July 2007

AOS Quick Configuration Guide

Port Forwarding

Port Forwarding Overview

Common Network Address Translation (NAT) allows users on a trusted internal network to access resources on public networks, by translating the source IP address of outgoing packets from their original private address to a public address. This form of NAT (known as many to one NAT) is perfect for users who need client access to public servers on the Internet. However, this is not ideal when the server is behind the ADTRAN OS (AOS) device because public clients cannot initiate new inbound connections to the server. For example, a public Web Server would be inaccessible to clients on the Internet.

Port Forwarding allows users on the public (or “outside”) interface of a Network Address Translation device to initiate sessions to a device on the private (or “inside”) network. This is accomplished by replacing the destination IP address on the public side with the corresponding private IP address on the private side and vice-versa.

Understanding Security Zones

AOS devices bundle NAT and Port Forwarding functionality into the stateful inspection firewall. Each IP Interface on the device can be configured with an Access Policy, which defines the action(s) that the firewall should perform on specified traffic. These actions include, among other things, translating addresses. Security Zones should be named in a way that makes sense to network administrators. For example, 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 rules 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 stateful inspection. For example, port forwarding HTTP traffic (port 80) from the WAN interface to a server in the private LAN is accomplished by creating a policy in the ‘Public’ Security Zone. This will allow users on the Internet to initiate connections to the web server on your private network.

Hardware/Software Requirements/Limitations

There are no hardware or software requirements for Port Forwarding. Port Forwarding with Translation requires AOS 10.1 or later.

Configuring Port Forwarding

Configuring Port Forwarding in the GUI

Public IP Address Requirement

> *The Public IP address, which public clients will use to access your server needs to be either the primary or a secondary address on your Public interface. If you plan to use your primary IP address, or if you have already configured the appropriate secondary address on your WAN interface, you may proceed to the section "Configuring the Port Forward." Otherwise, continue with the section "Adding a Secondary IP Address." (Note that it is assumed that a primary IP address has already been added to the WAN interface.)*

Adding a Secondary IP Address

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

Click the link for your WAN interface, as it is listed under the "Name" column.

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

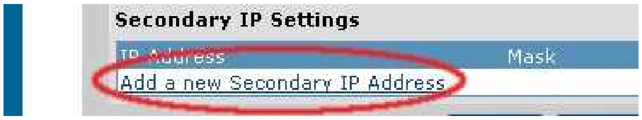


Figure 1 - Secondary IP Address

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 want to forward traffic for more than one IP, you will need to add each of the IPs separately.

Configuring 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.

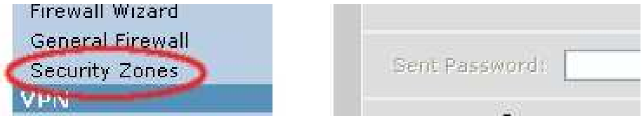


Figure 2 - Security Zones

Examine the top table to determine which Security Zone the Port Forward should be applied to. This is most often the ‘Public’ Security Zone associated with the WAN interface.

Click the name of the public Security Zone under ‘Modify Security Zones’.

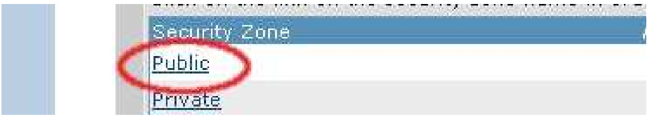


Figure 3 - Public Security Zone

Click the ‘Add Policy to Zone <Zone-Name>’ button.

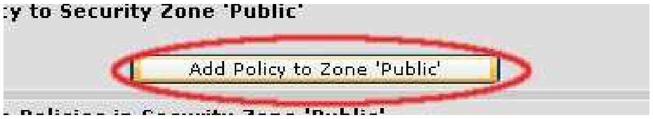


Figure 4 - Add Policy Button

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

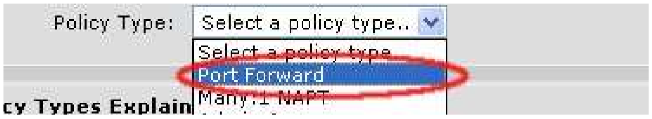
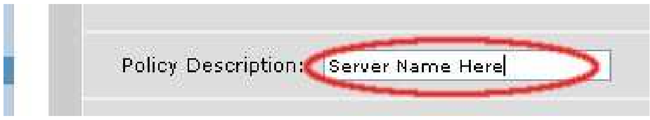


Figure 5 - Port Forward Selection

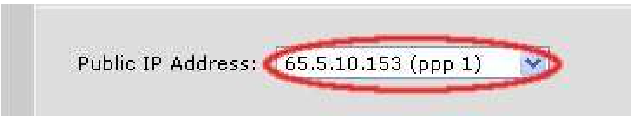
Enter a description for the Port Forward. This should clearly describe the port forward. A common description is the name of the server associated with the Port Forward.



Policy Description: Server Name Here

Figure 6 - Policy Description

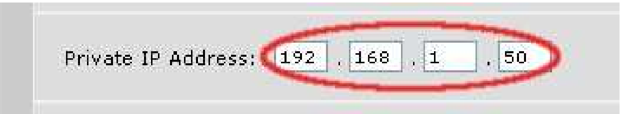
Choose the appropriate public IP Address in the “Public IP Address” drop down menu. If the IP address you wish to use is not listed in the drop down box, you must add that IP as a secondary address to the public interface (see *Adding a Secondary IP Address*).



Public IP Address: 65.5.10.153 (ppp 1)

Figure 7 - Public IP Selection

Enter the private IP address of the server to which traffic will be 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.



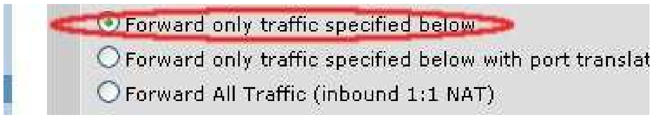
Private IP Address: 192 . 168 . 1 . 50

Figure 8 - Private IP

There are three methods of port forwarding. You may forward all ports (this is not secure), forward only specific ports, or forward specified ports with ‘translation’. Port translation allows both the destination IP address as well as destination port to be substituted on inbound traffic.

Forwarding only Selected Ports

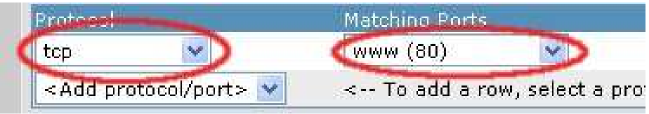
Choose ‘Forward only traffic specified below’ to forward only specific outside ports to the same inside ports. Remember that you must know the port number and protocol (TCP or UDP).



● Forward only traffic specified below
○ Forward only traffic specified below with port translat
○ Forward All Traffic (inbound 1:1 NAT)

Figure 9 - Forward Specified Traffic

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



Protocol	Matching Ports
tcp	www (80)
<Add protocol/port>	<-- To add a row, select a pro

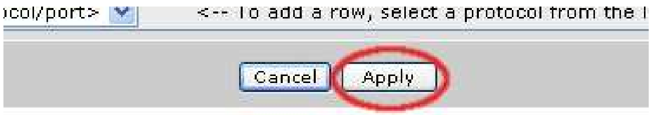
Figure 10 - Protocol and Port to be Forwarded

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 at the bottom of the list.

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



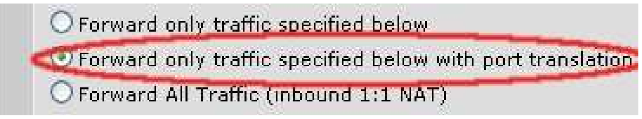
col/port> <-- To add a row, select a protocol from the

Figure 11 - Apply

Forwarding a Specific Port with 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 IP addresses are not available, and uncommon port numbers are not a problem for end users.

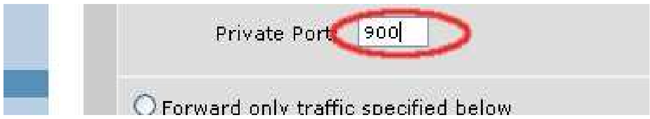
Choose ‘Forward only traffic specified below with port translation’.



○ Forward only traffic specified below
● Forward only traffic specified below with port translation
○ Forward All Traffic (inbound 1:1 NAT)

Figure 12 - 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).

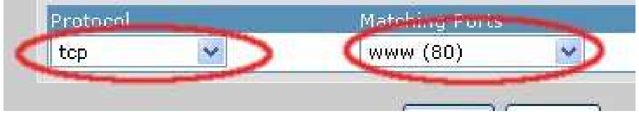


Private Port: 900

○ Forward only traffic specified below

Figure 13 - Private Port

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



Protocol	Matching Ports
tcp	www (80)

Figure 14 - 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.

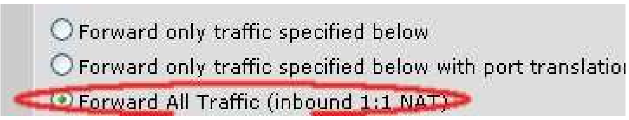
Click ‘Apply’ when finished.

All ports chosen will be forwarded to the corresponding ‘Private Port’. To configure additional port translations , 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 to 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’.



○ Forward only traffic specified below
○ Forward only traffic specified below with port translatio
● Forward All Traffic (inbound 1:1 NAT)

Figure 15 - Forward All Ports

Configuring Port Forwarding in the CLI

1. Assign the appropriate public IP to the WAN Interface. This address may be the primary serial WAN IP address of the router, or an address from a separate public address space (commonly referred to as a "public LAN block"). If you are adding an additional IP from your public LAN block to the WAN interface, it can be added as a secondary address. This can be accomplished by adding **secondary** to the end of the **ip address** command.

   Syntax: **ip address** <*A.B.C.D*> <*subnet mask*> [**secondary**]

2. Define forwarded traffic using an Access Control List (ACL).

   a. Create an access list to define the traffic that should be forwarded. Creating this access list will also allow you to specify, if need be, the remote subnets that are allowed to connect using this Port Forward. Each access list can contain multiple statements. As in this example, if a single PC was serving both SMTP and HTTP traffic, you could forward both from the same ACL.

   Syntax: **ip access-list extended** <*ACL Name*>

   b. Now, define the traffic you wish to act upon. You have the choice of specifying a specific host, a subnet, or **any** as the source or destination. Remember that all incoming traffic will be addressed to the WAN link of your router (either the primary IP or a secondary address) and not to the private address. Additionally, note that when you specify a subnet, a wildcard mask is used.

   Syntax: **permit** <*protocol*> **[any | host** <*A.B.C.D*> **|** <*A.B.C.D*> <*wildcard mask*>**]** **[any | host** <*A.B.C.D*> **|** <*A.B.C.D*> <*wildcard mask*>**]** [eq <*port number*>]

   For the first address, enter the source of the traffic to be forwarded. For most applications, traffic from any source should be forwarded. The second address is the public destination address of traffic that should be forwarded. For most applications, this should be a host address, with a single public IP address associated with your server.

3. Add the Port Forward to the public policy class.

   a. Navigate to your public security policy. This is the security policy assigned to your WAN link.

   Syntax: **ip policy-class** <*policy name*>

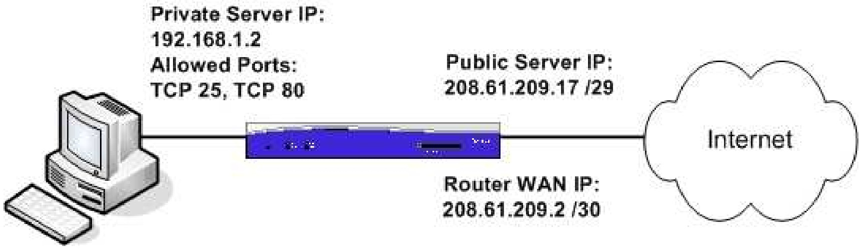
   b. Now, create the NAT in the policy class. This is where the private IP address is referenced. For Port Translation, you may also specify the appropriate private TCP or UDP port in the access control entry.

   Syntax: **nat destination list** <*ACL name*> **address** <*A.B.C.D*> [port <*port number*>]

Command Summary Table

	Command	Description
Step 1	(config)#**ip access-list extended** <*ACL name*>	Create an ACL to define traffic
Step 2	(config-ext-nacl)#**permit** <*protocol*> **[any | host** <*A.B.C.D*> **|** <*A.B.C.D*> <*wildcard mask*>**] [any | host** <*A.B.C.D*> **|** <*A.B.C.D*> <*wildcard mask*>**] [eq** <*port number*>**]**	Define the source, destination, and port for the traffic that you wish to forward
Step 3	(config-ext-nacl)#**ip policy-class** <*policy name*>	Access the policy assigned to your WAN interface
Step 4	(config-policy-class)#**nat destination list** <*ACL name*> **address** <A.B.C.D> [port <internal port>]	Create a NAT that references the internal IP address you are attempting to forward to. For Port Forwarding with Translation, use the optional **port** keyword.

Example Configuration



The example above shows a server that provides both SMTP (TCP port 25) and HTTP (TCP port 80) services that are to be accessible from the Internet. The server's private IP address is 192.168.1.2, but external clients should be able to reach the server via a public IP address, 208.61.209.17.

Assuming that there is already a public policy class assigned to the WAN interface (PPP for this example), called Public, you would enter the following commands to configure the Port Forward.

```
Router(config)# interface ppp 1
Router(config-ppp 1)# ip address 208.61.209.17 255.255.255.248 secondary
Router(config-ppp 1)# ip access-list extended PFWD
Router(config-ext-acl)# permit tcp any host 66.22.11.10 eq 25
Router(config-ext-acl)# permit tcp any host 66.22.11.10 eq 80
Router(config-ext-acl)# ip policy-class Public
Router(config-policy-class)# nat destination list PFWD address 192.168.1.2
```

Troubleshooting

In order to test a port forward, you will need to attempt to access your server from outside your network. It is not possible for a PC on the inside of the network to make use of the port forward. Traffic must originate from outside the network.

If the test is occurring from outside the network and it still fails, check the order of the policies. Rules are executed in sequential order. If there is a firewall rule above the one you have created that interferes with a new rule, then the new rule will not take effect.

The **show ip policy-sessions** <*policy name*> command is also useful for troubleshooting. The output of this command shows all sessions and NATs currently taking place in the firewall.