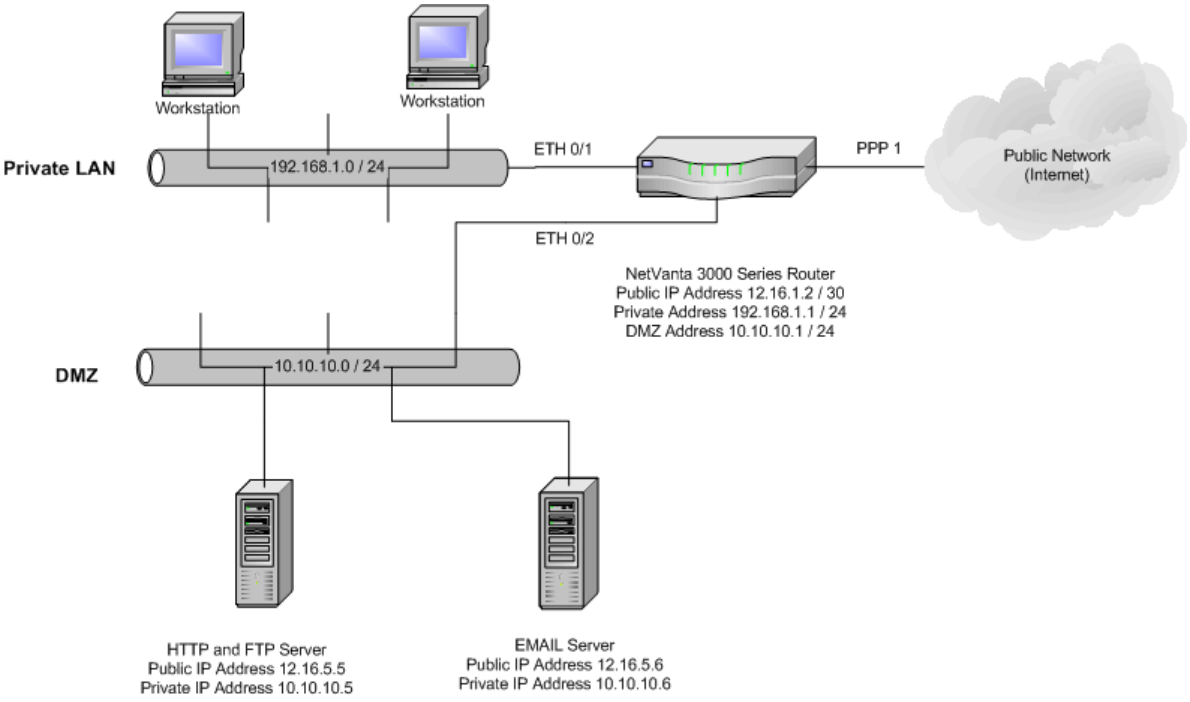
August 2007

AOS Quick Configuration Guide

Configuring a DMZ in AOS

A DMZ (De-Militarized Zone) is a network added between a Private network and a Public network in order to provide an additional layer of security. A DMZ doesn't allow a Public network to directly access a machine on the Private network. It does this by isolating the machine (or machines) that is being directly accessed from the Public network. Because the machine needs to be available to the Public network, it is the most vulnerable and therefore, more easily compromised. If this machine were compromised, and not in a DMZ, the perpetrator would have full access to the rest of the Private network. By moving the machine to a DMZ, and restricting access from the DMZ to the Private network, the compromised machine would still not have access to the Private network. Most of the time the public network is the Internet and the DMZ contains a web server, FTP server or email server.

In this example, users on the Private Network want to be able to host HTTP, FTP and email servers for the Internet. The public IP addresses of the servers are different than the NetVanta's WAN IP address, so the NetVanta needs to be told to respond for those addresses. This is done with the "**ip address <*address*> <*mask*> secondary**" command. The NetVanta will then have an Access-lists that allow TCP port 80 (HTTP) and 25 (SMTP), and an Application Level Gateway (ALG) that understands FTP for those public IP addresses. When the NetVanta receives traffic matching the Access-lists, it will translate the destination address using NAT, and forward the traffic on to the private IP address of the appropriate server. In this case, the HTTP and FTP servers are the same machine. The email server is on a separate machine.



Hardware/Software Requirements/Limitations

Any router based AOS product with firewall capacity and more than one routed Ethernet port is capable of supporting a DMZ. Additionally, any switch based product with an integrated routing engine can support a DMZ.

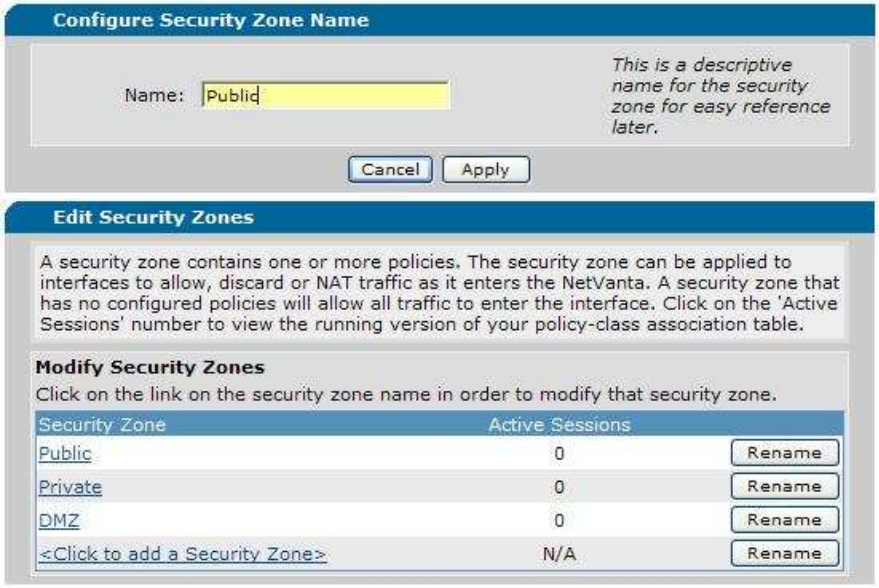
Configuring a DMZ

This guide covers configuration of a switch based router such as a 1224R. The same principles apply to routers such as the 3305, 3430, 3120, etc. The primary difference between configuring a router versus a switch based product is that in a router product, the IP and firewall information will be applied to Ethernet ports, while in a switch, they are applied to VLANs.

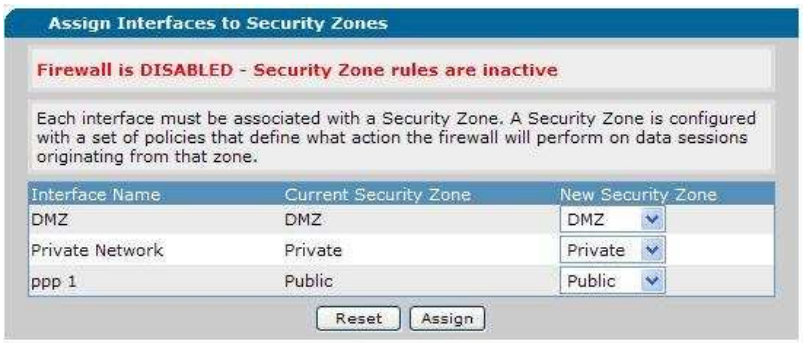
Configuring a DMZ in the GUI

First, navigate to “Security Zones” and create 3 security zones by clicking on the link “Click to add a Security Zone”.

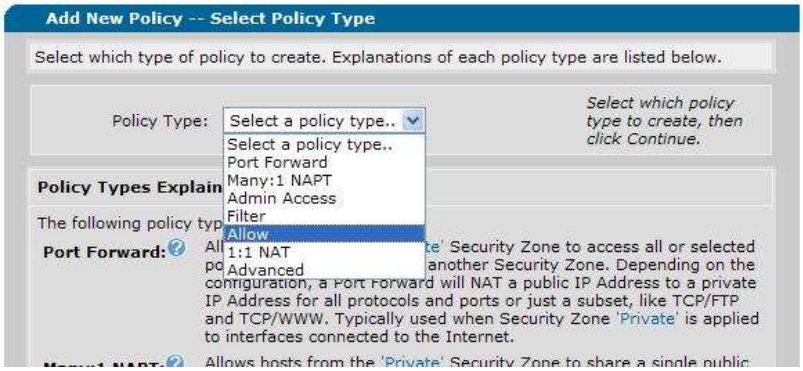
They can be named Public, Private, and DMZ



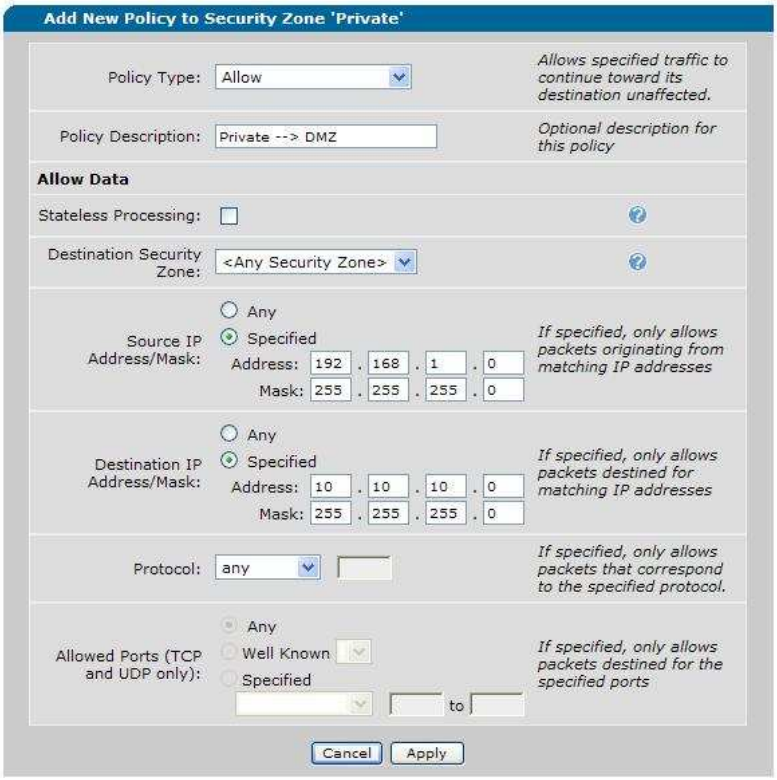
Once the Security Zones have been created, they must be assigned to interfaces. For the purpose of this configuration guide, the network consists of a 1224R with a T1 PPP based internet connection. The Private zone will be assigned to the local network, the DMZ zone to the DMZ network, and the Public zone to the PPP interface.



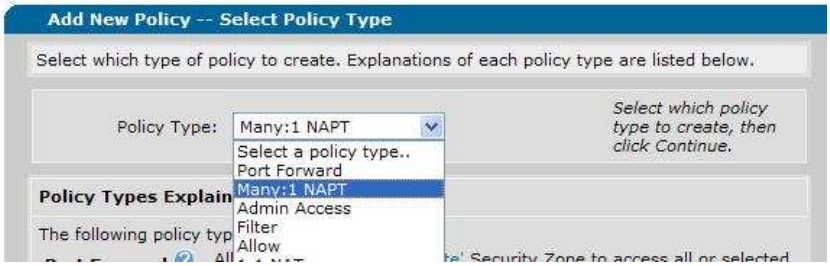
Next, firewall rules must be created for each zone. First, the rules for the Private security zone. First, an "Allow" rule must be created in order to allow traffic from the private security zone to the DMZ. Navigate to the Private security zone and click "Add a policy to zone Private". Select "Allow" and click "Continue".



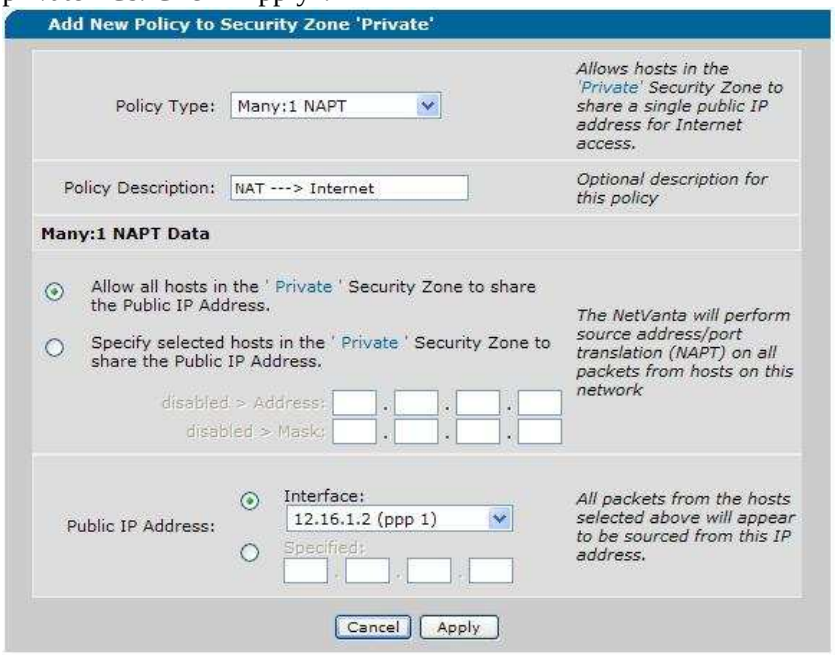
Next, fill in the details for the allow policy. The source subnet will be the subnet of the private network. The destination subnet will be the DMZ network. This will allow traffic to be initiated to the DMZ side from the private network.



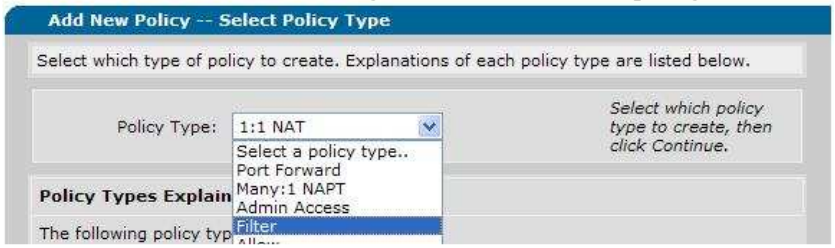
Next, create the Many:1 NAT for the private side. This will allow the private addresses to use the single public IP address assigned to the router. Navigate back to the Private security zone and click “Add Policy to Zone Private” and select Many:1 NAT. Click “Continue”.



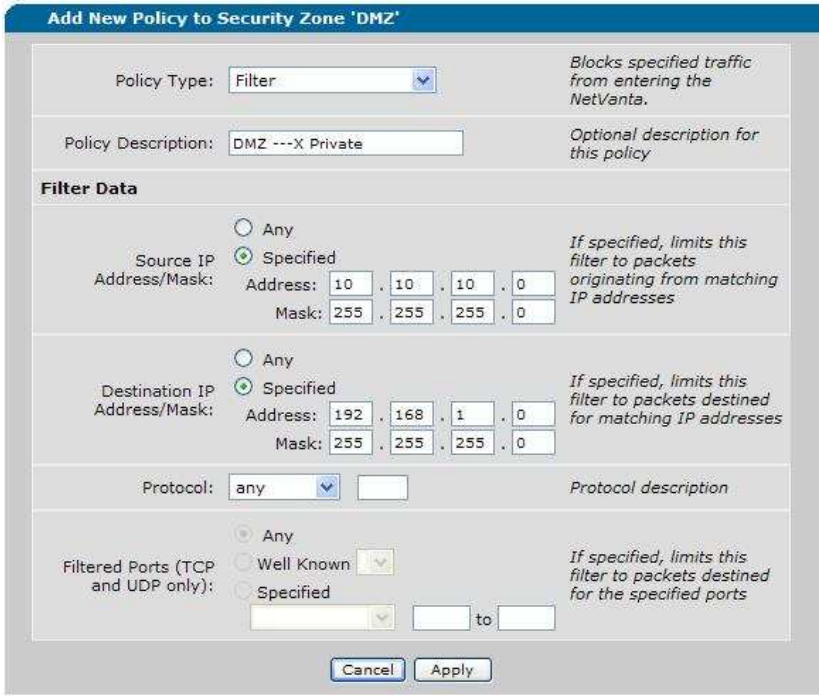
Fill in the description, if desired, and select the public IP address of the router as the address shared by the private PCs. Click “Apply”.



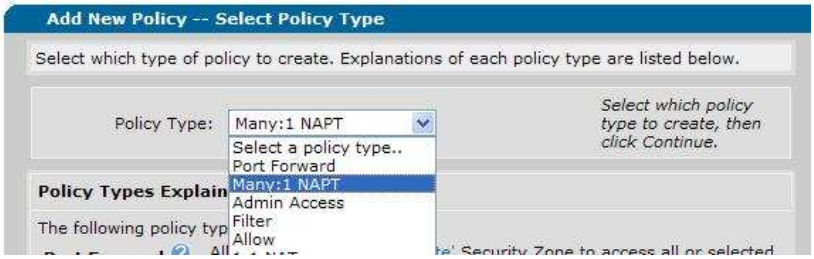
Next, move to the DMZ security zone. Click to add a policy and select “Filter”. Click “Continue”



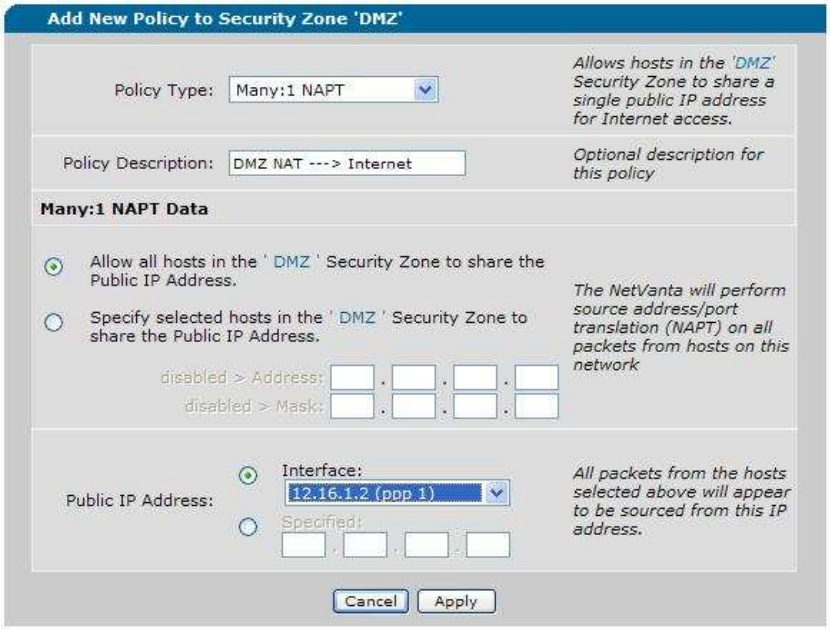
For the filter policy, fill in the source network as the subnet of the DMZ and the destination network as the subnet of the private network. This will block all traffic initiated from one of the devices on the DMZ destined for the private network, but will still allow the servers to respond to requests initiated from the private side. Click “Apply”.



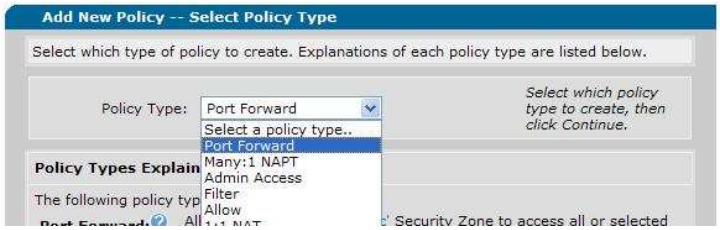
Next, add another policy to the DMZ zone. Select “Many:1 NAT”.



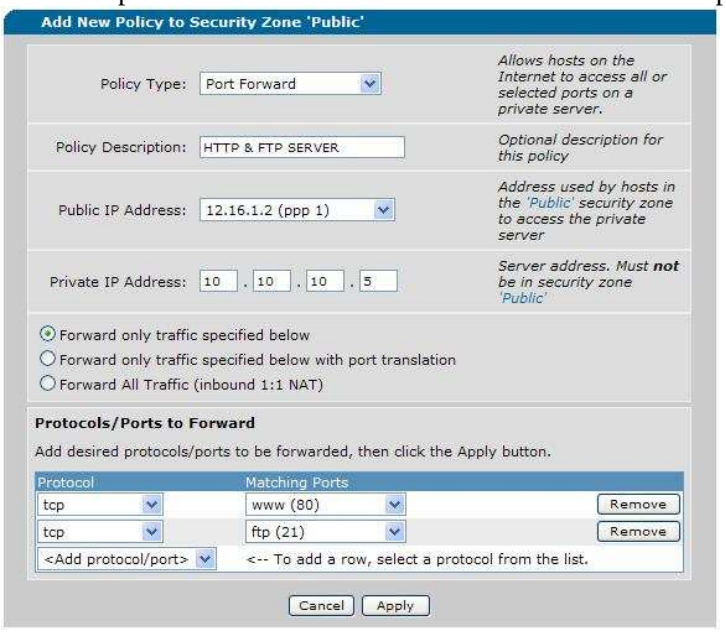
Fill in the description, if desired, and select the public IP address of the router. This policy will allow the devices in the DMZ to get out to the internet. Click “Apply”.



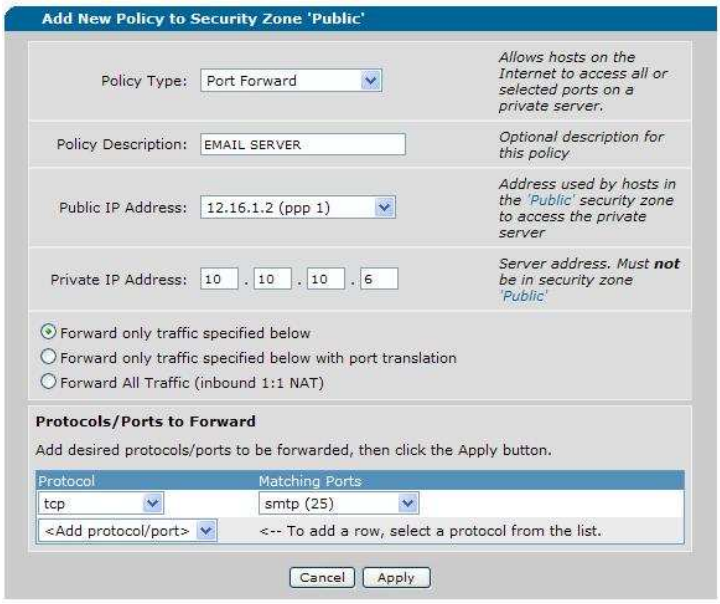
Finally, port forwards need to be configured on the public side for any traffic that will be iniated from the internet. In this example, there are two servers, one hosting mail and the other hosting FTP and HTTP. Navigate to the Public security zone and click to add a policy. Select “Port Forward” from the list and click “Continue”.



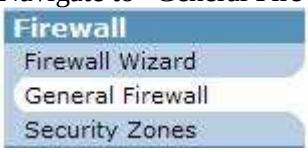
Fill in the information for the external and internal IP addresses that will be used. At the bottom of the page, select the ports that will be forwarded to the server. Click “Apply”.



Repeat this procedure for the second server.



With the configuration for the security zones complete, enable the firewall to complete the configuration. Navigate to “General Firewall”.



Check the “Enable” box and click “Apply”.

Configuring DMZ in the CLI

1. Create 3 policy classes. One zone will be for the private network, one for the DMZ, and the other for the public side of the router.

   Syntax: **ip policy-class** <*policy name*>
   EX: (config)# **ip policy-class Private**

2. Assign the classes to their appropriate interface.

   Syntax: **access-policy** <*policy name*>
   EX: (config-ppp 1)# **access-policy Public**

3. Create an access list for Many:1 NATs. This access list will define all traffic.

   Syntax: **ip access-list extended matchall**
   Syntax: **permit ip any any**

4. Create an access list to define traffic from LAN to DMZ.

   Syntax: **ip access-list extended toDMZ**
   Syntax: **permit ip** <*source subnet*> <*source wildcard*> <*destination subnet*> <*destination wildcard*>
   EX: (config-ext-nacl)# **permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255**

5. Create an access list to define traffic from DMZ to LAN

   Syntax: **ip access-list extended toLAN**

Syntax: **permit ip** <*source subnet*> <*source wildcard*> <*destination subnet*> <*destination wildcard*>
EX: (config-ext-nacl)# **permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255**

6. Create access-lists to define traffic to be port forwarded. The destination IP address will be the external IP receiving the traffic.

   Syntax: **ip access-list extended** <*list name*>
   Syntax: **ip access-list extended HTTP-FTP**
   Syntax: **permit tcp** <*source subnet*> <*source wildcard*> **host** <*host IP*> **eq** <*port number*>
   EX: (config-ext-nacl)#**permit tcp any host 12.16.1.2 eq 80**
   EX: (config-ext-nacl)#**permit tcp any host 12.16.1.2 eq 21**

7. Apply the toDMZ access list to the private policy class.

   Syntax: **allow list** <*list name*>
   EX: (config-policy-class)# **allow list toDMZ**

8. Create the Many:1 NAT within the private policy class to allow traffic out to the internet.

   Syntax: **nat source list** <*list name*> **interface** <*outside interface*> **overload**
   EX: (config-policy-class)# **nat source list matchall interface PPP 1 overload**

9. Apply the filter rule to the DMZ policy class. This rule will prevent devices within the DMZ from creating connections to the private network.

   Syntax: **discard list** <*list name*>
   EX: (config-policy-class)# **discard list toLAN**

10. Create the Many:1 NAT within the DMZ policy to allow traffic to the internet.

    Syntax: **nat source list** <*list name*> **interface** <*outside interface*> **overload**
    EX: (config-policy-class)# **nat source list matchall interface PPP 1 overload**

11. Apply the port forward access list to the public policy class.

    Syntax: **nat destination list** <*list name*> **address** <*internal IP*>
    EX: (config-policy-class)# **nat destination list HTTP-FTP address 10.10.10.5**

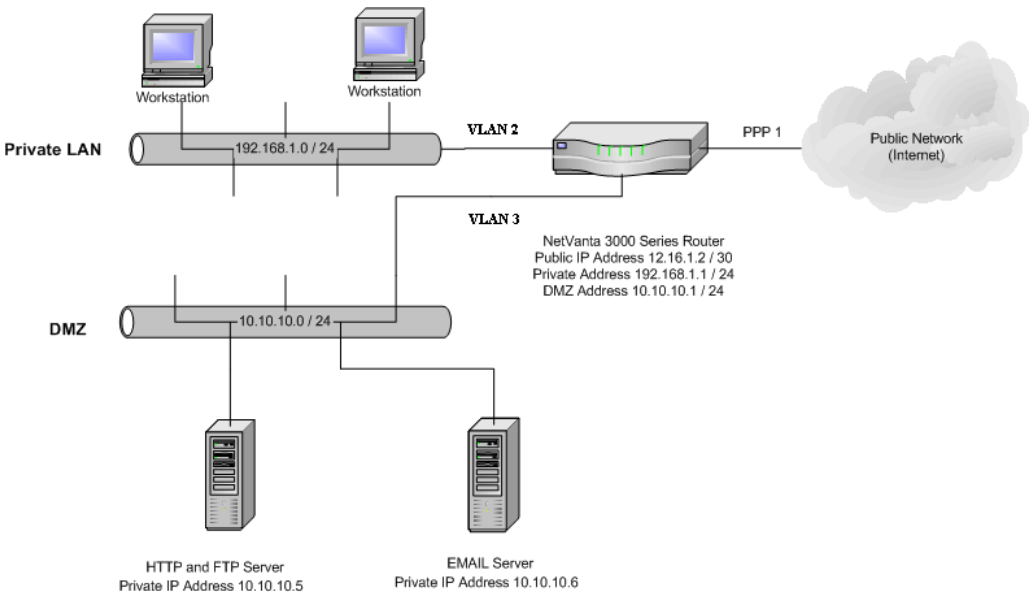
12. Finally, enable the firewall from the global config prompt.

    (config)# **ip firewall**

Command Summary Table

	Command	Description
Step 1	(config)# **ip policy-class** <*policy name*>	Create 3 policy classes. One for the private LAN, one for the DMZ, and one for the public side.
Step 2	(config-ppp 1)# **access-policy** <*policy name*>	Assign each policy class to its appropriate interface.
Step 3	(config)# **ip access-list extended matchall** (config-ext-nacl)# **permit ip any any**	Create an access list for use with the Many:1 NATs that defines all traffic.
Step 4	(config)# **ip access-list extended toDMZ** (config-ext-nacl)# **permit ip** <*source subnet*> <*source wildcard*> <*destination subnet*> <*destination wildcard*>	Create an access list to define traffic from the LAN to the DMZ.
Step 5	config)# **ip access-list extended toLAN** (config-ext-nacl)# **permit ip** <*source subnet*> <*source wildcard*> <*destination subnet*> <*destination wildcard*>	Create an access list to define traffic from the DMZ to the LAN.
Step 6	(config)# **ip access-list extended HTTP-FTP** (config-ext-nacl) **permit** <*protocol*> <*source subnet*> <*source wildcard*> **host** <*host IP*> **eq** <*port number*>	Create access lists to define the traffic that will be forwarded to the internal server. The destination IP address will be the external IP that the traffic will hit.
Step 7	(config-policy-class)# **allow list toDMZ**	Apply the "toDMZ" list to the private policy class.
Step 8	(config-policy-class)# **nat source list matchall interface PPP 1 overload**	Create the Many:1 NAT within the private policy class to allow traffic out to the internet.
Step 9	(config-policy-class)# **discard list toLAN**	Apply the filter rule to the DMZ policy class. This rule will prevent devices within the DMZ from creating connections to the private network.
Step 10	(config-policy-class)# **nat source list matchall interface PPP 1 overload**	Create the Many:1 NAT within the DMZ policy to allow traffic to the internet.
Step 11	(config-policy-class)# **nat destination list** <*list name*> **address** <*internal IP*>	Apply the port forward access list to the public policy class.
Step 12	(config)# **ip firewall**	Enable the firewall.

Example configuration




```
(config)# interface vlan 2
(config-vlan 2)# ip address  192.168.1.1  255.255.255.0
(config-vlan 2)# access-policy Private
(config-vlan 2)# no shutdown
(config-vlan 2)# interface vlan 3
(config-vlan 3)# ip address  10.10.10.1  255.255.255.0
(config-vlan 3)# access-policy DMZ
(config-vlan 3)# no shutdown
(config-vlan 3)# interface ppp 1
(config-ppp 1)# ip address  12.16.1.2  255.255.255.252
(config-ppp 1)# access-policy Public
(config-ppp 1)# no shutdown
 (config-ppp 1)# ip access-list extended toDMZ
(config-ext-acl)# permit ip 192.168.1.0 0.0.0.255  10.10.10.0 0.0.0.255
(config-ext-acl)# ip access-list extended matchall
(config-ext-acl)# permit ip any  any
(config-ext-acl)# ip access-list extended HTTP-FTP
(config-ext-acl)# permit tcp any  host 12.16.1.2 eq www  log
(config-ext-acl)# permit tcp any  host 12.16.1.2 eq ftp  log
(config-ext-acl)# ip access-list extended SMTP
(config-ext-acl)# permit tcp any  host 12.16.1.2 eq smtp  log
(config-ext-acl)# ip access-list extended toLAN
(config-ext-acl)# permit ip 10.10.10.0 0.0.0.255  192.168.1.0 0.0.0.255
(config-ext-acl)# ip policy-class DMZ
(config-policy-class)# discard list toLAN
(config-policy-class)# nat source list matchall interface ppp 1 overload
(config-policy-class)# ip policy-class Private
(config-policy-class)# allow list toDMZ
(config-policy-class)# nat source list matchall interface ppp 1 overload
```

```
(config-policy-class)# ip policy-class Public
(config-policy-class)# nat destination list HTTP-FTP address 10.10.10.5
(config-policy-class)# nat destination list SMTP address 10.10.10.6
```