



TECHNICAL SUPPORT NOTE

Configuring PPTP through NAT in AOS

Introduction

Network Address Translation (NAT) is an Internet Engineering Task Force (IETF) standard method of preserving precious Internet address space. Additionally, it can be used to hide the structure of server farms behind a router, in order to provide bandwidth sharing to Web, FTP, and Application Servers.

In this example, users on the Internet want to be able to initiate a PPTP session to a server on the LAN. The public IP address of the server is different than the NetVanta's WAN IP address, so the NetVanta needs to be told to respond for that address. This is done with the **ip address <address> <mask> secondary** command. The NetVanta will then have an access control list (ACL) that allows TCP port 1723 and IP protocol GRE for that public IP address. When the NetVanta receives traffic matching that ACL, it will translate the destination address using NAT, and forward the traffic on to the private IP address of the server. Follow the steps below to see how this is done.

*** Before You Begin**

Prior to configuring NAT on your NetVanta router, obtain all necessary IP address assignments from the network administrator and Internet Service Provider (ISP) if applicable. All circuits should be installed and tested prior to the installation of your router. Although the example shown here may differ from your configuration, all the basic concepts associated with activating NAT are presented. For additional assistance please contact [ADTRAN Technical Support](#).

Allowing PPTP through NAT

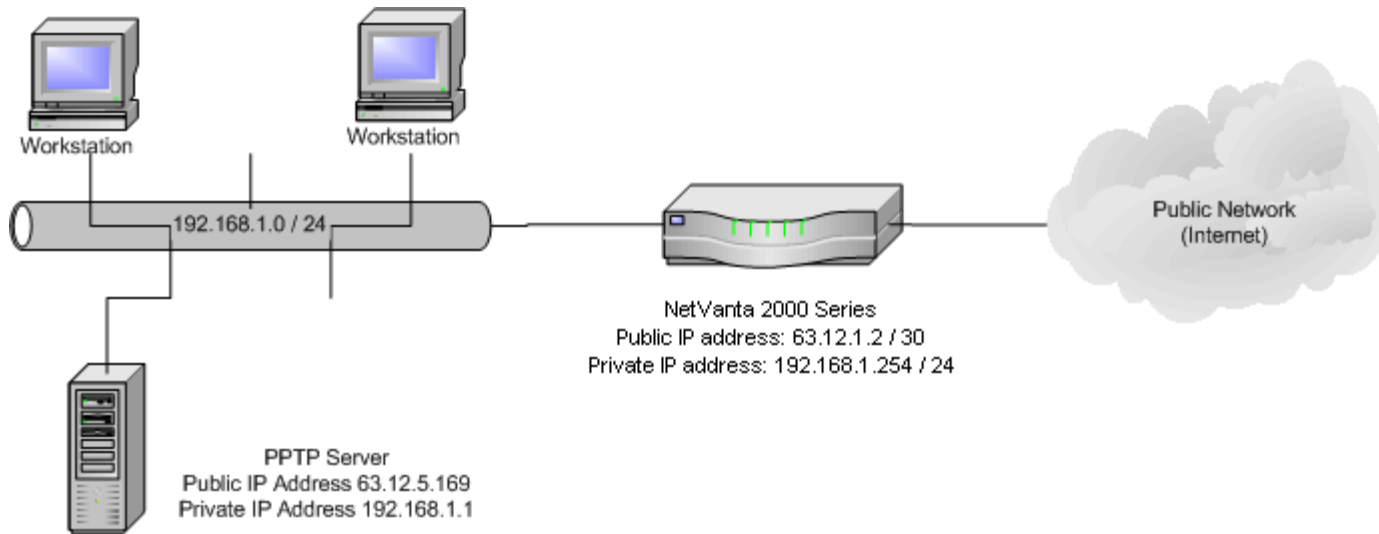


Figure 1 PPTP through NAT

1. First you must turn on the firewall by going into the global config menu and issuing the **ip firewall** command.
2. In the sample configuration we have created a couple of access lists. The first one, named **MATCHALL**, is to allow any traffic from our "Private Network" to access the "Public Network". The second, an extended access list named **PPTP**, is to allow traffic destined for TCP port 1723 and IP protocol GRE from any address on the public network to the address 63.12.5.169.
3. Since we want to use a public IP address for the PPTP server that is different than the NetVanta's WAN IP address, we must tell the NetVanta to respond for that address as well. In this case we need to enter the eth 0/1 interface config mode, and issue the **ip address 63.12.5.169 255.255.255.255 secondary** command.
4. The next step will be to create the needed Policy Classes. The Policy Classes decide whether to permit, deny, or NAT the packets that match the access-lists. The Access Lists are executed in a top down order inside the policy class. In the above example we have 2 Policy Classes. The first is named **PRIVATE**. It is configured to NAT the private source address 192.168.1.1 of the server (access list named **SERVER**) to the secondary public address added in the previous step (65.12.5.169). It is also configured to NAT the remaining packets (access list named **MATCHALL**) to the public address of 63.12.1.2 and enable overloading, creating a Many-to-One NAT policy. The other needed policy class for this example is named **PUBLIC**. The statement in this policy class will NAT the destination address of packets coming from the public network that match the list **PPTP** (65.12.5.169 TCP port 1723 and IP protocol GRE) to the private address of the server (192.168.1.1).

5. Now we must apply these Policy-classes to the appropriate interfaces. This is done by going into the interface config such as eth 0/1 and then adding the **access-policy** command followed by the name of the Policy-class you are invoking. This tells the NetVanta which Policy-class to use on this interface. In this example we have applied the access-policy **PRIVATE** to the ethernet 0/2 interface and the access-policy **PUBLIC** to the ethernet 0/1 interface.

Here's the PPTP through NAT configuration.

```
ip firewall
!
interface eth 0/1
ip address 63.12.1.2 255.255.255.252
ip address 63.12.5.169 255.255.255.255 secondary
access-policy PUBLIC
! – Tell the NetVanta to respond for the 63.12.5.169 address and
assign the WAN
! -- to the Access-Policy-Class "PUBLIC".
!
interface eth 0/2
ip address 192.168.1.254 255.255.255.0
access-policy PRIVATE
! – Assign the LAN to the Access-Policy-Class "PRIVATE".
!
ip route 0.0.0.0 0.0.0.0 63.12.1.1
!
ip access-list standard MATCHALL
permit any
!
ip access-list extended PPTP
permit tcp any host 63.12.5.169 eq 1723
permit gre any host 63.12.5.169
! – Create Extended Access-List "PPTP"
! – Permit any TCP port 1721 and GRE traffic with a destination
address of 63.12.5.169.
!
ip access-list standard SERVER
permit host 192.168.1.1
! – Create Standard Access-List "SERVER"
! – Permit any IP traffic with a source address of 192.168.1.1
!
ip policy-class PRIVATE
nat source list SERVER address 63.12.5.169
nat source list MATCHALL address 63.12.1.2 overload
! – Enable NAT for traffic that matches Access-List "SERVER"
and change
! -- the source address to 63.12.5.169
```

```
! – Enable NAT for traffic that matches Access-List "MATCHALL"
and change
! -- the source address to 63.12.1.2
!
ip policy-class PUBLIC
nat destination list PPTP address 192.168.1.1
! – Enable NAT for traffic that matches Access-List "PPTP" and
change
! -- the destination address 192.168.1.1
!
```

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.