6

Configuring Network Address Translation

Contents

NAT Services on the ProCurve Secure Router

When you enable the ProCurve Secure Router OS firewall, you can configure it to perform Network Address Translation (NAT) on traffic exchanged between the internal, trusted network and the untrusted, public network. Using NAT allows you to maintain private IP addresses on your network while providing Internet access to your company's users. It also adds another layer of security by concealing the actual IP addresses of devices on your network from all Internet users—including hackers.

The Secure Router OS firewall supports NAT for both source IP addresses and destination IP addresses. Specifically, it supports:

- many-to-one NAT for outbound traffic
- one-to-one NAT for inbound traffic

Many-to-One NAT for Outbound Traffic

Based on the *source* IP address, many-to-one NAT for outbound traffic is the most common implementation of NAT. Many companies have only one public IP address, but have many employees who need Internet access. With NAT, all these employees can share one IP address. When users on a company's internal network send requests to the Internet, the Secure Router OS firewall translates the senders' private IP addresses to the company's one public IP address—thus, the designation many-to-one. After translating packets' source IP addresses, the Secure Router OS firewall forwards the requests onto the Internet. (See Figure 6-1.)

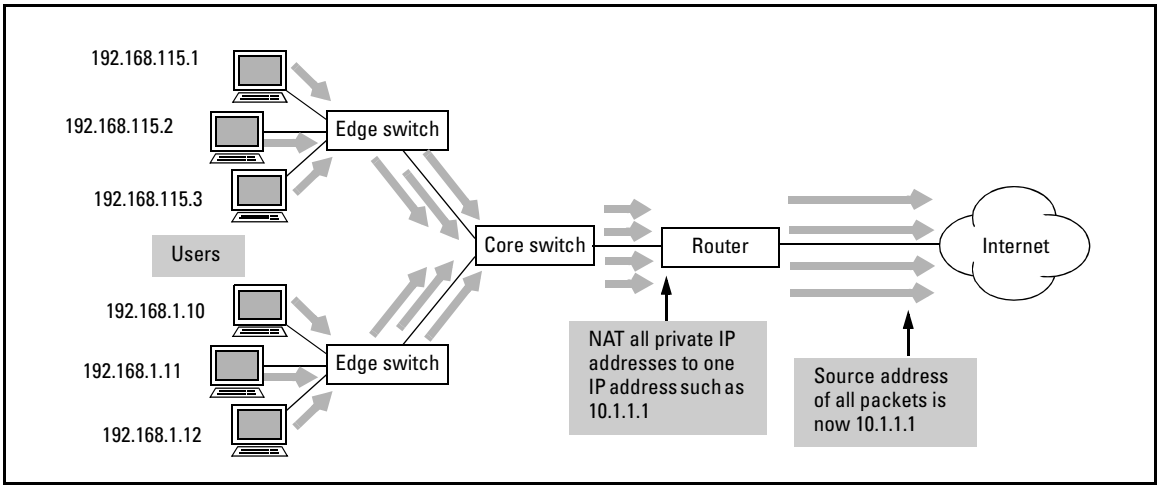

Figure 6-1. Many-to-One NAT

In addition to using NAT to translate private IP addresses to public IP addresses, companies can use NAT to connect two private networks that have conflicting IP addresses. For example, when two companies merge, the IT staff may discover that the two companies are using overlapping IP addresses that will cause conflicts when the companies' networks are combined. By using the ProCurve Secure Router to act as a NAT agent between the two networks, the companies can eliminate the address conflicts.

Using NAT with PAT

To enable multiple users to share one IP address, the ProCurve Secure Router uses port address translation (PAT) in conjunction with NAT. When the router translates a private IP address to the public IP address, it assigns each private IP address a unique port number. The router records this port number in its port-mapping table, which maps the internal address to the new public IP address.

The port-mapping table contains the user's private IP address, the translated public IP address, the source port, and the translated source port. This table also contains the destination address and port for the external device with which the internal user establishes a session. Table 6-1 shows the type of information that is recorded in the port-mapping table.

Table 6-1. Information Recorded in a Port-Mapping Table for a Sample Network

Private IP Address	Translated Public IP Address	Translated Port	Destination IP Address	Destination Port
192.168.1.10	10.1.1.1	4000	10.20.1.1	80
192.168.1.11	10.1.1.1	4001	172.16.1.10	80
192.168.1.12	10.1.1.1	4002	172.16.10.5	80
192.168.1.13	10.1.1.1	4003	10.45.16.1	80
192.168.1.14	10.1.1.1	4004	172.16.11.1	80

When the destination device sends a reply packet back through the router, it sends it to the public IP address on the translated port. The Secure Router OS firewall uses the port-mapping table to identify the original, private IP address. It translates the destination IP address to the private IP address and sends the reply back to the appropriate device on the trusted network.

For example, if the 192.168.1.10 device listed in Table 6-1 sends a packet to a device with the destination IP address of 10.20.1.1, the Secure Router OS receives the packet and records the source IP address. It then changes the IP source address to 10.1.1.1 with the port 4000 and sends the packet to the destination IP address 10.20.1.1.

When the 10.20.1.1 device replies, the Secure Router OS translates the destination IP address from 10.1.1.1 with the port 4000 to 192.168.1.10 and then forwards the packet to that device. (See Figure 6-2.)

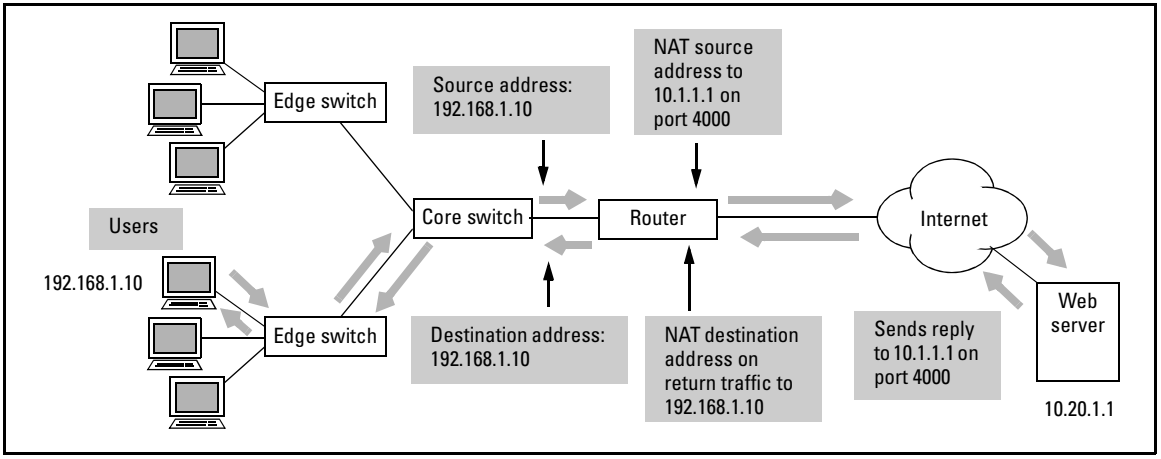

Figure 6-2. Secure Router OS NAT Replies

One-to-One NAT for Inbound Traffic

The Secure Router OS firewall performs one-to-one NAT on inbound traffic—traffic being transmitted from the outside, public network to a device on the internal, trusted network. In this case, NAT is based on the inside *destination* IP address.

One-to-one NAT provides translation between a specific local address on the internal, trusted network and a specific public address that is advertised on the outside, public network. When the ProCurve Secure Router receives a packet with a destination address that is the public IP address, the router translates the destination IP address, changing it to the private address. The router then forwards the packet to the internal network.

Companies use one-to-one NAT when a device is located on the internal, trusted network but must be accessed by clients on the Internet. For example, a company may have a Web server or an FTP server, which is housed on the company's internal network. To access this server, Internet users enter a URL, which is resolved (through a Domain Name System [DNS] server) to a public IP address. The Secure Router OS firewall uses NAT to translate this public IP address to a private IP address on the company's internal network.

In Figure 6-3, a Web server on the internal network has an IP address of 192.168.1.2. However, the IP address that is advertised for that Web server on the Internet is 10.10.10.1. When an Internet client sends a request to that Web server, the destination address is 10.10.10.1.

When the ProCurve Secure Router receives packets with the destination address of 10.10.10.1, it translates the destination address to the private IP address of the Web server: 192.168.1.2. The source IP address is not affected.

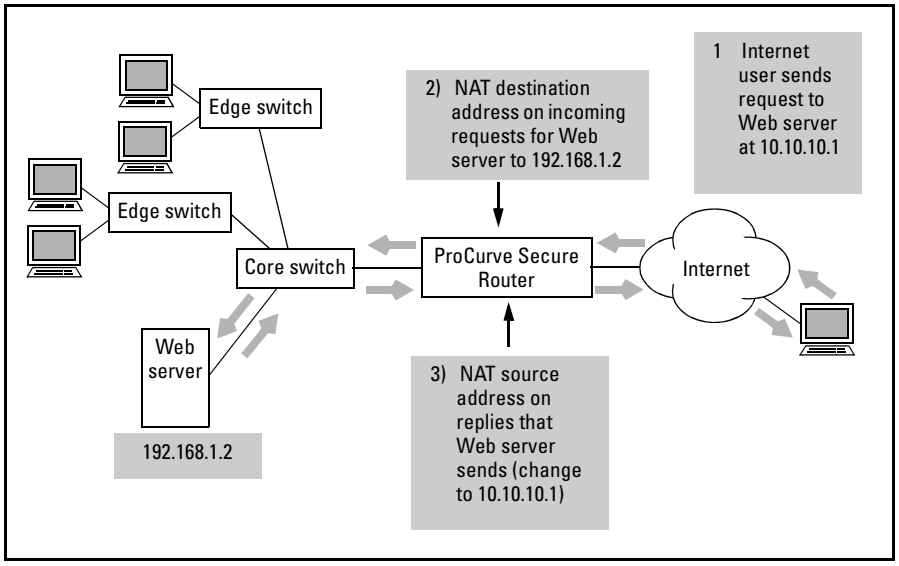

Figure 6-3. One-to-One NAT for Inbound Traffic

Again, the Secure Router OS firewall records information about the packets it NATs in its port-mapping table. When the internal server replies to a request, the Secure Router OS firewall changes the packet's source address—the server's private IP address—to the server's public IP address.

For example, when the Web server shown in Figure 6-3 sends replies to clients, the return packets have the source address of 192.168.1.2—the Web server's private IP address. To conceal this address from Internet users, the Secure Router OS firewall NATs the source address, changing it from 192.168.1.2 to 10.10.10.1.

One-to-One NAT with Port Translation

The Secure Router OS firewall also supports port translation for one-to-one NAT. With port translation, the Secure Router OS firewall can forward traffic to a device on the internal network using the port you specify.

Port translation allows two or more devices on the internal network to share one IP address. For example, the Secure Router OS firewall can translate the destination IP addresses of all traffic destined to port 80 to one private IP address, and it can translate the destination IP addresses of all traffic destined to port 21 to another private address. When the Secure Router OS firewall

translates the public IP address to the private IP address, it can also perform port translation, assigning the traffic to the particular port used by the internal device. (See Figure 6-4.)

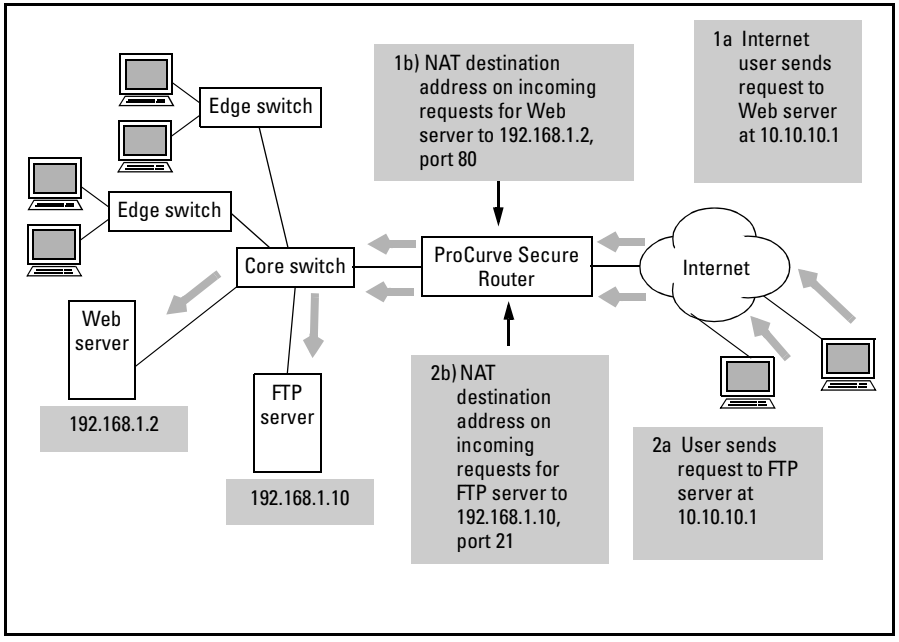

Figure 6-4. One-to-One NAT with Port Translation

Configuring NAT

Configuring NAT is a four-step process—the steps required to configure an access control policy (ACP):

1. Enable the firewall on the ProCurve Secure Router.
2. Configure at least one access control list (ACL).
3. Configure the ACP.
4. Assign the ACP to specific interfaces.

For detailed information about configuring ACLs and ACPs, see *Chapter 5: Applying Access Control to Router Interfaces*.

Enabling the Firewall

You enable the firewall by entering the following command from the global configuration mode context:

```
ProCurve(config)# ip firewall
```

When you assign an ACP to an interface, that ACP will take effect only if the firewall is enabled.

Configuring an ACL

You configure an ACL to select the traffic that you want the Secure Router OS firewall to NAT. ACLs are composed of an ordered list of entries, and each entry contains two parts:

- an action
- a packet pattern

Action. You can define one of two actions:

- permit
- deny

When you create ACLs that are used in ACPs, the permit and deny actions take on new meanings. Permit means that the traffic is selected for the action specified in the ACP entry. You should create a permit entry for the traffic that you want to NAT.

Deny means that the traffic is excluded from the action specified in the ACP entry. If you do not want to NAT certain traffic, you should create a deny entry. If a packet matches a deny entry, the Secure Router OS will stop processing that particular ACL and the related ACP entry and move to the next entry in the ACP (if there is another entry). (For more information about how ACLs are processed when they are used in combination with ACPs, see *Chapter 5: Applying Access Control to Router Interfaces*.)

Packet Pattern. You can define patterns based on:

- source IP address
- source and destination IP addresses
- protocol
- for TCP and UDP packets, source and destination port

Types of ACLs

The Secure Router OS firewall supports two types of ACLs:

- standard
- extended

If you want to define patterns based solely on source address, you should configure a standard ACL. If you want to define patterns based on source and destination addresses and on other fields in the IP, TCP, or UDP header, you should create an extended ACL. You must create an extended ACL for one-to-one NAT.

You can create a standard ACL or an extended ACL by entering this command from the global configuration mode context:

Syntax: ip access-list [standard | extended] <*listname*>

Replace ***<listname>*** with the name you want to assign to the ACL.

Configuring a Standard ACL for Many-to-One NAT. When you configure many-to-one NAT, you should create a standard ACL to select the traffic that the ProCurve Secure Router will NAT. For example, to create a standard ACL called Inside, enter:

```
ProCurve(config)# ip access-list standard Inside
```

You can then use the following command to select the traffic that you want to NAT:

Syntax: [permit | deny] [any | host <*A.B.C.D*> | hostname <*hostname*> | <*A.B.C.D*> <*wildcard bits*>]

Table 6-2 lists the options for specifying a source address.

Table 6-2. Options for Specifying Source Address

Option	Meaning
any	match all hosts
host <A.B.C.D>	specify a single host
host <hostname>	specify a single host
<A.B.C.D>	specify a single IP address
<A.B.C.D> <wildcard bits>	specify a range of IP addresses

For example, if you want to NAT all traffic that enters through the Ethernet interface, you create this permit entry in the ACL:

ProCurve(config-std-nacl)# permit any

If you want to NAT a subnet, enter:

ProCurve(config-std-nacl)# permit <*A.B.C.D*> <*wildcard bits*>

Replace ***<A.B.C.D>*** with the IP address of the subnet and use wildcard bits to define the number of hosts in the subnet. Wildcard bits define which address bits the Secure Router OS firewall should match and which address bits it should ignore. Although wildcard bits resemble subnet masks, they use reverse logic.

With wildcard bits, 0 means that you want the Secure Router OS firewall to match that bit; 1 means that you do not want the Secure Router OS firewall to match that bit.

For example, you might enter:

ProCurve(config-std-nacl)# deny 192.168.115.0 0.0.0.31

If you enter 192.168.115.0 with the wildcard bits 0.0.0.31, the Secure Router OS firewall will not match the last five address bits in the fourth octet. The firewall will match all hosts with addresses between 192.168.115.1 and 192.168.115.31 to the deny entry. If you enter **permit 192.168.115.0 0.0.0.255**, the Secure Router OS firewall will not match any address bits in the last octet. This entry selects all hosts in the 192.168.115.0 /24 network.

Configuring an Extended ACL for One-to-One NAT. When you configure one-to-one NAT, you must create an extended ACL to define the public destination address that the ProCurve Secure Router will NAT to a private IP on the internal network. For example, to create an extended ACL called Outside, enter:

```
ProCurve(config)# ip access-list extended Outside
```

You can then use the following command to create the permit and deny entries that select the traffic for NAT:

Syntax: [permit | deny] <*protocol*> <*source address*> <*source port*> <*destination address*> <*destination port*>

Replace ***<protocol>*** with one of the following:

- **icmp**
- **ip**
- **tcp**
- **udp**
- **ahp**
- **esp**
- **gre**

You can also specify a port number between 0 and 255.

To specify a source address or destination address, you use the following syntax:

Syntax: [any | host <*A.B.C.D*> | hostname <*hostname*> | <*A.B.C.D*> <*wildcard bits*>]

Table 6-3 shows the options for specifying source and destination addresses.

Table 6-3. Options for Specifying Source and Destination Addresses

Option	Meaning
any	match all hosts
host <A.B.C.D>	specify a single host or a single IP address
hostname <hostname>	specify a single host by name rather than by IP address
<A.B.C.D> <wildcard bits>	specify a range of IP addresses

For example, if you want to select all the traffic destined for IP address 10.1.1.10, enter:

```
ProCurve(config-ext-nacl)# permit ip any host 10.1.1.10
```

If you select UDP or TCP as the protocol, you can also specify a source or destination port (although you do not have to). For example, if you want to configure one-to-one NAT for multiple devices, you should include a destination port as part of the criteria used to select traffic.

Table 6-4 shows the options you have for defining ports when you select UDP or TCP as the protocol.

Table 6-4. Specifying Ports in Extended ACLs

Option	Explanation
eq <port number>	specific port
gt <port number>	all ports that are a larger number than the port number you specify (*not* including the specified port)
lt <port number>	all ports that are a smaller number than the port number you specify (*not* including the specified port)
range <first port number last port number>	range of ports
neq <port number>	all ports except the port number you specify

When you finish configuring the ACL, enter **exit** to return to the global configuration mode context where you can configure the ACP.

Configuring an Extended ACL for Many-to-One NAT. You can also configure an extended ACL for many-to-one NAT. You may need to use this option if your router provides both an Internet connection and a connection to a remote private network. If you do not want the Secure Router OS firewall to NAT traffic sent to the remote private network, complete these steps:

1. Create the extended ACL.

   Syntax: ip access-list extended <*listname*>

2. Deny traffic destined to the remote private network.

   Syntax: deny <*protocol*> <*source address*> <*source port*> <*destination address*> <*destination port*>

   For example, enter:

   ProCurve(config-ext-nacl)# deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

3. Enter a permit entry to select all other traffic for NAT.

   Syntax: deny <*protocol*> <*source address*> [<*source port*>] <*destination address*> [<*destination port*>]

   Use the **any** option for the destination. For example, enter:

   ProCurve(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 any

4. Configure a second ACL to select the traffic to the remote private network. When you configure the ACP, create a NAT entry for the first ACL and another entry to allow second ACL.

Configuring an ACP

After you create the ACL that will select the traffic that you want to NAT, you must create the ACP. In the ACP, you define the action that the Secure Router OS firewall will take on the selected traffic. Specifically, you specify how the Secure Router OS will NAT the traffic—based on source address or based on destination address.

To create an ACP, enter the following command from the global configuration mode context:

Syntax: ip policy-class <*policyname*>

Replace ***<policyname>*** with a name that is meaningful to you. This name can be a maximum of 255 alphanumeric characters.

For example, to create an ACP called NATInside, enter:

```
ProCurve(config)# ip policy-class NATInside
```

The router prompt shows that you are at the policy class configuration mode context:

```
ProCurve(config-policy-class)#
```

Configuring Many-to-One NAT for Outbound Traffic

When you configure many-to-one NAT, you base NAT on the source IP address. From the policy-class configuration mode context, enter:

Syntax: nat source list <*listname*> [address <*A.B.C.D*> | interface <*interface*>] overload

Replace ***<listname>*** with the name of the ACL that selects the traffic that you want to NAT. For example, you may have created an ACL called MatchAll.

You have two options for specifying the public IP address. You can use the **address <*A.B.C.D*>** option to specify a particular IP address, or you can use the **interface <*interface*>** option to specify a particular interface. If you use the **interface** option, the Secure Router OS will NAT the traffic selected by the ACL to the IP address assigned to that interface.

You must include the **overload** keyword to enable many devices to share one IP address.

For example, to configure the Secure Router OS firewall to NAT all traffic selected by the MatchAll ACL to the IP address 10.10.1.1, enter:

```
ProCurve(config-policy-class)# nat source list MatchAll address 10.10.1.1 overload
```

After you configure the ACP, you must assign it to an interface, or it will have no affect on the traffic entering the router. This step is described in "Assigning the ACP to an Interface" on page 6-16.

Configuring One-to-One NAT for Inbound Traffic

To configure one-to-one NAT for inbound traffic, you base NAT on the destination IP address. From the policy-class configuration mode context, enter:

Syntax: nat destination list <*listname*> address <*A.B.C.D*>

Replace ***<listname>*** with the name of the ACL that selects traffic for one-to-one NAT, and replace ***<A.B.C.D>*** with the public destination IP address. Because this is one-to-one NAT, you do not include the **overload** keyword.

For example, to configure the Secure Router OS firewall to NAT all traffic selected by the Outside ACL to the IP address 192.168.1.10, enter:

```
ProCurve(config-policy-class)# nat destination list Outside address 192.168.1.10
```

Configuring One-to-One NAT with Port Translation

To configure one-to-one NAT with port translation, you base NAT on the destination IP address. From the policy class configuration mode context, enter:

Syntax: nat destination list <*listname*> address <*A.B.C.D*> port <1-65525>

For example, if you have two servers on your internal network that must share a public IP address, you can configure ACLs to base one-to-one NAT on the destination address and the destination port.

You first create an extended ACL to select traffic inbound to the public IP address and a specific port. In this example, the ACL is called Webserver:

```
ProCurve(config)# ip access-list extended Webserver
```

You then create a permit entry to select traffic from any device that is destined for the public IP address on port 80, the well-known port for HTTP traffic.

```
ProCurve(config-ext-nacl)# permit tcp any host 10.1.10.1 eq 80
ProCurve(config-ext-nacl)# exit
```

You then create a second ACL called FTPserver, to select traffic from any device that is destined for the public IP address (in this example, 10.1.10.1) on port 21, the well-known port for FTP traffic.

```
ProCurve(config)# ip access-list extended FTPServer
ProCurve(config-ext-nacl)# permit tcp any host 10.1.10.1 eq 21
ProCurve(config-ext-nacl)# exit
```

Next, you create an ACP with two entries: one for the Web server and one for the FTP server. Traffic selected by the Webserver ACL is assigned the destination IP address of 192.168.2.11, the actual IP address of the Web server on the internal network. When configuring the ACP, you include the **port** option so that the traffic continues to be transmitted on port 80. Traffic selected by FTPserver ACL is assigned the destination IP address of 192.168.2.12, the actual IP address of the FTP server on the internal network. Again, you include the port number for FTP, port 21.

```
ProCurve(config)# ip policy-class NATservers
ProCurve(config-policy-class)# nat destination list Webserver address 192.168.2.11
port 80
ProCurve(config-policy-class)# nat destination list FTPServer address 192.168.2.12
port 21
ProCurve(config-policy-class)# exit
```

Assigning the ACP to an Interface

The ACP you configure will have no effect until you assign it to an active interface. After you assign the ACP to an interface, the Secure Router OS firewall will use it to NAT traffic arriving on the interface. Traffic sent from the interface will not be affected.

To assign the ACP to a particular interface, you must move to the configuration mode context for that interface and enter:

Syntax: access-policy <*policyname*>

For example, to assign the NATInside ACP to the Ethernet 0/1 interface, enter:

```
ProCurve(config)# interface eth 0/1
ProCurve(config-eth 0/1)# access-policy NATInside
```

Viewing ACLs and ACPs

After you configure NAT on the ProCurve Secure Router, you can use **show** commands to:

- view ACLs configured to select the traffic for NAT
- view NAT entries in ACPs
- display information about connections associated with particular ACPs

The **show** commands related to ACLs and ACPs are listed in Table 6-5.

Table 6-5. show Commands for ACLs and ACPs

Command	Explanation
show access-lists	displays all of the ACLs configured on the ProCurve Secure Router
show ip access-lists	displays all of the IP-based ACLs configured on the ProCurve Secure Router
show ip policy-class	displays all of the ACPs configured on the ProCurve Secure Router
show ip policy-sessions	displays the total number of sessions (connections) associated with ACPs, the number of sessions per ACP, and detailed information about each device that has established a session
show ip policy-sessions [all | <policyname>]	displays all of the sessions or the sessions associated with the specific ACP and detailed information about each device that has established a session
show ip policy-stats	displays information related to ACPs, such as the number of current sessions and the maximum number of sessions allowed

Note

You enter **show** commands from the enable mode context. If you are in a different context (other than the basic mode context), you can use the **do** command. For example:

```
ProCurve(config)# do show ip access-lists
```

Displaying ACLs

To view all of the ACLs that are configured on the ProCurve Secure Router, move to the enable mode context and enter:

```
ProCurve# show access-lists
```

As Figure 6-5 shows, this command lists the following information for each ACL:

- type of ACL—standard or extended
- all entries in the ACLs
- number of matches for each entry

```
ProCurve# show access-lists
Extended IP access list Internet
    permit tcp any  any eq www  (300 matches)
    permit tcp any  any eq smtp  (1 matches)
    permit tcp any  any eq pop3  (0 matches)
    permit tcp any  any eq ftp  (0 matches)
    permit tcp any  any eq ftp-data (0 matches)
    permit tcp any  any eq domain  (0 matches)
    remark ACL for traffic destined to the Internet
Extended IP access list Webserver
    permit tcp any  10.1.1.1 eq www   (42 matches)
    remark ACL for traffic to internal Web server
```

Figure 6-5. Displaying All the ACLs Configured on the Router

You can use this information to review the ACLs that are configured and to ensure that they are configured correctly.

Displaying ACPs

To view all of the ACPs that are configured on the ProCurve Secure Router, move to the enable mode context and enter:

```
ProCurve# show ip policy-class
```

```
ProCurve# show ip policy-class
Policy-class "Inside":
  Entry 1 - nat source list Internet address 10.1.1.1 overload
Policy-class "Outside":
  Entry 1 - allow list Region
  Entry 2 - nat destination list Webserver address 192.168.2.11
  Entry 3 - nat destination list FTPserver address 192.168.2.12
```

Figure 6-6. Displaying All the ACPs Configured on the Router

As Figure 6-6 shows, entries for each ACP are displayed in the order in which they will be implemented. When an ACP is not enforcing your policies in the way you expected, you may have entered commands in the wrong order.

For example, if you have included an entry to NAT an entire subnet before an entry to deny specific hosts on that subnet, the Secure Router OS firewall will match all packets from the subnet to the NAT entry. The firewall will NAT and forward the packets, and the deny entry will not take effect.

Viewing Access Policy Sessions

After you enable the firewall and assign an ACP to an interface, the Secure Router OS firewall checks all the packets entering that interface. When traffic matches a permit statement in an ACP, the ProCurve Secure Router records information about the session established between the packet's source and destination. To view this information, move to the enable mode context and enter:

```
ProCurve# show ip policy-sessions
```

The Secure Router OS lists each ACP (policy class) by name. Under a specific policy, you can view the traffic that matched this policy as it arrived on the interface. You can also view information about the traffic, such as:

- source IP address
- source port
- destination IP address
- destination port

If the traffic has been manipulated using NAT, the NAT IP address and port are also listed. (See Figure 6-7.)

```
ProCurve# show ip policy-sessions
Src IP Address     Src Port    Dest IP Address    Dst Port    NAT IP Address   NAT Port
---------------   ---------   --------------    --------   ---------------  -------

Policy class "Inside":
tcp (80)
  192.168.20.1     2001        172.16.1.1          80       d 10.10.3.10      80

Policy class "Outside":
tcp (20)
  192.168.100.99   1908        172.16.3.10         80       d 10.10.3.10      80

Policy class "self":
icmp (50)
  0.0.0.0          10         192.168.100.1       10
```

Figure 6-7. Displaying IP Policy Sessions

If you want to view information about the sessions associated with a specific ACP, enter:

ProCurve# show ip policy-sessions <*policyname*>

Replace ***<policyname>*** with the name of the specific ACL.

Viewing Access Policy Statistics

You can also display a summary of ACP statistics by entering the following command from the enable mode context:

ProCurve# show ip policy-stats

The Secure Router OS displays the total number of current sessions. (See Figure 6-8.) It also lists all ACPs assigned to interfaces and the entries of each ACP. It displays:

- the number of sessions established using each ACP (policy class)
- the number of maximum sessions allowed for that ACP
- the number of hits for each entry in the ACP
- the number of bytes for traffic associated with a particular ACP entry

```
ProCurve# show ip policy-stats
Global 0 current sessions (255300 max)
Policy-class "Inside":
  121 current sessions (85100 max)
  Entry 1 - allow list MatchAll
     1424221 in bytes, 14222323 out bytes, 123 hits

Policy-class "Outside":
 554 current sessions (85100 max)
  Entry 1 - allow list Region
      2345352 in bytes, 56363536 out bytes, 554 hits

  Entry 2 - allow list InWeb
      0 in bytes, 0 out bytes, 0 hits

  Entry 2 - discard list MatchAll
      0 in bytes, 0 out bytes, 0 hits
```

Figure 6-8. Displaying IP Policy-Stats

Troubleshooting

In addition to using **show** commands to view information about ACLs and ACPs and to verify that your configuration is correct, you can use these commands for troubleshooting. For example, suppose that several users call you, complaining that they cannot send traffic to the Internet. However, the PPP 1 interface, which provides the Internet connection, is up, and other users are successfully sending traffic across the interface. You can use the **show ip policy-sessions** command to determine whether or not the traffic is being blocked by an ACP. You can then change the appropriate ACP as required.

Monitoring Packets Matched to an ACP

The Secure Router OS firewall tracks the number of connections made using each ACP configured on the router. By default, the firewall generates a log message after it creates 100 sessions (connections) using an ACP.

You can customize the number of connections made before a log message is generated. For example, you may want to be notified when 50 connections are made. If you have a large network, on the other hand, you may want to be notified when 200 connections are made. To change the default setting, move to the global configuration mode context and enter:

Syntax: ip firewall policy-log threshold <*connections*>

You can specify a number between 0 and 4294967295.

Clearing Existing Policy Sessions

Whenever you change your ACP configurations, you are prompted to clear the existing sessions. This enables you to apply your new configurations. Otherwise, an existing session may violate an ACP that you just configured.

To clear all of the policy sessions on the router, move to the enable mode context and enter:

```
ProCurve# clear ip policy-sessions
```

You can also clear a particular policy session. For example, if you enter the **show ip policy-sessions** command and determine that an existing session should be terminated, you can use one of the following commands to do so:

Syntax: clear ip policy-sessions <*policyname*> [ahp | esp | gre | icmp | tcp | udp | <*protocol number*>] <*source A.B.C.D*> <*source port*> <*destination A.B.C.D*> <*destination port*>

or

Syntax: clear ip policy-sessions <*policyname*> [ahp | esp | gre | icmp | tcp | udp | <*protocol number*>] <*source A.B.C.D*> <*source port*> <*destination A.B.C.D*> <*destination port*> [destination | source] <*nat A.B.C.D*> <*nat port*>

Enter the command as follows:

- Replace ***<policyname>*** with the name of the policy class (or ACP) associated with that IP policy session.
- Specify the protocol: **ahp**, **esp**, **gre**, **icmp**, **tcp**, **udp**, or a protocol number between 0 and 255.
- Replace ***<source A.B.C.D>*** with the source IP address.
- Replace ***<source port>*** with the port specified by the source. Use hexadecimal format for AHP, ESP, and GRE; use the decimal for all other protocols.
- Replace ***<destination A.B.C.D>*** with the destination IP address.
- Replace ***<destination port>*** with the destination port. Use hexadecimal format for AHP, ESP, and GRE; use decimal format for all other protocols.

The remaining options apply only to NAT:

- Include the **destination** option to select a session that uses one-to-one NAT (NAT based on the destination address). Include the **source** option to select a session that uses many-to-one NAT (NAT based on the source IP address).
- Replace ***<nat A.B.C.D>*** with the IP address that replaced the original IP address.
- Replace ***<nat port>*** with the port used by NAT. Use hexadecimal format for AHP, ESP, and GRE; use decimal format for all other protocols.

Note Rather than input this entire command, you can enter the **show ip policy-sessions** command to display the current sessions and then copy the second part of the command, beginning with the source IP address, from the display. (See Figure 6-9.)

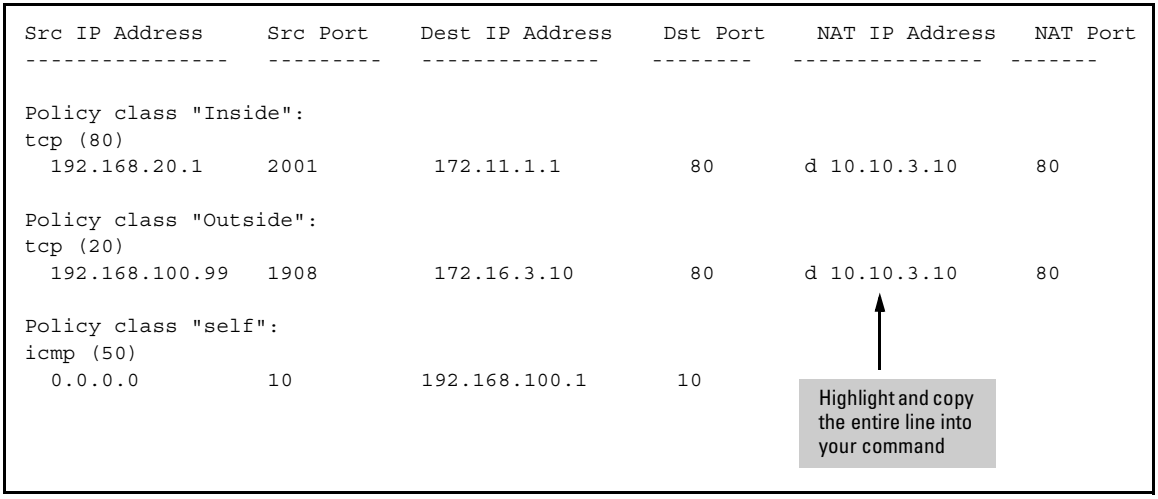

Figure 6-9. Using the Information from the show ip policy-sessions Command to Clear a Specific Session

Clearing ACL Counters

Clearing ACL counters helps you to troubleshoot and isolate problems with the ACLs that are configured on a router. When you clear the counters, the Secure Router OS resets the number of matches to every ACL entries. You can then reproduce a problem and check the number of matches for a particular entry to determine whether the ACL is selecting traffic correctly. To clear ACL counters, enter this command from the enable mode context:

Syntax: clear access-list [<*listname*>]

If you want to clear all counters, enter:

ProCurve# clear access-list

If you want to clear counters for a particular ACL, use the ***<listname>*** option:

ProCurve# clear access-list <*listname*>

For example, if you want to clear the counters for the Inside ACL, enter:

ProCurve# clear access-list Inside

Debugging ACLs

You can debug events associated with a particular ACL. From the enable mode context, enter:

Syntax: debug access-list <*listname*>

Replace ***<listname>*** with the name of the ACL you want to debug.

For example, if you want to debug the Inside ACL, enter:

ProCurve# debug access-list Inside

Messages display dealing with the incoming packets that matches entries in the ACL.

To stop the debug messages, enter the following command:

Syntax: no debug access-list <*listname*>

Quick Start

This "Quick Start" section provides the CLI commands you will need to configure network address translation (NAT) on the ProCurve Secure Router. Only a minimal explanation is provided.

If you need additional information about any of these options, check the "Contents" on page 6-1 to locate the section and page number that contains the explanation you need.

Note

The fastest way to set up basic NAT services on the ProCurve Secure Router is to use firewall wizard in the Web browser interface. For information about using the firewall wizard, see *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks*.

Using the CLI to Configure Many-to-One NAT

Like most organizations, your company probably uses private IP addresses on its internal network. In fact, your company may have only one public IP address. When employees need to access the Internet, a NAT device must change all the private IP addresses to that one public IP address—a process called many-to-one NAT.

To implement many-to-one NAT on the ProCurve Secure Router, you must configure an access control policy (ACP) and apply it to the appropriate interface:

1. From the global configuration mode context, enable the firewall on the ProCurve Secure Router.

   ```
   ProCurve(config)# ip firewall
   ```

2. From the global configuration mode context, create a standard access control list (ACL).

   Syntax: ip access-list standard <*listname*>

   Replace ***<listname>*** with the name you want to assign the ACL.

   For example, to create an ACL called NAT, enter:

   ```
   ProCurve(config)# ip access-list standard NAT
   ```

3. Create entries in the ACL to select the traffic that you want to NAT.

   Syntax: [permit | deny] [any | host <*A.B.C.D*> | hostname <*hostname*> | <*A.B.C.D*> <*wildcard bits*>]

   For example, to NAT all traffic, enter:

   ProCurve(config-std-nacl)# permit any

   To NAT traffic from subnet 192.168.115.0 /24, use wildcard bits to specify a range of IP addresses.

   ProCurve(config-std-nacl)# permit 192.168.115.0 0.0.0.255

4. Exit the ACL to return to the global configuration mode context.

   ProCurve(config-std-nacl)# exit

5. Create an ACP.

   Syntax: ip policy-class <*policyname*>

   Replace ***<policyname>*** with a name that is a maximum of 255 alphanumeric characters. For example, to create a policy called NATInside, enter:

   ProCurve(config)# ip policy-class NATInside

6. Create a NAT entry based on the source IP address.

   Syntax: nat source list <*listname*> [address <*A.B.C.D*> | interface <*interface*>] overload

   Replace ***<listname>*** with the ACL you created.

   You have two options for specifying the public IP address. You can use the **address *<A.B.C.D>*** option to specify a particular IP address, or you can use the **interface *<interface>*** option to specify a particular interface. If you use the **interface** option, the Secure Router OS will NAT the traffic selected by the ACL to the IP address assigned to that interface.

   Replace ***<A.B.C.D>*** with your company's public IP address.

   Use the **overload** keyword to replace multiple source IP addresses with one IP address.

   For example, to NAT the traffic that you specified in the NAT ACL to the IP address 10.1.1.1, enter:

   ProCurve(config-policy-class)# nat source list NAT address 10.1.1.1 overload

7. Return to the global configuration mode context.

   ProCurve(config-policy-class)# exit

8. To apply the ACP to an interface, move to the configuration mode context for that interface.

   Syntax: interface <*interface*> <*number*>

   Valid interfaces include PPP interfaces, Frame Relay subinterfaces, ATM subinterfaces, HDLC, Ethernet interfaces, and demand interfaces. (If you have enabled support for virtual LANs [VLANs], you must apply the ACP to an Ethernet subinterface.)

9. Apply the ACP to the interface by entering the following command from the appropriate interface configuration mode context:

   Syntax: access-policy <*policyname*>

   For example, if you want to apply the NATInside ACP to the Ethernet 0/1 interface, enter:

   ```
   ProCurve(config-eth 0/1)# access-policy NATInside
   ```

Using the CLI to Configure One-to-One NAT

Unlike many-to-one NAT, one-to-one NAT is based on the *destination* IP address of *inbound* traffic. One-to-one NAT is used when a host, such as an FTP server or a Web server, is located on the internal, trusted network but must be accessed by clients on the Internet.

To access this server, Internet users enter a URL, which is resolved (through DNS) to a public IP address. However, this IP address is not the IP address that the server is using on the internal network. The Secure Router OS firewall uses NAT to translate the public IP address to the server's internal IP address.

To implement one-to-one NAT on the ProCurve Secure Router, you must configure an access control policy (ACP) and apply it to the appropriate interface:

1. From the global configuration mode context, enable the firewall on the ProCurve Secure Router.

   ```
   ProCurve(config)# ip firewall
   ```

2. From the global configuration mode context, create an extended access control list (ACL).

   Syntax: ip access-list extended <*listname*>

   Replace ***<listname>*** with the name you want to assign the ACL.

   For example, to create an ACL called Webserver, enter:

   ```
   ProCurve(config)# ip access-list extended Webserver
   ```

3. Define the traffic that you want to NAT. For example, if you want to NAT all traffic with the destination address of the Web server, enter:

   Syntax: [permit | deny] <*protocol*> [any | host <*A.B.C.D*> | hostname <*hostname*> | <*A.B.C.D*> <*wildcard bits*>] <*source port*> [any | host <*A.B.C.D*> | <*A.B.C.D*> <*wildcard bits*>] <*destination port*>

   For example, to NAT all traffic sent to the IP address 10.1.1.1, enter:

   ```
   ProCurve(config-ext-nacl)# permit ip any host 10.1.1.1
   ```

4. If your company has more than one server that clients on the Internet need to access, you should configure an extended ACL for each server. Use the ***<destination port>*** options to select traffic for a particular server. For example, to select traffic to a Web server, create the extended ACL and enter this permit entry:

   ```
   ProCurve(config-ext-nacl)# permit tcp any host 10.1.1.1 eq 80
   ```

5. Exit the ACL to return to the global configuration mode context.

   ```
   ProCurve(config-ext-nacl)# exit
   ```

6. Create an ACP.

   Syntax: ip policy-class <*policyname*>

   Replace ***<policyname>*** with a name that is a maximum of 255 alphanumeric characters. For example, to create a policy called NATWeb, enter:

   ```
   ProCurve(config)# ip policy-class NATWeb
   ```

7. Create a NAT entry based on the destination IP address.

   Syntax: nat destination list <*listname*> address <*A.B.C.D*> [port <1-65525>]

   Replace ***<listname>*** with the ACL you created and replace ***<A.B.C.D>*** with the private IP address of the device. For example, to NAT the traffic that you specified in the Webserver ACL to the private IP address 192.168.115.1, enter:

   ```
   ProCurve(config-policy-class)# nat destination list Webserver address
   192.168.115.1
   ```

   You can use the **port** option to ensure that the Secure Router OS firewall forwards the traffic to the port used by your server.

8. Return to the global configuration mode context.

   ```
   ProCurve(config-policy-class)# exit
   ```

9. To apply the ACP to an interface, move to the configuration mode context for that interface.

   Syntax: interface <*interface*> <*number*>

   Valid interfaces include PPP interface, Frame Relay subinterfaces, ATM subinterfaces, HDLC, Ethernet interfaces, and demand interfaces. (If you have enabled support for virtual LANs [VLANs], you must apply the ACP to an Ethernet subinterface.)

10. Apply the ACP to the interface by entering the following command from the appropriate interface configuration mode context:

    Syntax: access-policy <*policyname*>

    For example, if you want to apply the NATInside ACP to the Ethernet 0/1 interface, enter:

    ```
    ProCurve(config-eth 0/1)# access-policy NATInside
    ```