

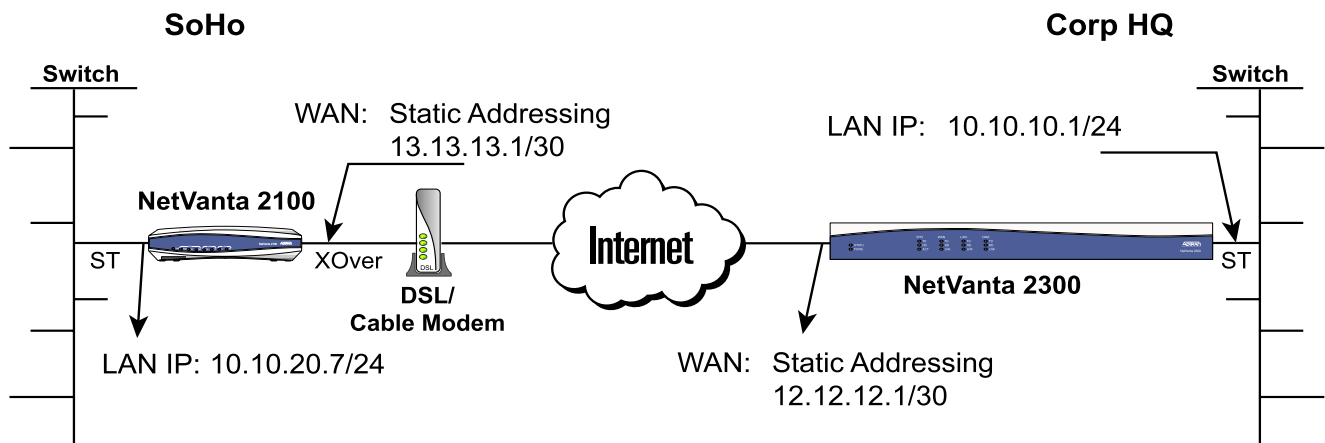
### Tools Required

- Category 5 - UTP crossover and/or straight-through (ST) cables, as required, for connection to existing network
- A PC with an internet browser (IE 5.5 or greater) for configuring the unit



*In this document, the term "NetVanta 2000" means any router in the NetVanta 2000 series (e.g., NetVanta 2100, NetVanta 2300, etc). If a statement only applies to one particular router, the text refers to the router individually.*

## Network Diagram

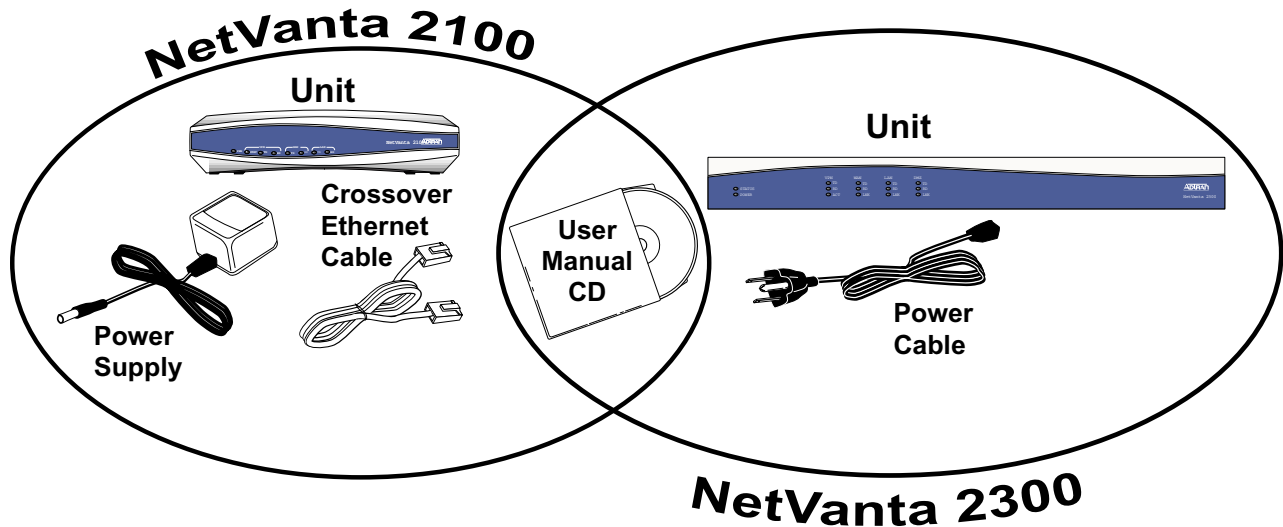


STEPS 1-2, 3-4d — Provide the stateful inspection firewall configuration.

STEPS 1-2, 5-6 — Configure a VPN connection between the NetVanta 2100 and the Corporate office (for the above network diagram).

## 1 Unpacking and Inspecting the System

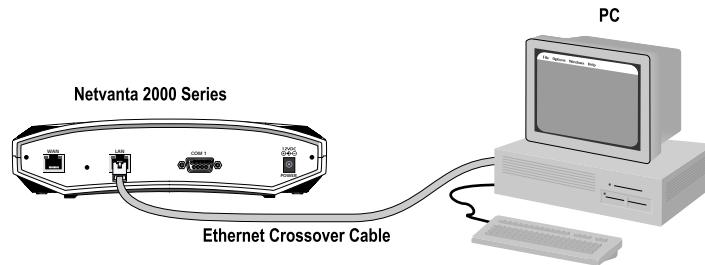
Each NetVanta 2000 is shipped in its own cardboard shipping carton. Open each carton carefully and avoid deep penetration into the carton with sharp objects.



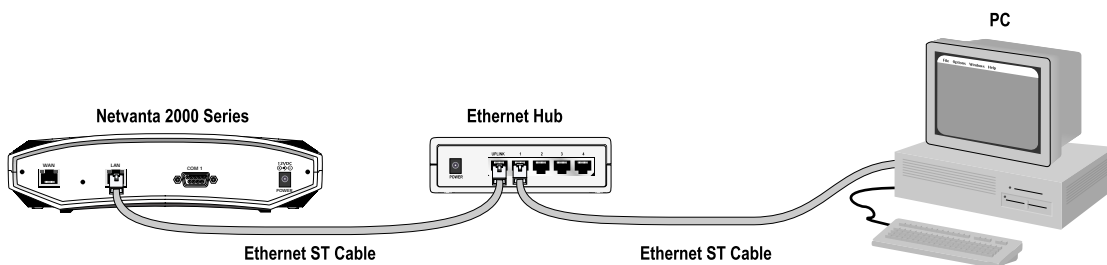
## 2

### Connecting to the NetVanta

The NetVanta 2000 can be accessed and managed via the LAN interface using an Ethernet crossover cable (provided with the NetVanta 2100). Alternately, the NetVanta 2000 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 5.5 for optimal viewing), the NetVanta can be configured using the web GUI. WAN connections are made in the same manner and with the same cabling considerations as LAN connections.



Direct Connection to PC or DSL/Cable Modem



Connection through Hub

## 3

### Configuring the System

1. Connect the NetVanta 2000 LAN interface to the PC using the appropriate Ethernet cable.
2. Supply power to the PC and the NetVanta 2000 and begin the operating system boot up process. During boot up, the PC obtains an IP address from the NetVanta 2000 DHCP server. Alternately, you could manually change your IP address to 10.10.10.1/24. Refer to your specific operating system's documentation for details on that process.
3. Open your installed browser, and enter 10.10.10.1 in the URL field. The NetVanta 2000 login screen appears.
4. Enter **admin** as the username, enter your admin password (if set), and click the **Login** button. When connecting to the NetVanta for the first time, there is no set password.

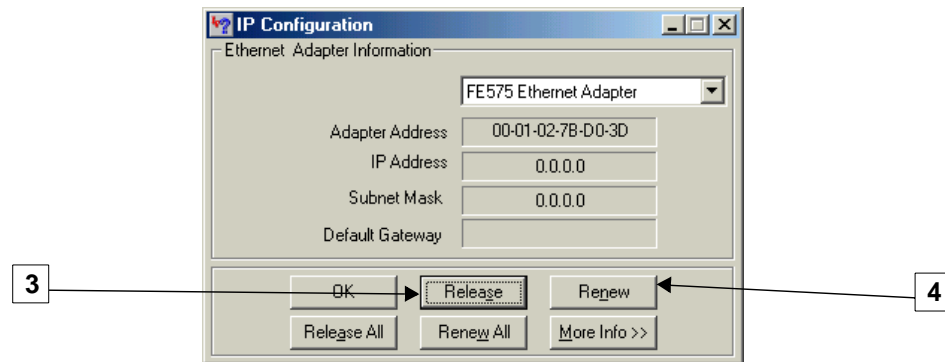


*For security purposes, it is important to set up an **admin** password immediately. Refer to the NetVanta 2000 System Manual (PN 61200361L1-1) for details.*

5. After logging in to the NetVanta 2000, the welcome screen appears.

## 3b Changing the IP Address to Your PC

If you wish to obtain a new IP address from the NetVanta 2000 DHCP server, you must release and renew your system's captured IP addresses. Refer to your specific operating system's documentation for details on that process if it differs from the procedure provided below.



1. Click **Start** on the 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.

## 4

## Configuring the LAN and WAN IP Parameters

The NetVanta 2000 comes 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 supports three types of WAN IP addresses: 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 (which is common in cable modems), configure the NetVanta 2000 for Dynamic addressing. Use PPPoE 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 results in a loss of management connectivity. Follow the correct procedure for your operating system 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 'NetVanta', 'CONFIG', 'ADMIN', 'POLICIES', 'MONITOR', 'LOGOUT', and the 'ADIRAN' logo. The left sidebar menu lists: 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: 13 . 13 . 13 . 1
- Subnet Mask: 255 . 255 . 255 . 0
- PPP over Ethernet section with fields for Username (required), Password, Password Confirmation, Service Name, and AC Name, and a 'Change Password?' checkbox.
- Buttons for 'Submit' and 'Reset' at the bottom.

1. Select **CONFIG**.
2. Select **Network Interface**.
3. Enter the assigned **LAN IP** address and associated **Subnet Mask**.
4. Enable the **Static** radio button for static addressing.



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

5. Enter the assigned **WAN IP** address and associated **Subnet Mask**.



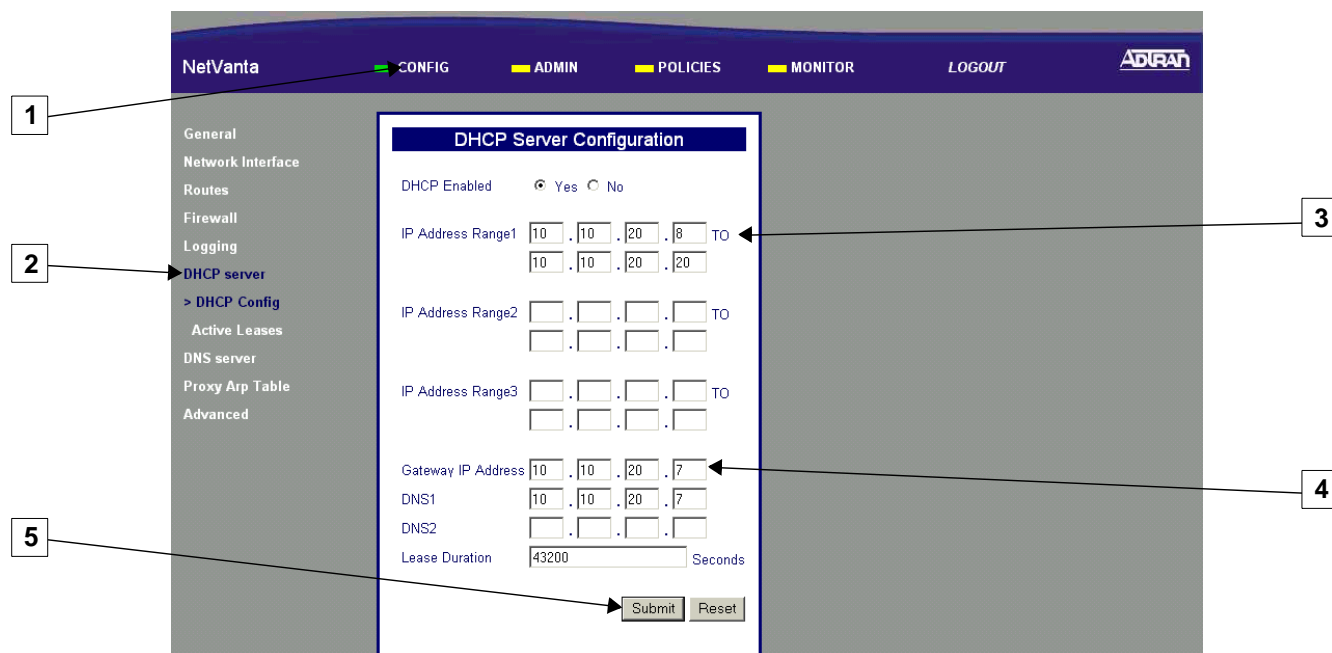
*The WAN IP parameters are set by the service provider. Contact your ISP before configuring the unit.*

6. Click **Submit** to register the changes.

# 4b

## Configuring the DHCP Server IP Parameters - Optional

The NetVanta 2000 automatically populates the DHCP IP Address Range 1 with ten addresses based on your assigned LAN network address.

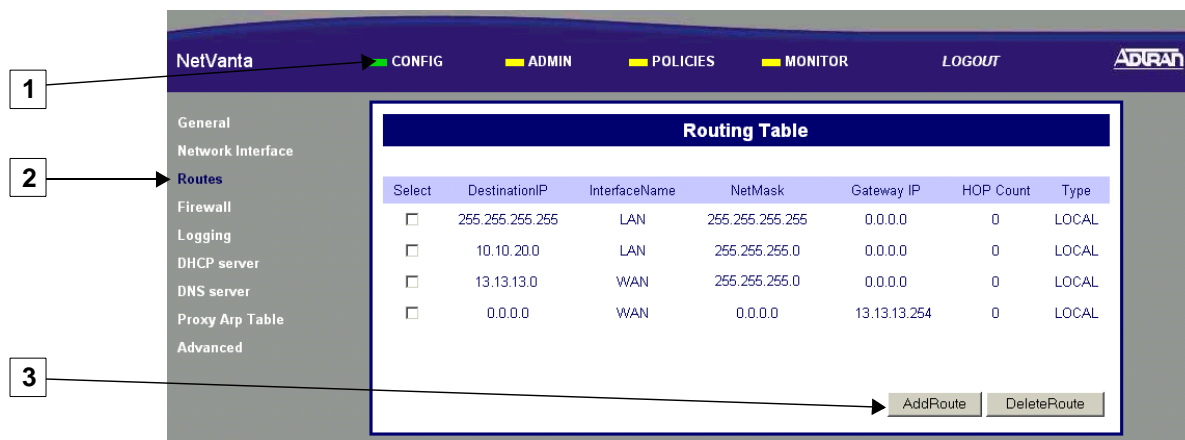


1. Select **CONFIG**.
2. Select **DHCP server**.
3. Enter an IP address range that is on the same subnet as the assigned LAN IP address of the unit.
4. Enter the assigned LAN IP address of the unit.
5. Click **Submit** to register the changes.

# 4c

## Adding a Default Route

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



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

## 4c

### Adding a Default Route (continued)

4. Select **WAN** to associate this default route with the WAN interface.
5. Select **Yes** to configure this as the default.
6. Enter all zeros.
7. Enter the next hop IP address for the **Gateway IP Address**.



*The Gateway IP Address is supplied by your provider.*

8. Click **Add Route** to submit this route to the route table.

## 4d

### Saving the Settings

1. Select **ADMIN**.
2. Select **Save Settings**.
3. Select **Yes** to confirm.



*The NetVanta is now configured for use as a stateful inspection firewall. To configure VPN, proceed to **Step 5**.*

## 5

## Defining a VPN Policy

*IKE Policy Configuration*

NetVanta    CONFIG    ADMIN    **POLICIES**    MONITOR    LOGOUT    ADIRAN

Manage Lists  
Access Policies: To LAN  
Access Policies: From LAN  
VPN  
Tunnels  
**IKE**  
Certificates

**IKE Policies**

Select	Policy Name	Exchange Type	Policy Type	Local ID Type
--------	-------------	---------------	-------------	---------------

Add    Delete    Modify    Show

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



*This example assumes the NetVanta 2300 is already similarly configured for a VPN connection to this NetVanta 2100.*

## IKE Policy Configuration (continued)

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** as the **Exchange Type**.

**NOTE** *If both sides do not have permanent IP addresses, see the Aggressive Mode tech note on [www.adtran.com](http://www.adtran.com).*

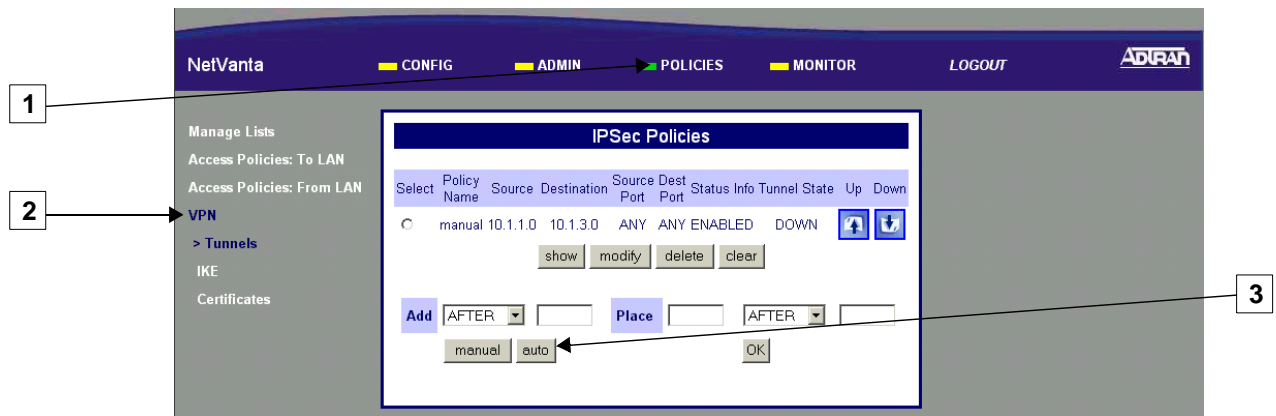
4. Use the unique Fully Qualified Domain Name (**FQDN**) for the local NetVanta 2000 and enter the identification data (these need not be registered names).
5. Use the unique **FQDN** for the remote users and enter the identification data (these need not be registered names).
6. Enter the local NetVanta 2000's assigned WAN IP address.
7. Enter the remote NetVanta 2000's assigned WAN IP address.
8. Select **3DES** to invoke Triple DES encryption.
9. Select **SHA** to use the secure hash authentication algorithm #1.
10. Select **Pre-SharedKey** and enter the key as a 12-character (minimum) alphanumeric string (spaces are not valid characters). This key **MUST** be the same for both the local and remote units.
11. Set the **Life time of key** to **86400** seconds (this 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 for key negotiation overhead.*

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



# IPSec Policy Configuration



1. Select **POLICIES**.
2. Select **VPN**.
3. Click the **auto** button.

## IPSec Policy Configuration (continued)

The screenshot shows the NetVanta configuration interface for an IPSec policy. The policy name is 'MyPolicy1' and its status is 'ENABLE'. The source address is 'OTHER' with IP '10.10.20.0' and mask '24'. The destination address is 'OTHER' with IP '10.10.10.0' and mask '24'. Both source and destination ports are set to 'ANY'. The protocol is 'ALL'. The peer security gateway is '12.12.12.1'. Perfect Forward Secrecy is set to 'NONE'. The security protocol is 'ESP WITH AUTH' with 'SHA1' authentication and '3DES' encryption. The life time is set to '28800' seconds. There are two 'LAST TRANSFORM' entries, each with 'MD5' authentication and 'DES' encryption. The 'Add' button is at the bottom.

1. Enter an alphanumeric string (spaces are not valid characters) to identify this policy (this is usually the same as the IKE name).
2. Select **ENABLE** to configure this as an active policy.
3. Select **OTHER** and enter the local NetVanta 2000's assigned LAN network address (e.g., 10.10.20.0) and associated subnet mask.
4. Select **OTHER** and enter the remote NetVanta 2000's assigned LAN network address (e.g., 10.10.10.0) and associated subnet mask.
5. Select **ANY** (for both the **Source Port** and **Destination Port**) to apply this policy to all data ports.
6. Select **ALL** to apply this policy to all data protocols.
7. Enter the remote NetVanta 2000's assigned WAN IP address.



*If the remote NetVanta 2000 is configured for dynamic addressing on the WAN interface, enter 0.0.0.0 here.*

8. Select **NONE**.
9. Select **ESP WITH AUTH**.
10. Select **SHA1** to invoke secure hash algorithm #1.
11. Select **3DES** to use Triple-DES encryption algorithm.
12. Set the key lifetime value to **28800** seconds (this is the ADTRAN suggested value).



*When determining the 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** for both **Security Protocol** settings.
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 tabs for CONFIG, ADMIN, POLICIES, MONITOR, and LOGOUT. The main content area is titled "To LAN" and contains a table of application diagrams. The table has columns for Select, 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. A "Submit" button is highlighted in the configuration area.

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 has a navigation bar with 'CONFIG', 'ADMIN', 'POLICIES', 'MONITOR', and 'LOGOUT' buttons. The main content area is titled 'Internet Access Policy Configuration' and contains the following fields and options:

- 1**: Points to the 'Source IP (WAN network address)' dropdown menu, which is set to 'OTHER'.
- 2**: Points to the 'IP if Source IP is OTHER' field, which is set to '10 . 10 . 10 . 0' with 'Mask Bits' set to '24'.
- 3**: Points to the 'Destination IP (LAN network address)' dropdown menu, which is set to 'OTHER'.
- 4**: Points to the 'IP if Dest IP is OTHER' field, which is set to '10 . 10 . 20 . 0' with 'Mask Bits' set to '24'.
- 5**: Points to the 'Protocol Type' dropdown menu, which is set to 'ALL'.
- 6**: Points to the 'Enable Log' radio button, which is set to 'No'.
- 7**: Points to the 'Action Type' dropdown menu, which is set to 'PERMIT'.
- 8**: Points to the 'Security' radio button, which is set to 'No'.
- 9**: Points to the 'Submit' button.

1. Select **OTHER** and enter the remote unit's assigned LAN IP network address and associated mask bits.
2. Select **OTHER** and enter the local NetVanta 2000's assigned LAN IP network address and associated mask bits.
3. Select **ANY** to forward all TCP/UDP ports, or select **OTHER** and enter the port (or port range) in the field below it.
4. Select **ALL** to forward all data protocols, or select **OTHER** and enter the protocol value (using decimal notation) in the field below it.
5. Select **PERMIT** to configure this policy to permit only the specified data.
6. Set **Enable Log** to **No**.
7. Set **Enable NAT** to **No**.
8. For **Security**, select **No**.
9. Click **Submit** to register this policy.

## From LAN Access Policy Configuration (Outbound Traffic)

The screenshot shows the NetVanta configuration interface. The navigation bar at the top has 'POLICIES' selected. The left sidebar shows 'Access Policies: From LAN' selected. The main content area displays the 'From LAN' configuration page. A table of application diagrams is shown with one rule selected. Below the table is a form to add a new rule, with 'Beginning' selected in the 'Add' dropdown menu. The 'Submit' button is highlighted.

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	<input type="button" value="Up"/> <input type="button" value="Down"/>

Buttons: Delete Edit Log Show Clear

Add  Rule ID  Submit Place Rule ID   Before  After  Submit

Dropdown menu: Beginning (selected), 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)

NetVanta CONFIG ADMIN POLICIES MONITOR LOGOUT ADIRAN

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

### Internet Access Policy Configuration

RULE ID: 12  
Policy Class: LAN\_OUTBOUND

1 SOURCE IP (LAN network address): OTHER

IP if Source IP is OTHER: 10 . 10 . 20 . 0 Mask Bits 24

2

4 Destination IP (DMZ or WAN network address): OTHER

IP if Dest IP is OTHER: 10 . 10 . 10 . 0 Mask Bits 24

3 Destination Port: ANY

Port Range if Dest Port is OTHER: TO

7 Protocol Type: ALL

If Protocol is OTHER enter Protocol value:

5 Action Type: PERMIT

6 Time Schedule Used:

8 Enable Log:  Yes  No

Enable NAT:  Yes  No

NAT to specific policy:

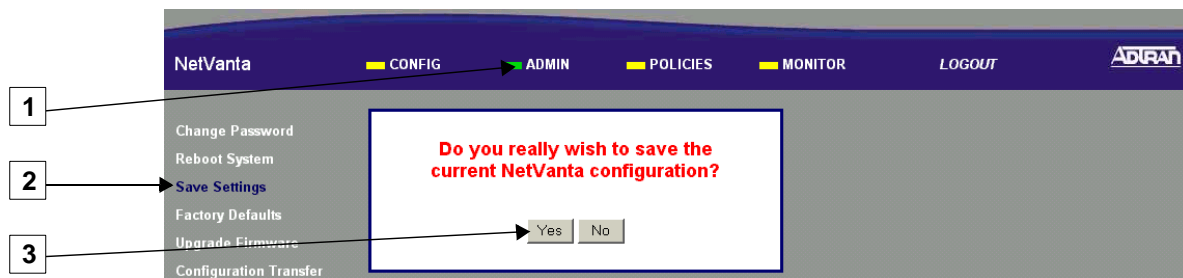
9 OR an IP Address (if OTHER):

OR Dynamic Interface:

Security:  Yes  No

Submit Reset

1. Select **OTHER** and enter the local NetVanta 2000's assigned LAN IP network address and associated mask bits.
2. Select **OTHER** and enter the remote NetVanta 2000's assigned LAN IP network address and associated mask bits.
3. Select **ANY** to forward all TCP/UDP ports, or select **OTHER** and enter the port (or port range) in the field below it.
4. Select **ALL** to forward all data protocols, or select **OTHER** and enter the protocol value (using decimal notation) in the field below it.
5. Select **PERMIT** to configure this policy to permit only the specified data.
6. Set **Enable Log** to **No**.
7. Set **Enable NAT** to **No**.
8. For **Security**, select **No**.
9. Click **Submit** to register this policy.

**5c****Saving the Settings**

1. Select **ADMIN**.
2. Select **Save Settings**.
3. Select **Yes** to confirm.

**6****Testing the New Tunnel**

1. Ping the LAN IP address of the corporate NetVanta 2300 (10.10.10.1) to test the new tunnel.
2. If the ping is not successful, have the administrator recheck the values and key configured on the NetVanta 2300 for this tunnel (as well as all the policies).