

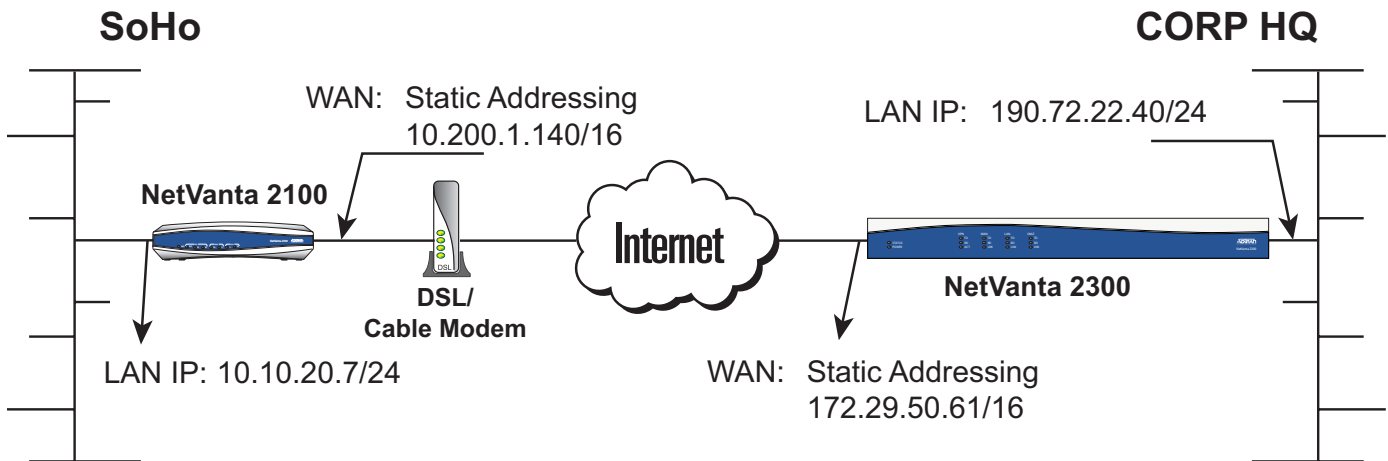
About this guide...

Before you begin...

■ Tools Required

- Category 5 - UTP cable for connecting the system to the existing network
- A PC with an internet browser (IE 5.0 or greater) for configuring the unit

Network Diagram

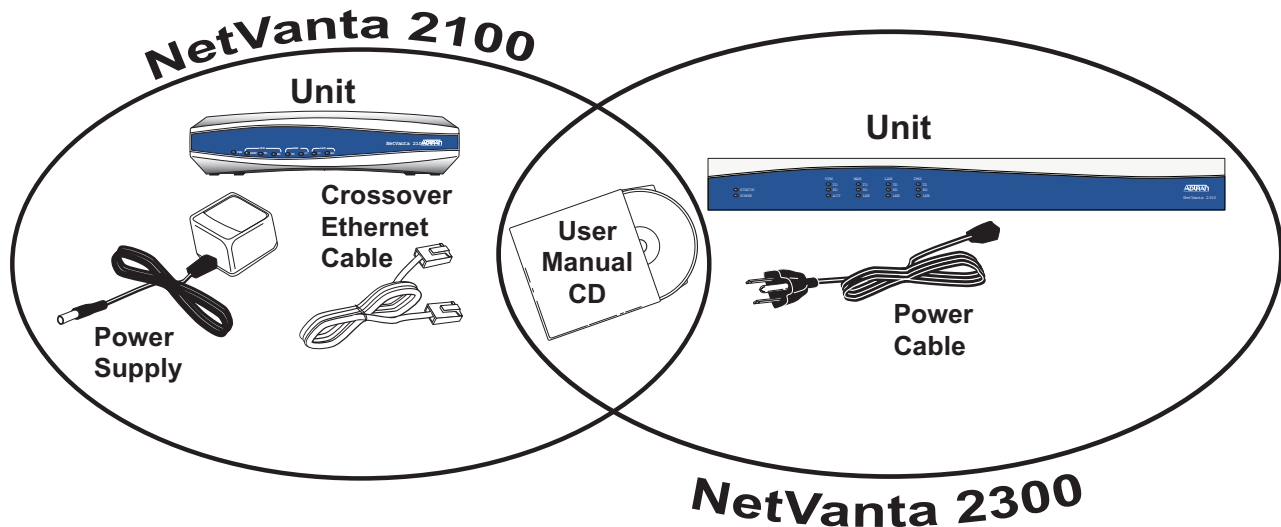


STEPS 2-2f — Provide the stateful inspection firewall configuration.

STEPS 2g-3 — Configures a VPN connection between the NetVanta 2100 at the Corporate office (for the the above network diagram).

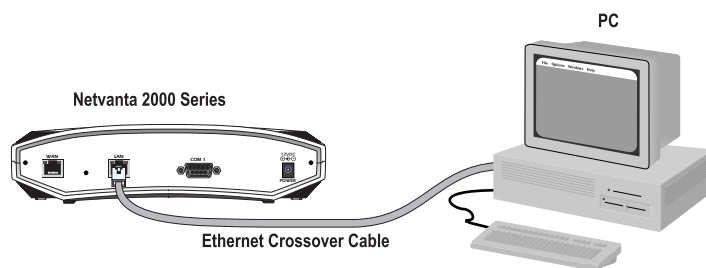
1 Unpacking and Inspecting the System

Each NetVanta 2000 series unit is shipped in its own cardboard shipping carton. Open each carton carefully and avoid deep penetration into the carton with sharp objects.

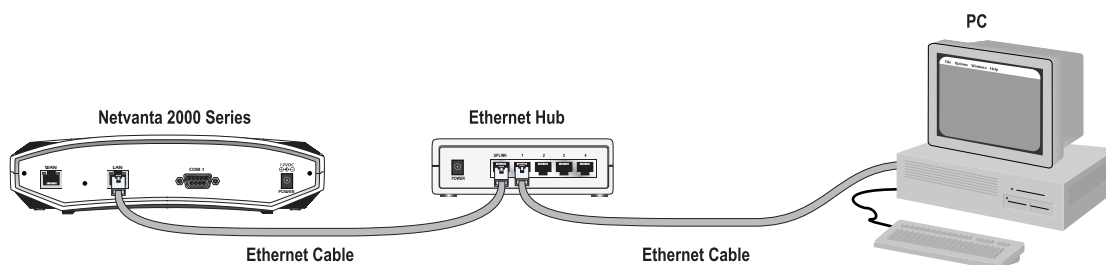


Configuring the System

The NetVanta 2000 series products can be accessed and managed via the LAN interface using an ethernet crossover cable (provided with the NetVanta 2100). Alternately, the NetVanta 2000 series may be accessed using a hub and two ethernet cables (one for the PC and one for the NetVanta). Using a PC with an installed browser (Internet Explorer 5.0 for optimal viewing), the NetVanta can be configured using the web GUI.



Direct Connection to PC



Connection through Hub

2 Connecting to the NetVanta

1. Connect the NetVanta 2000 series LAN interface to the PC using the appropriate ethernet cable.
2. Supply power to the PC and the NetVanta unit and begin the operating system boot up process. During the boot up process, the PC will obtain an IP address from the NetVanta 2000 series DHCP server. Alternately, complete the process for releasing and renewing captured IP addresses to obtain a new IP address from the NetVanta 2000 series DHCP server. Please refer to your specific PC operating system documentation for details on that process.
3. Open your installed browser and in the URL field enter 10.10.10.1. The NetVanta 2000 series login screen will appear.
4. Enter your username and password and click the login button. When connecting to the NetVanta 2000 series for the first time, the username is **admin** and there is no set password.

NOTE

*ADTRAN strongly recommends immediately changing the **admin** password for security purposes. Refer to DLP-002 in the NetVanta 2000 series System Manual (PN 61200361L1-1) for details.*

5. After logging in to the NetVanta 2000 series, the welcome screen will appear.

3

Configuring the LAN and WAN IP Parameters

The NetVanta 2000 series units come factory programmed with a LAN IP address of 10.10.10.1 (24-bit subnet mask) and no pre-programmed WAN IP address. The procedures outlined in this step include changing both the LAN and WAN IP parameters.

The NetVanta 2000 series supports three types of WAN IP address: Dynamic, Static, and PPPoE (PPP over Ethernet). The IP parameters for your WAN interface must be supplied by your Internet Service Provider (ISP). If your ISP is performing DHCP for IP address assignment, configure the NetVanta 2000 series unit for Dynamic addressing. Use PPP over Ethernet when your ISP has supplied you with the configuration parameters for PPPoE (including a username and password).



Changing the LAN IP parameters through the LAN interface will result in a loss of management connectivity. Follow the procedure in Step 2c to change the IP address of the managing PC to match the new NetVanta LAN IP parameters.

The screenshot shows the NetVanta configuration interface. The top navigation bar includes 'CONFIG', 'ADMIN', 'POLICIES', 'MONITOR', and 'LOGOUT'. The left sidebar menu has 'General', 'Network Interface', 'RIP config', 'DHCP Info', 'Routes', 'Firewall', 'Logging', 'DHCP server', 'DNS server', and 'Advanced'. The main content area is titled 'Ethernet IP Address' and contains the following fields and options:

- LAN IP: 10 . 10 . 20 . 7
- Subnet Mask: 255 . 255 . 255 . 0
- WAN IP TYPE: Dynamic Static PPP over Ethernet
- WAN IP: 10 . 200 . 1 . 140
- Subnet Mask: 255 . 255 . 0 . 0
- PPP over Ethernet section with fields for Username (required), Password, Password Confirmation, Service Name, and AC Name.
- Buttons for 'Submit' and 'Reset'.

1. Select Config
2. Select Network Interface
3. Enter the Assigned LAN IP address and associated subnet mask
4. Select the Static radio button for static addressing



Your WAN IP address scheme will be supplied by your provider. Static addressing used above is an example only.

5. Enter the assigned WAN IP address and associated subnet mask

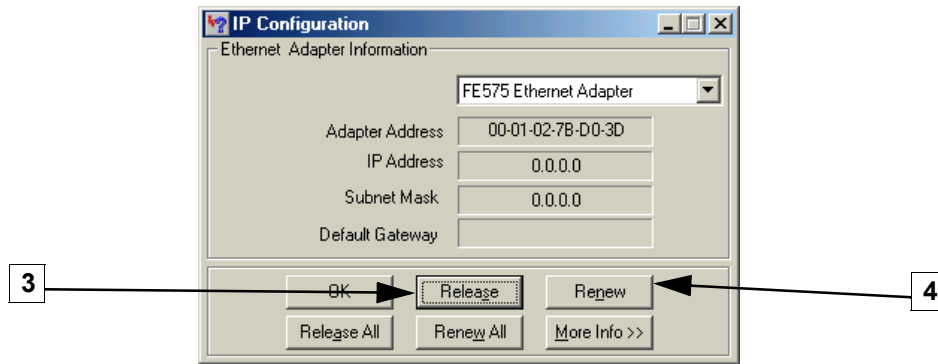


The WAN IP parameters are set by the service provider. Contact your ISP before configuring the unit.

6. Click Submit to register the changes

3b Changing the IP address to your PC

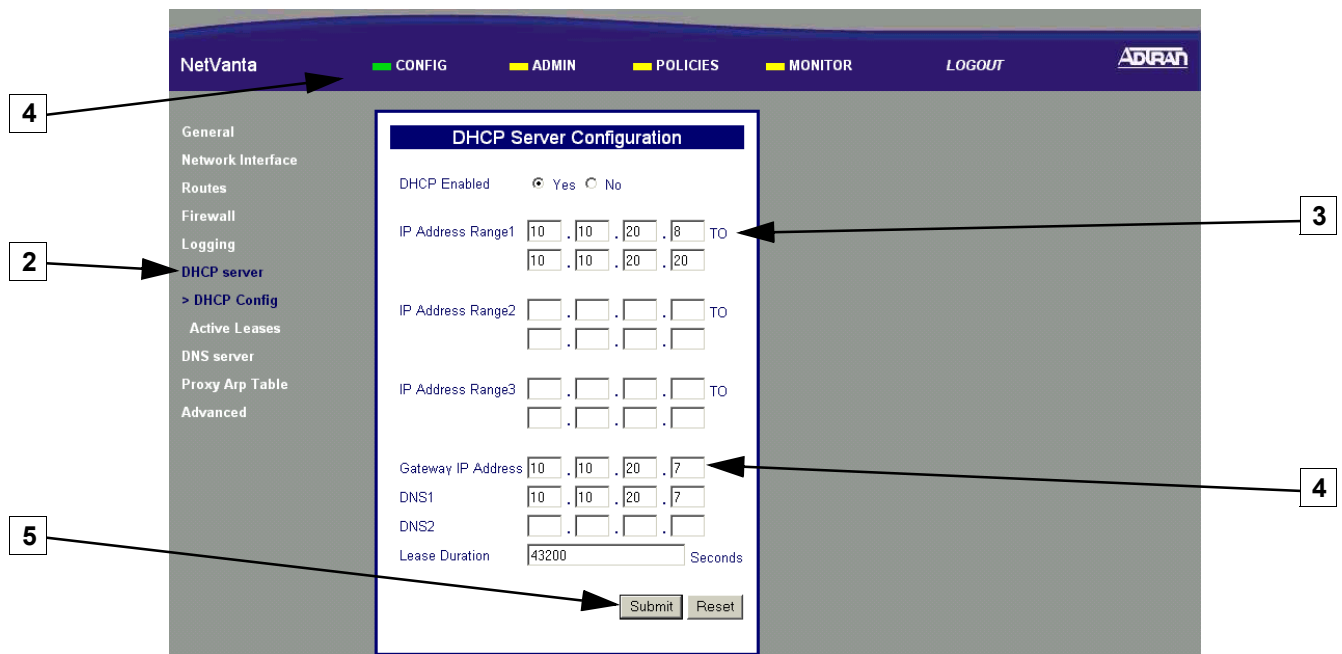
Alternately, complete the process for releasing and renewing captured IP addresses to obtain a new IP address from the NetVanta 2000 series DHCP server. The following screen applies to Microsoft Windows 95 to 2000. Please refer to your specific operating system documentation for details on that process.



1. Click Start on the Windows task bar
2. Choose Run, then type WINIPCFG in the text field
3. Click Release to reset all IP parameters
4. Click Renew to obtain new IP parameters

3c Configuring the DHCP Server IP Parameters - Optional

The NetVanta 2000 series will automatically populate the DHCP IP address range 1 with ten addresses based on your assigned LAN network address.



1. Select CONFIG
2. Select DHCP Server
3. Enter an IP address range that is on the same subnet as the assigned LAN IP address of the unit
4. Enter the assigned LAN IP address of the unit
5. Click Submit to register the changes

2e Adding a Default Route

Skip this step when configuring the NetVanta for dynamic addressing on the WAN interface.

Select	DestinationIP	InterfaceName	NetMask	Gateway IP	HOP Count	Type
<input type="checkbox"/>	255.255.255.255	LAN	255.255.255.255	0.0.0.0	0	LOCAL
<input type="checkbox"/>	10.200.1.139	lo	255.255.255.255	0.0.0.0	0	LOCAL
<input type="checkbox"/>	10.10.10.0	LAN	255.255.255.0	0.0.0.0	0	LOCAL
<input type="checkbox"/>	10.200.0.0	WAN	255.255.0.0	0.0.0.0	0	LOCAL
<input type="checkbox"/>	0.0.0.0	WAN	0.0.0.0	10.200.254.254	0	LOCAL

1. Select CONFIG
2. Select Routes
3. Select AddRoute

Interface Name: WAN
Default Route: Yes No
Destination IP Address: 0 . 0 . 0 . 0
Net Mask: 0 . 0 . 0 . 0
Gateway IP Address: 180 . 25 . 64 . 200
Hop Count:

1. Select WAN to associate this default route with the WAN interface
2. Select Yes to configure this as the default
3. Enter all zeros
4. Enter the next hop IP address

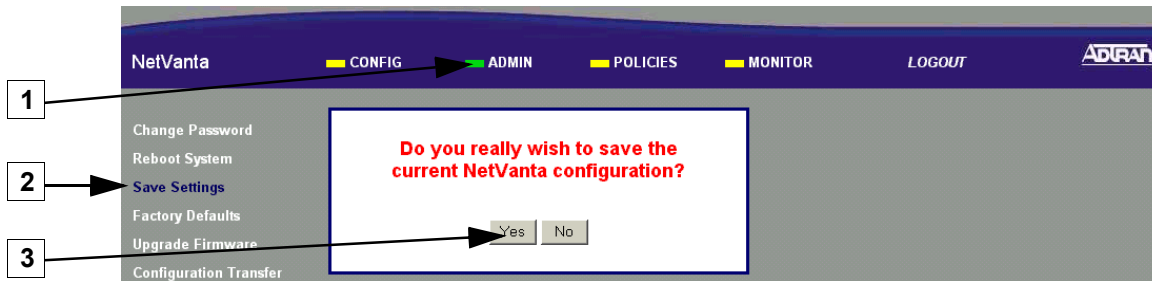
NOTE This is supplied by your provider

5. Click Add Route to submit this route to the route table



The NetVanta is now configured for use as a Stateful inspection firewall. To configure VPN, please proceed to **Step 2f**. If VPN is not desired, proceed to **Step 3**.

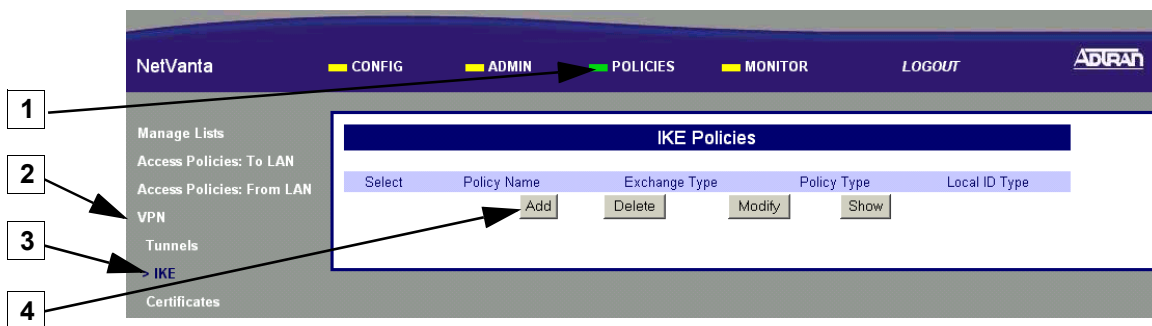
2f Saving the Settings



1. Select ADMIN
2. Select Save Settings
3. Select Yes to Confirm

2g Defining a VPN Policy

■ IKE Policy Configuration



1. Select POLICIES
2. Select VPN
3. Select IKE
4. Click the Add button

■ IKE Policy Configuration (continued)

The screenshot shows the NetVanta IKE Policy Configuration interface. The interface is divided into several sections: Manage Lists, Access Policies, VPN, Tunnels, IKE, and Certificates. The main configuration area is titled 'IKE Policy Configuration' and contains the following fields and options:

- Policy Name:** MyIKEPolicy1
- Direction:** BOTH DIRECTIONS
- Exchange Type:** MAINMODE
- Local ID Type:** FQDN
- Local ID Data:** unit1.domain.com
- Remote ID Type:** FQDN
- Remote ID Data:** unit2.domain.com
- Local IP Address:** 10.200.1.140 - OR -
- Remote IP Address:** 172.29.50.61
- Encrypt Algo:** 3DES
- Auth Algo:** SHA
- Auth mode:** Pre-SharedKey
- If Auth mode is Pre-Shared Key enter the key:** *my567key#0!
- Life time of key:** 1800
- DH Group:** Group 2
- Buttons:** SUBMIT, RESET

Numbered callouts (1-13) point to the following fields:

- 1: Policy Name
- 2: Direction
- 3: Exchange Type
- 4: Local ID Type
- 5: Remote ID Type
- 6: Local IP Address
- 7: Remote IP Address
- 8: Encrypt Algo
- 9: Auth Algo
- 10: Auth mode
- 11: Life time of key
- 13: SUBMIT button

1. Enter an alphanumeric string (spaces are not valid characters) used to identify this policy
2. Select BOTH DIRECTIONS to allow IKE to be initiated by either the local or remote NetVanta
3. Select MAINMODE exchange type
4. Use the Fully Qualified Domain Name (FQDN) for the local NetVanta unit and enter the identification data
5. Use the FQDN for the remote users and enter the identification data
6. Enter the local NetVanta unit's assigned WAN IP address
7. Enter the remote NetVanta unit's assigned WAN IP address
8. Select 3DES to invoke Triple DES encryption
9. Select SHA to use the Secure Hash authentication Algorithm No. 1
10. Select Pre-SharedKey and enter a 12 character alphanumeric string (spaces are not a valid character)



This key MUST be the same for both the local and remote units.

11. 1800 is the ADTRAN suggested value



When determining the appropriate value for your application, typical usage contains a 3:1 ratio between the IKE and IPsec key lifetime values. This ratio provides for key negotiation overhead.

12. Select Group 2 to invoke Diffie-Hellman Group 2
13. Click SUBMIT to register the changes

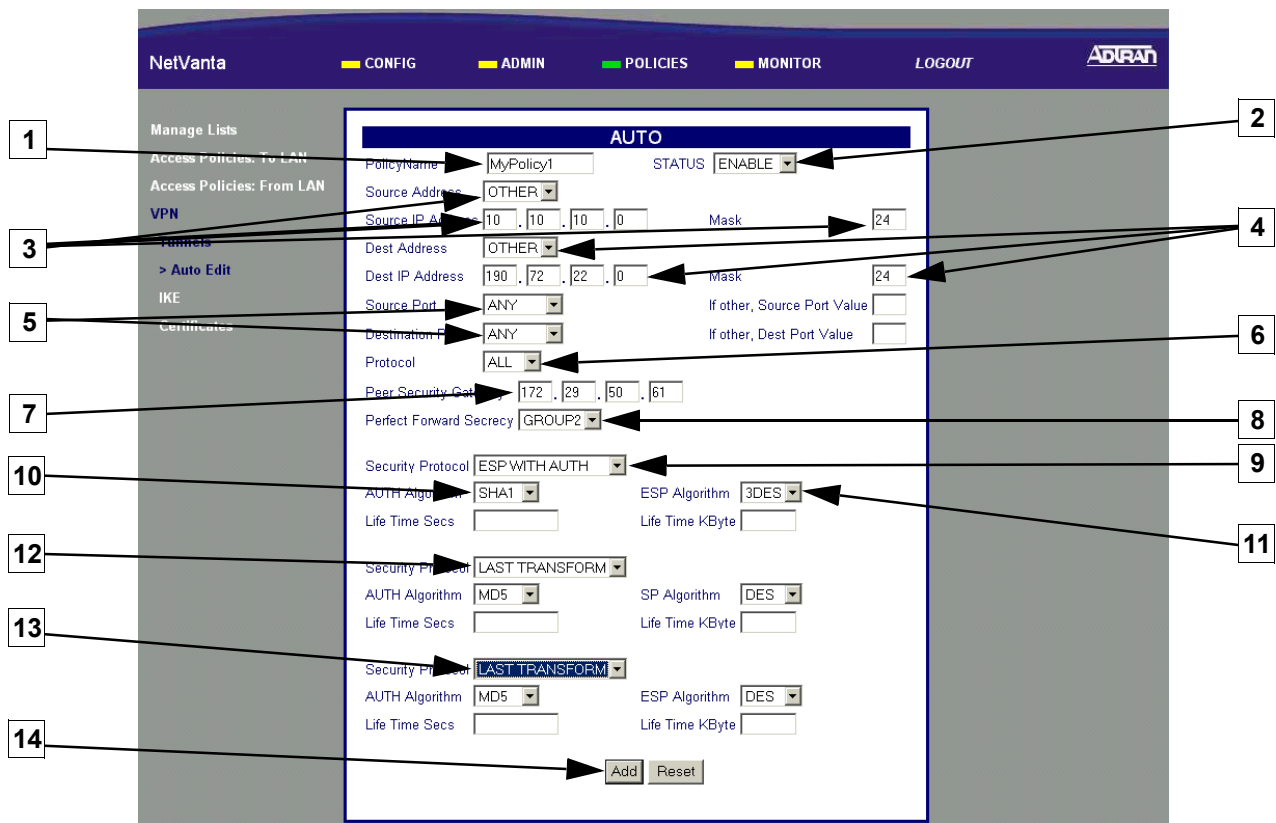
■ IPsec Policy Configuration

The screenshot shows the NetVanta web interface for IPsec Policy Configuration. The top navigation bar includes 'NetVanta', 'CONFIG', 'ADMIN', 'POLICIES', 'MONITOR', 'LOGOUT', and the ADIRAN logo. The left sidebar contains 'Manage Lists', 'Access Policies: To LAN', 'Access Policies: From LAN', 'VPN', '> Tunnels', 'IKE', and 'Certificates'. The main content area is titled 'IPsec Policies' and contains a table with the following data:

Select	Policy Name	Source	Destination	Source Port	Dest Port	Status	Info	Tunnel State	Up	Down
<input type="radio"/>	manual	10.1.1.0	10.1.3.0	ANY	ANY	ENABLED		DOWN	<input type="button" value="↑"/>	<input type="button" value="↓"/>

Below the table are buttons for 'show', 'modify', 'delete', and 'clear'. At the bottom, there are 'Add' and 'Place' sections, each with a dropdown menu set to 'AFTER' and an input field. Below these are 'manual' and 'auto' buttons, with an 'OK' button to the right. Three numbered callouts are present: '1' points to the 'POLICIES' tab, '2' points to the 'VPN' link in the sidebar, and '3' points to the 'auto' button.

1. Select POLICIES
2. Select VPN
3. Click the Auto button



1. Enter an alphanumeric string (spaces are not valid characters) to identify this policy
2. Select ENABLE to configure this as an active policy
3. Select OTHER and enter the local NetVanta unit's assigned LAN IP address and associated subnet mask here
4. Select OTHER and enter the remote NetVanta unit's assigned LAN IP address and associated subnet mask here
5. Select ANY to apply this policy to all data ports
6. Select ALL to apply this policy to all data protocols
7. Enter the remote NetVanta unit's assigned WAN IP address

NOTE *If the remote NetVanta unit is configured for dynamic addressing on the WAN interface, enter 0.0.0.0 here.*

8. Select Group2
9. Select ESP WITH AUTH
10. Select SHA1 to invoke Secure Hash Algorithm No. 1
11. Select 3DES to use Triple-DES encryption algorithm
12. 600 is the ADTRAN suggested value

NOTE *When determining the appropriate value for your application, typical usage contains a 3:1 ratio between the IKE and IPsec key lifetime values. This ratio provides minimal key negotiation overhead.*

13. Select LAST TRANSFORM
14. Click the Add button to register this policy

■ To LAN Access Policy Configuration (Inbound Traffic)

The screenshot shows the NetVanta web interface. The navigation bar at the top includes 'NetVanta', 'CONFIG', 'ADMIN', 'POLICIES' (highlighted), 'MONITOR', and 'LOGOUT'. The sidebar on the left has 'Manage Lists', 'Access Policies: To LAN' (highlighted), 'Access Policies: From LAN', and 'VPN'. The main content area is titled 'To LAN' and contains a table with columns: 'Application Diagrams', 'RuleID', 'Source', 'Destination', 'Service', 'Action', 'Up', and 'Down'. Below the table are buttons for 'Delete', 'Edit', 'Log', 'Show', and 'Clear'. At the bottom, there is an 'Add' dropdown menu with options 'Beginning', 'After', 'Before', and 'End'. The 'Beginning' option is selected. To the right of the dropdown are input fields for 'Rule ID' and 'Place Rule ID', and 'Submit' buttons.

1. Select POLICIES
2. Select Access Policies: To LAN (Incoming traffic)
3. Select Beginning to place the new access policy at the beginning of the table
4. Click Submit to begin the policy configuration

■ To LAN Access Policy Configuration (continued)

The screenshot shows the 'Internet Access Policy Configuration' page in the NetVanta interface. The page is titled 'Internet Access Policy Configuration' and has a 'RULE ID' of 11 and a 'Policy Class' of LAN_INBOUND. The configuration is divided into several sections:

- Source IP (WAN network address):** Set to OTHER. Below it, 'IP if Source IP is OTHER' is set to 190.72.22.0 with a 'Mask Bits' of 24.
- Destination IP (LAN network address):** Set to OTHER. Below it, 'IP if Dest IP is OTHER' is set to 10.10.10.0 with a 'Mask Bits' of 24.
- Destination Port:** Set to ANY. Below it, 'Port Range if Dest Port is OTHER' is empty.
- Protocol Type:** Set to ALL. Below it, 'If Protocol is OTHER enter Protocol value' is empty.
- Action Type:** Set to PERMIT.
- Time Schedule Used:** Set to (empty).
- Enable Log:** Radio buttons for Yes and No, with No selected.
- Enable NAT:** Radio buttons for Yes and No, with No selected.
- NAT to specific policy:** (empty dropdown)
- OR an IP Address (if OTHER):** (empty IP address field)
- OR Dynamic Interface:** (empty dropdown)

Below the main configuration is the 'Application Control Configuration' section:

- Web Control:** (empty dropdown)
- FTP Control:** (empty dropdown)
- SMTP Control:** (empty dropdown)
- RPC Control:** (empty dropdown)
- Security:** Radio buttons for Yes and No, with Yes selected.

At the bottom are 'Submit' and 'Reset' buttons. Numbered callouts 1 through 9 point to the following fields:

- Source IP dropdown (OTHER)
- IP if Source IP is OTHER (190.72.22.0)
- Destination IP dropdown (OTHER)
- IP if Dest IP is OTHER (10.10.10.0)
- Protocol Type dropdown (ALL)
- Enable Log radio buttons (No selected)
- Enable NAT radio buttons (No selected)
- Security radio buttons (Yes selected)
- Submit button

1. Select OTHER and enter the remote unit's assigned LAN IP address and associated mask bits here
2. Select OTHER and enter the local NetVanta unit's assigned LAN IP address and associated
3. Select ANY to forward all TCP/UDP ports or select OTHER and enter the port (or port range) below
4. Select ALL to forward all data protocols or select OTHER and enter the protocol value (using decimal notation) in the field below
5. Select PERMIT to configure this policy to permit only the specified data
6. Set Enable Log to No
7. Select No
8. Select Yes to configure the NetVanta to perform security check when the policy is submitted



The security check ensures that all inbound data covered by this access policy has an associated VPN policy as well

9. Click Submit to register this policy

■ From LAN Access Policy Configuration (Outbound Traffic)

NetVanta CONFIG ADMIN **POLICIES** MONITOR LOGOUT ADIRAN

Manage Lists
Access Policies: To LAN
Access Policies: From LAN
VPN

From LAN

Application Diagrams: To LAN From LAN To DMZ (2300 only) From DMZ (2300 only)

Select	RuleID	Source	Destination	Service	Action	Up	Down
<input type="radio"/>	1	ALL	ALL	ALL	PERMIT		

Delete Edit Log Show Clear

Add Rule ID Place Rule ID Before After

Beginning
After
Before
End

1. Select POLICIES
2. Select Access Policies: From LAN
3. Select Beginning to place the new access policy at the beginning of the table
4. Click Submit to begin the policy configuration

■ **From LAN Access Policy Configuration (continued)**

The screenshot shows the 'Internet Access Policy Configuration' page in the NetVanta interface. The page is divided into two main sections: 'Internet Access Policy Configuration' and 'Application Control Configuration'. The 'Internet Access Policy Configuration' section includes fields for Rule ID (12), Policy Class (LAN_OUTBOUND), Source IP (LAN network address) set to OTHER with IP 10.10.10.0 and Mask Bits 24, Destination IP (DMZ or WAN network address) set to OTHER with IP 190.72.22.0 and Mask Bits 24, Destination Port set to ANY, Protocol Type set to ALL, Action Type set to PERMIT, and various checkboxes for logging, NAT, and security. The 'Application Control Configuration' section includes dropdown menus for Web Control, FTP Control, SMTP Control, and RPC Control, and a Security checkbox set to Yes. At the bottom are 'Submit' and 'Reset' buttons. Numbered callouts 1 through 9 point to specific fields: 1 points to the Source IP dropdown, 2 to the Destination IP dropdown, 3 to the Destination Port dropdown, 4 to the Protocol Type dropdown, 5 to the Action Type dropdown, 6 to the 'Enable Log' radio button, 7 to the 'Enable NAT' radio button, 8 to the 'Security' radio button, and 9 to the 'Submit' button.

1. Select OTHER and enter the local NetVanta unit's assigned LAN IP address and associated mask bits here
2. Select OTHER and enter the remote NetVanta unit's assigned LAN IP address and associated mask bits here
3. Select ANY to forward all TCP/UDP ports or select OTHER and enter the port (or port range) below
4. Select ALL to forward all data protocols or select OTHER and enter the protocol value (using decimal notation) in the field below
5. Select PERMIT to configure this policy to permit only the specified data
6. Select No
7. Select No
8. Select Yes to configure the NetVanta to perform security check when the policy is submitted

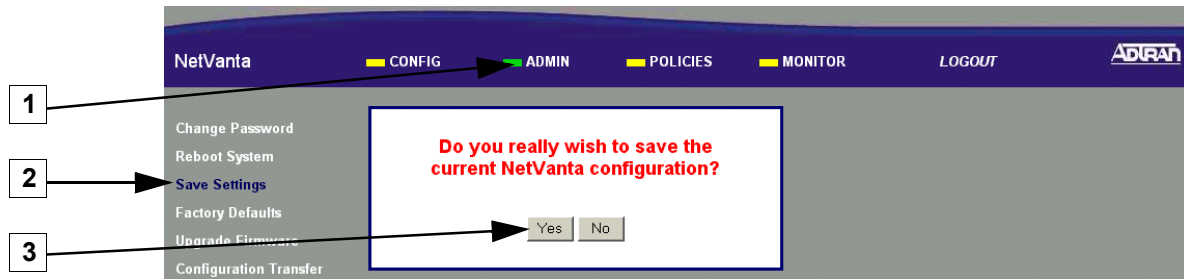


The security check ensures that all inbound data covered by this access policy has an associated VPN policy as well

9. Click Submit to register this policy

3

Saving the Settings



1. Select ADMIN
2. Select Save Settings
3. Select Yes to Confirm

