



TECH NOTE

Configuring Port Forwarding in AOS

Overview

Port Forwarding allows users on the 'Public' or 'Outside' interface of a NetVanta to initiate sessions to a device on the 'Private' or 'Inside' interface. The NetVanta accomplishes this by replacing the destination IP address on the Public side, with the corresponding Private IP address on the Private side; and vice-versa.

The NetVanta router inspects packets on its public interface, and replaces the destination IP address with the appropriate private IP Address. The router also keeps a table of sessions, to allow for the same action in the reverse direction.

Understanding Security Zones

The NetVanta router bundles its Firewall, NAT, and Port Forwarding functionality into a single application named Security Zones. Each IP Interface on the NetVanta router can be configured with a Security Zone. In the most common configuration, the Security Zone 'Public' is applied to the WAN interface of the router, and the Security Zone 'Private' is applied to the LAN interfaces of the of the router.

Security Zones have policies that define what hosts are allowed to initiate connections through that interface. Once a host has been allowed to initiate a connection through a Security Zone, the return traffic is automatically allowed; this is commonly called a statefull inspection. This means that 'allow' policies need only be defined on the initiating interface. For example, port forwarding http traffic (port 80) from the WAN interface to a server in the private LAN is accomplished by establishing a policy in the 'Public' Security Zone. This will allow internet users to initiate connections to the web server on your private network.

network.

Hardware/Software Requirements

This document describes Port Forwarding configuration for the AdTran, NetVanta product line through its Web Interface. You should use this document only *after* you have established reliable service across your NetVanta router, and completed the Firewall Wizard.

To accomplish this task you will need the following:

- Access to the Web Interface of the NetVanta product
- A Public IP Address, given to you by your ISP

- The Private IP Address, statically assigned to your server
- The TCP or UDP Port Number to be Forwarded

If you do not now know which protocol (Example: TCP and UDP), or Port Number (Example: 80) to select, please contact the application vendor.

Configuration Steps

Follow these instructions, substituting your information where prompted, to accomplish port forwarding.

The example shows a complete step-by-step Port Forward configuration for a Web Server on a private network. The example assumes that the Public IP 65.5.10.153 has been assigned by an ISP. The Web Server's private IP Address is 192.168.1.50.

Click '**Physical Interfaces**' in the main menu on the left side of the Web Interface.



Figure 1 - Physical Interfaces

Click the link under 'Logical Interface' (PPP, HDLC, or FR) next to your T1. Note that the 1/1 next to T1 in the example, stands for *slot 1* and *port 1* respectively. Be sure that you choose the appropriate logical interface, based on the slot and port number of your T1 interface.

Name	Logical Interface	Link
t1 1/1	ppp 1	LO Int
t1 1/2	none	LO Int

Figure 2 - Logical Interface

Frame Relay

Follow these instructions if you are using a frame-relay for your public interface.

After clicking 'fr 1', click the appropriate PVC name under Add/Mondify/Delete PVCs.

Description	DLCI
fr 1.16	16

Figure 3 - Frame PVC Interface

Public IP Address Requirement

The Public IP address, to be used by clients on the Public side, needs to be either the primary or a secondary address on your Public interface.

A screenshot of a web-based configuration interface. At the top, there is a header bar. Below it, there are two input fields: 'IP Address' containing '65 . 5 . 10 . 153' and 'Subnet Mask' containing '255 . 255 . 255 . 252'. Both fields have a small red circle with a question mark icon in the bottom right corner.

Figure 4 - Public IP Address Example

If the IP Address you are using is not the primary IP address of your Public Interface, it needs to be listed as a secondary IP address.

Adding a Secondary IP Address

To add a secondary IP address click the 'Add a new Secondary IP Address' link.



Figure 5 - Secondary IP Address

Enter the public IP address, assigned to you by your ISP, under 'IP Address', and the appropriate subnet mask under 'Mask'. Note that if you'd like to forward ports on more than one IP, you'll need to add each of the IPs separately.

Establishing the Port Forward

Note that at this point you should have already completed the 'Firewall Wizard', and have successfully connected to the Internet from your private network.

Port Forwards are configured as a policy in a security zone. Click 'Security Zones' under Firewall, in the left menu.



Figure 6 - Security Zones

Examine the top table to determine which Security Zone the Port Forward should be applied. This is most often the 'Public' Security Zone associated with WAN interface (PPP, HDLC or Frame Relay).

Click the name of the public Security Zone under 'Modify Security Zones'.

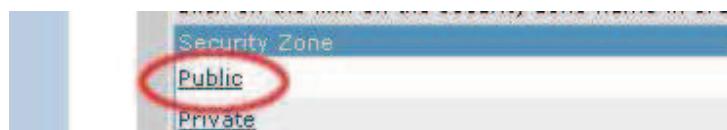


Figure 7 - Public Security Zone

Click ‘Add Policy to Security Zone ...’

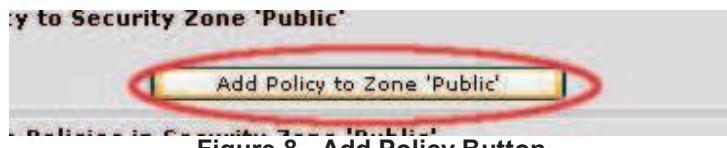


Figure 8 - Add Policy Button

Choose ‘Port Forward’ from the drop down menu and click ‘Continue’.

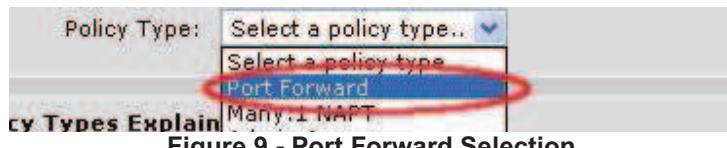


Figure 9 - Port Forward Selection

Enter a description for the Port Forward; for example the server name



Figure 10 - Policy Description

Choose the IP Address from which to be forwarded in the “Public IP Address”. If the IP address you wish to use is not listed in the drop down box, you must add that IP as a secondary address to the public interface (see *Adding a Secondary IP*).



Figure 11 - Public IP Selection

Enter the Private IP address of the server to which ports are forwarded. If you are unable to connect to this server using its private IP, you will not be able to connect to it using its public IP.

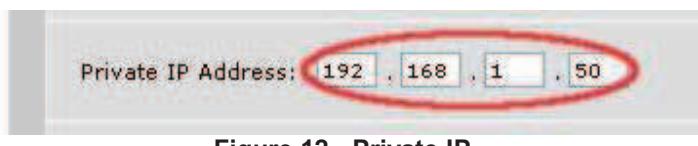


Figure 12 - Private IP

There are three methods of port forwarding. You may forward all ports (this is not secure), forward only specific ports, and forward specified ports with ‘translation’. Port translation forwards a single port on the outside IP address, to a different port on the inside IP; example port 80 to port 900.

Forwarding only Selected Ports

If you wish to forward traffic only on specific outside ports to the same inside ports, choose 'Forward only traffic specified below'. Remember that you must know the port number and protocol (TCP or UDP).

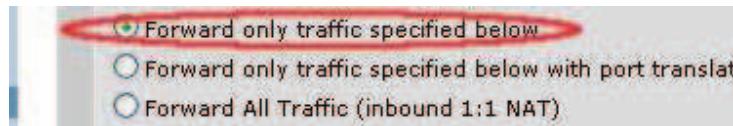


Figure 13 - Forward Specified Traffic

Under 'Protocols/Ports to Forward', choose the protocol on the far left. Then choose the appropriate 'Matching Port'.



Figure 14 - Protocol and Port to be Forwarded

If the common ports list does not include the port you wish to use, select <specified port> from the top of the list and enter the port number to the right.

To be able to ping the server from the public interface, you must choose ICMP from the protocol list; there is no associated port. Note that this will disable your ability to ping this public IP address, unless the server is up.

Multiple Port Forwards can be added by simply choosing additional protocols from the lowest row in the list.

Forwarding a Specific Port with Translation

If you wish to forward traffic from an outside port to a different inside port, choose 'Forward only traffic specified below with port translation'. Port Translation provides a service that alters the port number. For example, outside users may connect to port 80, while the router translates that to port 900 on the internal server. This is often used when additional Public IPs are not available, and uncommon port numbers are not a problem for outside users.

Choose 'Forward only traffic specified below with port translation'.

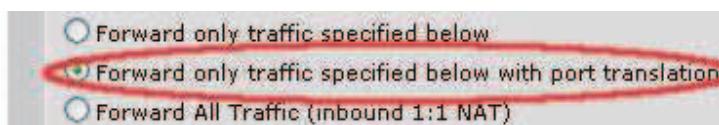


Figure 16 - Port Forwarding with Translation

The web interface will refresh, and a new 'Private Port' option will appear. Enter the port number to which clients will be forwarded; 900 in the example above.



Figure 17 - Private Port

Under 'Protocols/Ports to be Forwarded' choose the appropriate protocol on the left, and a port from the list on the right.



Figure 18 - Port Selection

If the common ports list does not include the port you wish to use, choose <specified port> at the top of the list, and enter the port number to the right.

Click 'Apply' when finished.

All ports chosen will be forwarded to the corresponding 'Private Port'. To port forward with translation to additional private ports, you must add additional Port Forward policies.

Forwarding All Ports

Forwarding all ports is not suggested, because it opens all ports on an otherwise secure server. If a vulnerability were to exist with any service on that server, forwarding all ports would allow easy access to that vulnerability; and possibly your entire network. Forwarding all ports is provided for completeness of the port forwarding feature.

To forward all ports simply select 'Forward All Traffic (inbound 1:1 NAT)', and then press 'Apply'.

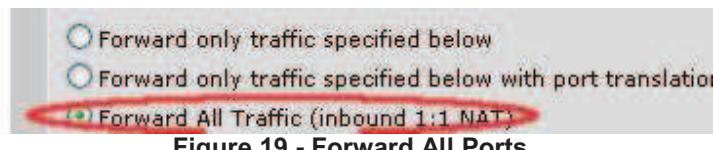


Figure 19 - Forward All Ports

Press 'Apply' after selecting all ports to be forwarded for this server.

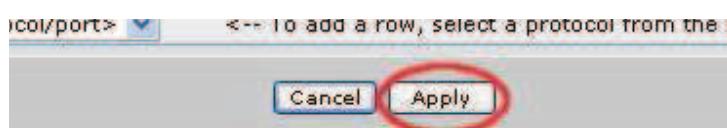


Figure 15 - Apply

Verifying Configuration

You will not be able to connect to the public IP address and port from the private side of your router. To verify that port forwarding is working, you must attempt to use the port forward from outside of your network. If you find that your portforward is not working from outside of your network, consult the troubleshooting section below.

Example Configuration

Example config is not applicable.

Troubleshooting

I can't connect to the public IP address of my server from my LAN.

You will not be able to connect to the public IP address from your LAN. From your LAN you will only be able to connect to the private IP address of your server.

I can't connect to the service from outside my network.

Security Zone policies are executed in order from top to bottom. You will probably find that moving the Port Forward policy to the top of your policy list resolves this issue. However, you must examine all of your policies in the security zone, to find those that overlap; affect the same IP and port. Be sure that policies in the top of your list, are not masking important policies below.

Please also check that the "Default Gateway" setting on your internal Server, is set to the NetVanta's private IP address. The server must respond to requests through the NetVanta for Port Forwarding to work correctly.

I have moved the policy to the top of the list, and double checked my gateway setting, but it still does not work.

The NetVanta keeps a table of all active sessions for each Security Zone. You can use this table to determine whether or not the NetVanta is properly forwarding packets. To view the active sessions click 'Security Zones', and then click on the "Active Sessions" column for the "Public" Security Zone; the link will be the number of current Active Sessions. Attempt to use the Port Forward (from outside of your network) and then browse the Active Sessions list for your connection; use your Source and Destination IP to find the appropriate row.

If you do not see a row that matches your source and destination IP, and you have moved the Port Forward policy to the top of Public Security zone, there is a device in front of the NetVanta that is blocking this traffic. Double check that your ISP allows the traffic you wish to Port Forward.

When you find a row that matches the Source IP, Destination IP and Destination Port check the "Nat Address/Port" column. This should match the server's private IP and port. If the "Nat Address/Port" does not have a value, or has an incorrect value, you have moved the Port Forward to the top of the Public Security Zone. You may need to restart the client, after doing so.

If you find that the "Nat Address/Port" column show the correct value, the NetVanta is properly configured. You will need to make changes to your Server. Double check the Default Gateway setting on your server, and contact the Server Application Vendor.

I am trying to Port Forward a TCP connection, and found it in the "Active Sessions" table. What else is there?

In the "Active Sessions" table, under the "Protocol" column, TCP connections will have a timeout listed in parenthesis. Example: TCP(200). If this number is less than 20 immediately after initiating a connection, the server is not responding. In this case, on the server can be at fault. If this number is greater than 20, the server has responded, and therefore the error may lie with the server's response, or the client's interpretation. In either case, please consult the application vendor.

If you experience any problems using your ADTRAN product, please contact [ADTRAN Technical Support](#).

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.