone Untrust screen tear-drop
set zone Untrust screen syn-flood
set zone Untrust screen ping-death
set zone Untrust screen ip-filter-src
set zone Untrust screen land
set zone V1-Untrust screen tear-drop
set zone V1-Untrust screen syn-flood
set zone V1-Untrust screen ping-death
set zone V1-Untrust screen ip-filter-src
set zone V1-Untrust screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface vlan1 ip 192.168.1.1/24
set interface ethernet1 ip 192.168.2.1/24
set interface ethernet1 nat
set interface ethernet3 ip 200.200.200.1/30
set interface ethernet3 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 manage-ip 192.168.2.2
set interface vlan1 ip manageable
unset interface ethernet1 ip manageable
set interface ethernet2 ip manageable
set interface ethernet3 ip manageable
set hostname ns25
set address "Trust" "192.168.2.0" 192.168.2.0 255.255.255.0
  "Created by vpn wizard"
set address "Untrust" "192.168.1.0" 192.168.1.0 255.255.255.0
  "Created by vpn wizard"
set snmp name "ns25"
set ike gateway "Gateway for 192.168.1.0" address 0.0.0.0 id "alliedtelesis"
  Aggr outgoing-interface "ethernet3" preshare "secret-key" sec-level standard
set ike gateway "Gateway for 192.168.1.0" nat-traversal udp-checksum
set ike gateway "Gateway for 192.168.1.0" nat-traversal keepalive-frequency 5
set ike policy-checking
set ike respond-bad-spi 1
set vpn "Tunnel for 192.168.1.0" id 1 gateway "Gateway for 192.168.1.0" no-
  replay tunnel idletime 0 sec-level standard
set ike id-mode subnet
set xauth lifetime 480
set xauth default auth server Local
set policy id 2 from "Trust" to "Untrust"  "192.168.2.0" "192.168.1.0" "ANY"
  Tunnel vpn "Tunnel for 192.168.1.0" id 2 pair-policy 1
set policy id 1 from "Untrust" to "Trust"  "192.168.1.0" "192.168.2.0" "ANY"
  Tunnel vpn "Tunnel for 192.168.1.0" id 2 pair-policy 2
set policy id 0 name "Created by policy wizard" from "Trust" to "Untrust"  "Any"
  "Any" "ANY" Permit
unset global-pro policy-manager primary outgoing-interface
unset global-pro policy-manager secondary outgoing-interface
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route  0.0.0.0/0 interface ethernet3 gateway 200.200.200.2
exit
```