CHAPTER 5

Configuring Network Address Translation

This chapter describes how to configure Network Address Translation (NAT) on the Cisco 4700 Series Application Control Engine (ACE) appliance. It contains the following major sections:

- Network Address Translation Overview
- Configuring an Idle Timeout for NAT
- Configuring Dynamic NAT and PAT
- Configuring Static NAT and Static Port Redirection
- Displaying NAT Configurations and Statistics
- Clearing Xlates
- NAT Configuration Examples

Network Address Translation Overview

When a client attempts to access a server in a data center, the client incorporates its IP address in the IP header when it connects to the server. An ACE placed between the client and the server can either preserve the client IP address or translate that IP address to a routable address in the server network, based on a pool of reserved dynamic NAT addresses or a static NAT address mapping, and pass the request on to the server.
This IP address translation process is called Network Address Translation (NAT) or source NAT (SNAT). The ACE tracks all SNAT mappings to ensure that response packets from the server are routed back to the client. If your application requires that the client IP address be preserved for statistical or accounting purposes, do not implement SNAT.

Destination NAT (DNAT) translates the IP address and port of an inside host so that it appears with a publicly addressable destination IP address to the rest of the world. Typically, you configure DNAT using static NAT and port redirection. You can use port redirection to configure servers that host a service on a custom port (for example, servers hosting HTTP on port 8080).

To provide security for a server, you can map the server private IP address to a global routable IP address that a client can use to connect to the server. In this case, the ACE translates the global IP address to the server private IP address when sending data from the client to the server. Conversely, when a server responds to a client, the ACE translates the local server IP address to a global IP address for security reasons. This process is called DNAT.

You can also configure the ACE to translate TCP and UDP port numbers greater than 1024, and ICMP identifiers. This process is known as Port Address Translation (PAT). The ACE provides 64 K minus 1 K ports for each IP address for PAT. Ports 0 through 1024 are reserved and cannot be used for PAT.

Some of the benefits of NAT are as follows:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a server in the data center.
- You can resolve IP routing problem, such as overlapping addresses, when you have two interfaces connected to overlapping subnets.

The ACE provides the following types of NAT and PAT:

- Dynamic NAT
- Dynamic PAT
- Static NAT
- Static port redirection
This section contains the following topics:

- Dynamic NAT
- Dynamic PAT
- Static NAT
- Static Port Redirection
- Maximum Number of NAT Statements
- Global Address Guidelines

**Dynamic NAT**

Dynamic NAT, which is typically used for SNAT, translates a group of local source addresses to a pool of global source addresses that are routable on the destination network. The global pool can include fewer addresses than the local group. When a local host accesses the destination network, the ACE assigns an IP address from the global pool to the host.

Because the translation times out after being idle for a user-configurable period of time, a user does not keep the same IP address. For this reason, users on the destination network cannot reliably initiate a connection to a host that uses dynamic NAT (even if the connection is allowed by an access control list [ACL]). Not only can you not predict the global IP address of the host, but the ACE does not create a translation unless the local host is the initiator. See the “Configuring Static NAT and Static Port Redirection” section for details about reliable access to hosts.

---

**Note**

For the duration of the translation, a global host can initiate a connection to the local host if an ACL allows it. Because the address is unpredictable, a connection to the host is unlikely. However, in this case, you can rely on the security of the ACL.

Dynamic NAT has these disadvantages:

- If the global address pool has fewer addresses than the local group, you could run out of addresses if the amount of traffic is greater than expected.

  Use dynamic PAT if this event occurs often, because dynamic PAT provides over 64,000 translations using multiple ports of a single IP address.
If you need to use a large number of routable addresses in the global pool and the destination network requires registered addresses (for example, the Internet), you may encounter a shortage of usable addresses.

The ACE supports a maximum of 4 M SNAT sessions

The advantage of dynamic NAT is that some protocols cannot use dynamic PAT. Dynamic PAT does not work with some applications that have a data stream on one port and the control path on another, such as some multimedia applications.

**Dynamic PAT**

Dynamic PAT, which is also used for SNAT, translates multiple local source addresses and ports to a single global IP address and port that are routable on the destination network from a pool of IP addresses and ports reserved for this purpose. The ACE translates the local address and local port for multiple connections and/or hosts to a single global address and a unique port starting with port numbers greater than 1024.

When a local host connects to the destination network on a given source port, the ACE assigns a global IP address to it and a unique port number. Each host receives the same IP address but, because the source port number is unique, the ACE sends the return traffic, which includes the IP address and port number as the destination, to the correct host.

The ACE supports over 64,000 ports for each unique local IP address. Because the translation is specific to the local address and local port, each connection, which generates a new source port, requires a separate translation. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The translation is valid only for the duration of the connection, so a user does not keep the same global IP address and port number. For this reason, users on the destination network cannot reliably initiate a connection to a host that uses dynamic PAT (even if the connection is allowed by an ACL). Not only can you not predict the local or global port number of the host, but the ACE does not create a translation unless the local host is the initiator. See the “Configuring Static NAT and Static Port Redirection” section for reliable access to hosts.

Dynamic PAT allows you to use a single global address, which helps to conserve routable addresses. Dynamic PAT does not work with some multimedia applications that have a data stream on a port that is different from the control path port.
Static NAT

Static NAT, which is typically used for DNAT, translates each local address to a fixed global address. With dynamic NAT and PAT, each host uses a different address or port after the translation times out. Because the global address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the global network to initiate traffic to a local host (if there is an ACL that allows it).

The main differences between dynamic NAT and static NAT are as follows:

- Static NAT uses a one-to-one correspondence between a local IP address and a fixed global IP address, while dynamic NAT assigns a global IP address from a pool of global addresses.
- With static NAT, you need an equal number of global IP addresses and local IP addresses. With dynamic NAT, you can have a pool of fewer global addresses than local addresses.

Static Port Redirection

Static port redirection, also used for DNAT, performs the same function as static NAT and additionally translates TCP or UDP ports or ICMP identifiers for the local and global addresses. With static port redirection, you can use the same global address in multiple static NAT statements, provided that, along with the address, you use different port numbers.

For example, if you want to provide a single address for global users to access FTP, HTTP, and SMTP, but there are different servers for each protocol on the local network, you can specify static port redirection statements for each server that use the same global IP address with different ports.

Maximum Number of NAT Statements

The ACE supports the following maximum numbers of nat, global, and static commands divided among all contexts:

- nat command—8 K
- nat-pool command—8 K
- static command—8 K
Global Address Guidelines

When you translate the local address to a global address, you can use the following global addresses:

- Addresses on the same network as the global interface—If you use addresses on the same network as the global interface (through which traffic exits the ACE), the ACE uses proxy ARP to answer any requests for translated addresses and thus intercepts traffic destined for a local address. This solution simplifies routing, because the ACE does not need to be the gateway for any additional networks. However, this approach does put a limit on the number of available addresses used for translations.

  \[\text{Note}\] You cannot use the IP address of the global interface for NAT or PAT.

- Addresses on a unique network—If you need more addresses than are available on the global interface network, you can identify addresses on a different subnet. The ACE uses proxy ARP to answer any requests for translated addresses, so it intercepts traffic destined for a local address. You need to add a static route on the upstream router that sends traffic destined for the translated addresses on the ACE.

You cannot configure global IP address ranges across subnets. For example, the following command is not allowed and will generate an Invalid IP address error:

```
nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0
```

You must configure a netmask when configuring a NAT pool. A netmask of 255.255.255.255 instructs the ACE to use all the IP addresses in the range.
Configuring an Idle Timeout for NAT

You can configure an idle timeout for NAT by using the `timeout xlate` command in configuration mode. The syntax of this command is as follows:

```
timeout xlate seconds
```

For the `seconds` argument, enter an integer from 60 to 2147483. The default is 10800 seconds (3 hours). The `seconds` value determines how long the ACE waits to free the Xlate slot after it becomes idle.

For example, to specify an idle timeout of 120 seconds (2 minutes), enter:

```
host1/Admin(config)# timeout xlate 120
```

To reset the NAT idle timeout to the default value of 10800 seconds, enter:

```
host1/Admin(config)# no timeout xlate 120
```

Configuring Dynamic NAT and PAT

This section describes how to configure dynamic NAT and PAT on an ACE for SNAT. It contains the following topics:

- Dynamic NAT and PAT Configuration Quick Start
- Configuring an ACL
- Creating a Global IP Address Pool for NAT
- Configuring a Class Map
- Configuring a Policy Map
- Configuring Dynamic NAT and PAT as a Policy-Map Action
- Applying the Dynamic NAT and PAT Policy Map to an Interface Using a Service Policy
## Dynamic NAT and PAT Configuration Quick Start

Table 5-1 provides a quick overview of the steps required to configure dynamic NAT and PAT. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 5-1.

### Table 5-1 Dynamic NAT and PAT Configuration Quick Start

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.</td>
</tr>
<tr>
<td>host1/Admin# changeto C1</td>
</tr>
<tr>
<td>host1/C1#</td>
</tr>
<tr>
<td>The rest of the examples in this table use the C1 user context, unless otherwise specified. For details on creating contexts, see the Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.</td>
</tr>
<tr>
<td>2. Enter global configuration mode.</td>
</tr>
<tr>
<td>host1/C1# config</td>
</tr>
<tr>
<td>host1/C1(config)#</td>
</tr>
<tr>
<td>3. Configure an ACL to allow traffic that requires NAT.</td>
</tr>
<tr>
<td>host1/C1(config)# access-list NAT_ACCESS extended permit tcp 192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80</td>
</tr>
<tr>
<td>host1/C1(config-acl)# exit</td>
</tr>
<tr>
<td>4. Configure a local interface to receive traffic that requires NAT.</td>
</tr>
<tr>
<td>host1/C1(config)# interface vlan 100</td>
</tr>
<tr>
<td>host1/C1(config-if)# mtu 1500</td>
</tr>
<tr>
<td>host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0</td>
</tr>
<tr>
<td>host1/C1(config-if)# exit</td>
</tr>
</tbody>
</table>
### Table 5-1 Dynamic NAT and PAT Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Configure a second interface and define a global IP address pool on it. To configure dynamic PAT, include the <code>pat</code> keyword in the <code>nat-pool</code> command.</td>
</tr>
</tbody>
</table>
| `host1/C1(config)# interface vlan 200`  
`host1/C1(config-if)# mtu 1500`  
`host1/C1(config-if)# ip address 172.27.16.2 255.255.255.0`  
`host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask 255.255.255.0 pat`  
`host1/C1(config-if)# exit` |
| 6. Configure a class map and define a match statement for the ACL that you configured in Step 3 for the client source address. |
| `host1/C1(config)# class-map match-any NAT_CLASS`  
`host1/C1(config-cmap)# match access-list NAT_ACCESS`  
`host1/C1(config-cmap)# exit` |
| 7. Configure a policy map and associate the class map with the policy map. |
| `host1/C1(config)# policy-map multi-match NAT_POLICY`  
`host1/C1(config-pmap)# class NAT_CLASS`  
`host1/C1(config-pmap-c)#` |
| 8. Configure dynamic NAT as a policy-map action. |
| `host1/C1(config-pmap-c)# nat dynamic 1 vlan 200`  
`host1/C1(config-pmap-c)# exit`  
`host1/C1(config-pmap-c)# exit` |
| 9. Activate the policy on an interface using a service policy. |
| `host1/C1(config)# interface vlan 100`  
`host1/C1(config-if)# service-policy input NAT_POLICY`  
`host1/C1(config-if)# ctrl-z` |
| 10. (Optional) Save your configuration changes to flash memory. |
| `host1/Admin(config)# exit`  
`host1/Admin# copy running-config startup-config` |
| 11. Display and verify your dynamic NAT and PAT configuration. |
| `host1/C1# show running-config class-map`  
`host1/C1# show running-config policy-map` |
Configuring an ACL

You can use a security access control list (ACL) to permit the traffic that requires NAT. For details about configuring an ACL, see Chapter 1, Configuring Security Access Control Lists.

To configure an ACL for dynamic NAT, use the `access-list` command in global configuration mode. The syntax of this command is as follows:

```
access-list name [line number] extended {deny | permit} {protocol} {src_ip_address netmask | any | host src_ip_address} [operator port1 [port2]] {dest_ip_address netmask | any | host dest_ip_address} [operator port3 [port4]]
```

For example, enter:

```
host1/C1(config)# access-list NAT_ACCESS extended permit tcp 192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80
```

To delete the ACL from the configuration, enter:

```
hos1t1/C1(config)# no access-list NAT_ACCESS
```

Creating a Global IP Address Pool for NAT

Dynamic NAT uses a pool of global IP addresses that you specify. You can define either a single global IP address for a group of servers with PAT to differentiate between them, or a range of global IP addresses when using dynamic NAT only.

To use a single IP address or a range of addresses, you assign an identifier to the address pool. You then associate the NAT pool with a VLAN interface.

```
Note
```
If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

```
To create a pool of IP addresses for dynamic NAT, use the `nat-pool` command in interface configuration mode. The syntax of this command is as follows:

```
nat-pool nat_id ip_address1 [ip_address2] netmask mask [pat]
```
The keywords, arguments, and options are as follows:

- **nat_id**—Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.

  **Note** If you configure more than one NAT pool with the same ID, the ACE uses the last-configured NAT pool first, and then the other NAT pools.

- **ip_address1**—Single IP address, or if also using the **ip_address2** argument, the first IP address in a range of global addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).

- **ip_address2**—(Optional) Highest IP address in a range of global IP addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.109). You can configure a maximum of 64 K addresses in a NAT pool.

  **Note** If you specify PAT, you can configure a maximum of 32 IP addresses in a NAT pool range. You cannot configure an IP address range across subnets. For example, the following command is not allowed and will generate an Invalid IP address error: `nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0`.

- **netmask**—Specifies the subnet mask for the IP address pool. Enter a mask in dotted-decimal notation (for example, 255.255.255.255). A network mask of 255.255.255.255 instructs the ACE to use all the IP addresses in the specified range.

- **pat**—(Optional) Specifies that the ACE perform Port Address Translation (PAT) in addition to NAT.

If the ACE runs out of IP addresses in a NAT pool, it can switch over to a PAT rule, if configured. For example, you can configure the following:

```plaintext
nat-pool 1 10.1.100.10 10.1.100.99 netmask 255.255.255.255
nat-pool 1 10.1.100.100 10.1.100.100 netmask 255.255.255.255 pat
```

If your network configuration has the following conditions, you should configure multiple PAT pools with a single IP address in each pool:

- Traffic coming from the same source IP address
- Source ports varying from 1 to 64000
- The same destination port going to different destination addresses
- All ports in one PAT pool are used
So instead of configuring:

```bash
host1/ Admin(config-if)# nat-pool 1 3.3.3.3 3.3.3.5 netmask 255.255.255.255 pat
```

configure:

```bash
host1/Admin(config-if)# nat-pool 1 192.161.12.3 netmask 255.255.255.255 pat
host1/Admin(config-if)# nat-pool 1 192.161.12.4 netmask 255.255.255.255 pat
host1/Admin(config-if)# nat-pool 1 192.161.12.5 netmask 255.255.255.255 pat
```

To configure a NAT pool consisting of a range of 32 (the maximum number of IP addresses per PAT pool) global IP addresses with PAT, enter:

```bash
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask 255.255.255.255 pat
```

---

**Note**

Before you can remove a NAT pool from an interface, you must remove the service policy and the policy map associated with the NAT pool.

To remove a NAT pool from the configuration, enter:

```bash
host1/C1(config-if)# no nat-pool 1
```

### Configuring a Class Map

You can configure a traffic class for dynamic NAT and PAT by using the `class-map` command in global configuration mode. For more information about class maps, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

The syntax of this command is as follows:

```
class-map match-any name
```

For the `name` argument, enter a unique identifier for the class map as an unquoted text string with a maximum of 64 alphanumeric characters.
For example, enter:

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

To remove a class-map from the configuration, enter:

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

Enter match criteria for the ACL or the client source address using the `match` command in class-map configuration mode. For example, enter:

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

or

```
host1/C1(config-cmap)# match source-address 192.168.12.15 255.255.255.0
```

To remove a match statement from a class map, enter:

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

### Configuring a Policy Map

You can configure a traffic policy for dynamic NAT and PAT by using the `policy-map` command in global configuration mode. For more information about policy maps, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

The syntax of this command is as follows:

```
policy-map multi-match name
```

The `name` argument is the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

To remove a policy map from the configuration, enter:

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```
Associate the previously created class map with the policy map. For example, enter:

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

To dissociate a class map from a policy map, enter:

```
host1/C1(config-pmap)# no class NAT_CLASS
```

### Configuring Dynamic NAT and PAT as a Policy-Map Action

You can configure dynamic NAT and PAT (SNAT) as an action in a policy map by using the `nat dynamic` command in policy-map class configuration mode. The ACE applies dynamic NAT from the interface attached to the traffic policy (through the `service-policy` interface configuration command) to the interface specified in the `nat` command.

The syntax of this command is as follows:

```
nat dynamic nat_id vlan number
```

The keywords, arguments, and options are as follows:

- **dynamic nat_id**—Refers to the identifier of a global pool of IP addresses that was configured using the `nat-pool` command on the specified VLAN (see the “Creating a Global IP Address Pool for NAT” section). Dynamic NAT translates a group of local source IP addresses to a pool of global IP addresses that are routable on the destination network. All packets egressing the interface attached to the traffic policy have their source address translated to one of the available addresses in the global pool. Enter an integer from 1 to 2147483647.

- **vlan number**—Specifies the VLAN interface number for which you are configuring NAT.

---

**Note**

If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.
The following example specifies the `nat` command as an action for a dynamic NAT policy map:

```
host1/C1(config)# policy-map multi-action NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)# nat dynamic 1 vlan 200
```

To remove a dynamic NAT action from a policy map, enter:

```
host1/C1(config-pmap-c)# no nat dynamic 1 vlan 200
```

### Applying the Dynamic NAT and PAT Policy Map to an Interface Using a Service Policy

You can activate the dynamic NAT and PAT policy map and associate it with an interface by using the `service-policy` command in interface configuration mode. For details about the `service-policy` command, see the Cisco 4700 Series Application Control Engine Appliance Administration Guide.

---

![Note](image)

The following example specifies the `service-policy` command as an action for an input service policy:

```
host1/C1(config)# service-policy input policy_name
```

The keywords and arguments are as follows:

- **input**—Specifies that the traffic policy is to be attached to the input direction of a VLAN interface. The traffic policy evaluates all traffic received by that interface.
- **policy_name**—Name of a previously defined policy map. The name can have a maximum of 64 alphanumeric characters.

For example, to apply a service policy to a specific interface, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0
host1/C1(config-if)# service-policy input NAT_POLICY
```
To apply a service policy globally to all interfaces in a context, enter:

```
host1/C1(config)# service-policy input NAT_POLICY
```

To remove a service policy from an interface, enter:

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

To remove a service policy globally from all interfaces in a context, enter:

```
host1/C1(config)# no service-policy input NAT_POLICY
```

---

**Note**

When you detach a traffic policy either individually from the last VLAN interface on which you applied the service policy or globally from all VLAN interfaces in the same context, the ACE automatically resets the associated service-policy statistics. The ACE performs this action to provide a new starting point for the service-policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

---

**Configuring Static NAT and Static Port Redirection**

This section describes how to configure static NAT and static port redirection on an ACE for DNAT. It contains the following topics:

- Static NAT Configuration Quick Start
- Configuring an ACL for Static NAT and Port Redirection
- Configuring a Class Map
- Configuring a Policy Map
- Configuring Static NAT and Static Port Redirection as a Policy Action
- Applying the Static NAT Policy Map to an Interface Using a Service Policy
Table 5-2 provides a quick overview of the steps required to configure static NAT and static port redirection. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 5-2.

**Table 5-2 Static NAT Configuration Quick Start**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.</td>
</tr>
</tbody>
</table>
| host1/Admin# changeto C1  
host1/C1# |

The rest of the examples in this table use the C1 user context, unless otherwise specified. For details on creating contexts, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.*

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| host1/C1# config  
host1/C1(config)# |

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Configure an ACL to allow traffic that requires NAT.</td>
</tr>
</tbody>
</table>
| host1/C1(config)# access-list ACL1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any  
host1/C1(config-acl)# exit |

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Configure a local interface to filter and receive traffic that requires NAT.</td>
</tr>
</tbody>
</table>
| host1/C1(config)# interface vlan 100  
host1/C1(config-if)# mtu 1500  
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0  
host1/C1(config-if)# no shutdown  
host1/C1(config-if)# exit |
### Configuring Static NAT and Static Port Redirection

#### Table 5-2  Static NAT Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Configure a second interface (global interface) for performing NAT.</td>
</tr>
<tr>
<td>host1/C1(config)# interface vlan 101</td>
</tr>
<tr>
<td>host1/C1(config-if)# mtu 1500</td>
</tr>
<tr>
<td>host1/C1(config-if)# ip address 172.27.16.100 255.255.255.0</td>
</tr>
<tr>
<td>host1/C1(config-if)# no shutdown</td>
</tr>
<tr>
<td>host1/C1(config-if)# exit</td>
</tr>
<tr>
<td>6. Configure a class map and define match criteria.</td>
</tr>
<tr>
<td>host1/C1(config)# class-map match-any NAT_CLASS</td>
</tr>
<tr>
<td>host1/C1(config-cmap)# match access-list ACL1</td>
</tr>
<tr>
<td>host1/C1(config-cmap)# exit</td>
</tr>
<tr>
<td>7. Configure a policy map and associate the class map with the policy map.</td>
</tr>
<tr>
<td>host1/C1(config)# policy-map multi-match NAT_POLICY</td>
</tr>
<tr>
<td>host1/C1(config-pmap)# class NAT_CLASS</td>
</tr>
<tr>
<td>host1/C1(config-pmap-c)#</td>
</tr>
<tr>
<td>8. Configure static NAT as a policy-map action.</td>
</tr>
<tr>
<td>host1/C1(config-pmap-c)# nat static 192.0.0.0 netmask 255.0.0.0 vlan 101</td>
</tr>
<tr>
<td>host1/C1(config-pmap-c)# exit</td>
</tr>
<tr>
<td>host1/C1(config-pmap-c)# exit</td>
</tr>
<tr>
<td>host1/C1(config)#</td>
</tr>
<tr>
<td>9. Activate the policy on an interface using a service policy.</td>
</tr>
<tr>
<td>host1/C1(config)# interface vlan 100</td>
</tr>
<tr>
<td>host1/C1(config-if)# service-policy input NAT_POLICY</td>
</tr>
<tr>
<td>host1/C1(config-if)# ctrl-z</td>
</tr>
<tr>
<td>10. (Optional) Save your configuration changes to flash memory.</td>
</tr>
<tr>
<td>host1/Admin(config)# exit</td>
</tr>
<tr>
<td>host1/Admin# copy running-config startup-config</td>
</tr>
<tr>
<td>11. Display and verify your static NAT and static port redirection configuration.</td>
</tr>
<tr>
<td>host1/C1# show running-config class-map</td>
</tr>
<tr>
<td>host1/C1# show running-config policy-map</td>
</tr>
</tbody>
</table>
Configuring an ACL for Static NAT and Port Redirection

Use an access control list (ACL) to permit the traffic that requires static NAT and port redirection. For details about configuring an ACL, see Chapter 1, Configuring Security Access Control Lists.

To configure an ACL for static NAT, use the `access-list` command in global configuration mode. The syntax of this command is as follows:

\[
\text{access-list } \text{name} \ \left[\text{line number}\right] \ \text{extended} \ \{\text{deny} \ | \ \text{permit}\} \ \
\{\text{protocol}\} \ \{\text{src_ip_address netmask} \ | \ \text{any} \ | \ \text{host src_ip_address}\} \\
\left[\text{operator port1 [port2]}\right] \ \{\text{dest_ip_address netmask} \ | \ \text{any} \ | \ \text{host dest_ip_address}\} \ \left[\text{operator port3 [port4]}\right]
\]

For example, enter:

```
host1/C1(config)# access-list acl1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any
```

To delete the ACL from the configuration, enter:

```
host1/C1(config)# no access-list nat_access
```

Configuring a Class Map

You can configure a traffic class for static NAT and port redirection by using the `class-map` command in global configuration mode. For more information about class maps, see the Cisco 4700 Series Application Control Engine Appliance Administration Guide.

The syntax of this command is as follows:

\[
\text{class-map match-any name}
\]

For the `name` argument, enter a unique identifier for the class map as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

To remove a class-map from the configuration, enter:

```
host1/C1(config)# no class-map match-any NAT_CLASS
```
Enter match criteria as required using the `match` command in class-map configuration mode. For example, enter:

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

or

```
host1/C1(config-cmap)# match source address 192.168.12.15
```

To remove a match statement from a class map, enter:

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

## Configuring a Policy Map

You can configure a traffic policy for NAT by using the `policy-map` command in global configuration mode. For more information about policy maps, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

The syntax of this command is as follows:

```
policy-map multi-match name
```

The `name` argument is the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

To remove a policy map from the configuration, enter:

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

Associate the previously created class map with the policy map. For example, enter:

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

To dissociate a class map from a policy map, enter:

```
host1/C1(config-pmap)# no class NAT_CLASS
```
Configuring Static NAT and Static Port Redirection as a Policy Action

You can configure static NAT and static port redirection as an action in a policy map by using the `nat static` command in policy-map class configuration mode. Typically, you use static NAT and port redirection for DNAT. Static NAT allows you to identify local traffic for address translation by specifying the source and destination addresses in an extended ACL, which is referenced as part of the class map traffic classification. The ACE applies static NAT from the interface to which the traffic policy is attached (through the `service-policy` interface configuration command) to the interface specified in the `nat static` command.

The syntax of this command is as follows:

```
nat static ip_address netmask mask {port1 | tcp eq port2 | udp eq port3} vlan number
```

The keywords, arguments, and options are as follows:

- **static ip_address**—Sets up a single static translation. The `ip_address` argument establishes the globally unique IP address of a host as it appears to the outside world. The policy map performs the global IP address translation for the source IP address specified in the ACL (as part of the class-map traffic classification).

- **netmask mask**—Specifies the subnet mask for the static IP address. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).

- **port1**—Global TCP or UDP port for static port redirection. Enter an integer from 0 to 65535.

- **tcp eq port2**—Specifies a TCP port name or number. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to match any port. Alternatively, you can enter a protocol keyword that corresponds to a TCP port number. See Table 5-3 for a list of supported well-known TCP port names and numbers.
Configuring Static NAT and Static Port Redirection

**Table 5-3** Well-Known TCP Port Numbers and Key Words

<table>
<thead>
<tr>
<th>Key Word</th>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>21</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>http</td>
<td>80</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>https</td>
<td>443</td>
<td>HTTP over TLS/SSL</td>
</tr>
<tr>
<td>irc</td>
<td>194</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>matip-a</td>
<td>350</td>
<td>Mapping of Airline Traffic over Internet Protocol (MATIP) Type A</td>
</tr>
<tr>
<td>nntp</td>
<td>119</td>
<td>Network News Transport Protocol</td>
</tr>
<tr>
<td>pop2</td>
<td>109</td>
<td>Post Office Protocol v2</td>
</tr>
<tr>
<td>pop3</td>
<td>110</td>
<td>Post Office Protocol v3</td>
</tr>
<tr>
<td>rtsp</td>
<td>554</td>
<td>Real Time Streaming Protocol</td>
</tr>
<tr>
<td>smtp</td>
<td>25</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>telnet</td>
<td>23</td>
<td>Telnet</td>
</tr>
</tbody>
</table>

- **udp eq port3**—Specifies a UDP port name or number. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to match any port. Alternatively, you can enter a protocol keyword that corresponds to a UDP port number. See **Table 5-4** for a list of supported well-known UDP port names and numbers.

**Table 5-4** Well-Known UDP Port Numbers and Key Words

<table>
<thead>
<tr>
<th>Key Word</th>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>53</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>wsp</td>
<td>9200</td>
<td>Connectionless Wireless Session Protocol (WSP)</td>
</tr>
<tr>
<td>wsp-wtls</td>
<td>9202</td>
<td>Secure Connectionless WSP</td>
</tr>
<tr>
<td>wsp-wtp</td>
<td>9201</td>
<td>Connection-based WSP</td>
</tr>
<tr>
<td>wsp-wtp-wtls</td>
<td>9203</td>
<td>Secure Connection-based WSP</td>
</tr>
</tbody>
</table>

- **vlan number**—Specifies the interface for the global IP address.
Note

If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

The following DNAT static port redirection example specifies the `nat static` command as an action for a static NAT policy map:

```plaintext
host1/C1(config)# access-list acl1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)# match access-list acl1
host1/C1(config-cmap)# exit
host1/C1(config)# policy-map multi-action NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)# nat static 192.168.12.0 255.255.255.0 80 vlan 101
```

To remove a NAT action from a policy map, enter:

```plaintext
host1/C1(config-pmap-c)# no nat static 192.168.12.15 255.255.255.0 vlan 200
```

### Applying the Static NAT Policy Map to an Interface Using a Service Policy

You can activate the static NAT and port redirection policy and assign it to an interface by using the `service-policy` command in interface configuration mode. For details about the `service-policy` command, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Note

You can configure static NAT as an input service policy only; you cannot configure it as an output service policy.
The syntax of this command is as follows:

```
service-policy input policy_name
```

The keywords and arguments are as follows:

- **input**—Specifies that the traffic policy is to be attached to the input direction of a VLAN interface. The traffic policy evaluates all traffic received by that interface.

- **policy_name**—Name of a previously defined policy map. The name can have a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0
host1/C1(config-if)# service-policy input NAT_POLICY
```

To remove a service policy from an interface, enter:

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

### Note

When you remove a traffic policy from the last VLAN interface on which you applied the service policy, the ACE automatically resets the associated service-policy statistics. The ACE performs this action to provide a new starting point for the service-policy statistics the next time that you attach a traffic policy to a specific VLAN interface.

## Displaying NAT Configurations and Statistics

The following sections describe the commands used to display dynamic and static NAT and PAT configurations and statistics:

- Displaying NAT and PAT Configurations
- Displaying IP Address and Port Translations
Displaying NAT and PAT Configurations

You can display NAT and PAT configurations by using the `show running-config class-map` and `show running-config policy-map` commands in Exec mode.

For example, enter:

```
host1/C1# show running-config class-map
host1/C1# show running-config policy-map
```

Displaying IP Address and Port Translations

You can display IP address and port translation (Xlate) information by using the `show xlate` command in Exec mode. The syntax of this command is as follows:

```
show xlate [global {ip_address1 [ip_address2 [netmask mask1]]}] [local {ip_address3 [ip_address4 [netmask mask2]]}] [gport port1 [port2]] [lport port1 [port2]]
```

The keywords, arguments, and options are as follows:

- **global ip_address1 ip_address2**—(Optional) Displays information for a global IP address or range of global IP addresses to which the ACE translates source addresses for static and dynamic NAT. For a single global IP address, enter the address in dotted-decimal notation (for example, 192.168.12.15). To specify a range of IP addresses, enter a second IP address.

- **netmask mask**—(Optional) Displays the subnet mask for the specified IP addresses.

- **local ip_address3 ip_address4**—(Optional) Displays the local IP address or range of local IP addresses. For a single local IP address, enter the address in dotted-decimal notation (for example, 192.168.12.15). To specify a range of local IP addresses, enter a second IP address.

- **gport port1 port2**—(Optional) Displays information for a global port or a range of global ports to which the ACE translates source ports for static port redirection and dynamic PAT, respectively. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.
- **lport port3 port4**—(Optional) Displays information for a local port or a range of local ports. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.

For example, enter:

```
host1/Admin# show xlate global 172.27.16.3 172.27.16.10 netmask 255.255.255.0 gport 100 200
```

You can also use the `show conn` command to display NAT information. See the examples in the following sections.

### Dynamic NAT Example

The following example output of the `show xlate` command shows dynamic NAT (SNAT in this example). When a user uses Telnet from 172.27.16.5 in VLAN 2020, the ACE translates it to 192.168.100.1 in VLAN 21.

```
host1/Admin# show xlate global 192.168.100.1 192.168.100.10
NAT from vlan2020:172.27.16.5 to vlan2021:192.168.100.1 count:1
```

### Dynamic PAT Example

The following example shows dynamic PAT. When a user uses Telnet from 172.27.16.5 in VLAN 2020, the ACE translates it to 192.168.201.1 in VLAN 21.

```
host1/Admin# show xlate
TCP PAT from vlan2020:172.27.16.5/38097 to vlan2021:192.168.201.1/1025
```
**Static NAT Example**

The following example shows static NAT. The ACE maps a real IP address (172.27.16.5) to 192.168.210.1.

```
host1/Admin# show xlate
NAT from vlan2020:172.27.16.5 to vlan2021:192.168.210.1 count:1
```

```
host1/Admin# show conn
```

```
total current connections : 2

conn-id   dir  prot  vlan  source     destination     state
----------+-----+----+-----+----------------+----------------+----------+
   7       in  TCP  2020 172.27.16.5 192.168.100.1 ESTAB
   6       out  TCP  2021 192.168.100.1 192.168.210.1 ESTAB
```

**Static Port Redirection (Static PAT) Example**

The following example shows static port redirection (DNAT in this example). A host at 192.168.0.10:37766 uses Telnet to connect to 192.168.211.1:3030 on VLAN 2021 on the ACE. The ACE maps 172.27.0.5:23 on VLAN 2020 to 192.168.211.1:3030 on VLAN 2021.

```
host1/Admin# show xlate
TCP PAT from vlan2020:172.27.0.5/23 to vlan2021:192.168.211.1/3030
Mar 24 2006 20:05:41 : %ACE-7-111009: User 'admin' executed cmd: show xlate
```

```
host1/Admin# show conn
```

```
total current connections : 2

conn-id   dir  prot  vlan  source     destination     state
----------+-----+----+-----+----------------+----------------+----------+
   6       in  TCP  2021 192.168.0.10:37766 192.168.211.1:3030 ESTAB
   7       out  TCP  2020 172.27.0.5:23 192.168.0.10:1025 ESTAB
```
Clearing Xlates

You can clear the global address-to-local address mapping information based on the global address, the global port, the local address, the local port, the interface address as the global address, and the NAT type by using the `clear xlate` command in Exec mode. When you enter this command, the ACE releases sessions that are using the translations (Xlates). The syntax of this command is as follows:

```
clear xlate [{global | local} start_ip [end_ip [netmask netmask]]] [{gport | lport} start_port [end_port]] [interface vlan number] [state static] [portmap]
```

The keyword, arguments, and options are as follows:

- **global**—(Optional) Clears the active translation by the global IP address.
- **local**—(Optional) Clears the active translation by the local IP address.
- **start_ip**—Global or local IP address in a global or local range of IP addresses. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
- **end_ip**—(Optional) Last IP address in a global or local range of IP addresses. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
- **netmask netmask**—(Optional) Specifies the network mask for global or local IP addresses. Enter a mask in dotted-decimal notation (for example, 255.255.255.0).
- **gport**—(Optional) Clears active translations by the global port.
- **lport**—(Optional) Clears active translations by the local port.
- **start_port**—Global or local port number.
- **end_port**—(Optional) Last port number in a global or local range of ports.
- **interface vlan number**—(Optional) Clears active translations by the VLAN number.
- **state static**—(Optional) Clears active translations by the state.
- **portmap**—(Optional) Clears active translations by the port map.

**Note**
If you configured redundancy, then you need to explicitly clear Xlates on both the active and the standby ACEs. Clearing Xlates on the active appliance alone will leave the standby appliance’s Xlates at the old mappings.
For example, to clear all static translations, enter:

```
host1/Admin# clear xlate state static
```

## NAT Configuration Examples

The following sections show typical scenarios that use dynamic and static NAT solutions:

- **Dynamic NAT and PAT (SNAT) Configuration Example**
- **Static Port Redirection (DNAT) Configuration Example**

### Dynamic NAT and PAT (SNAT) Configuration Example

The following SNAT configuration example shows the commands that you use to configure dynamic NAT and PAT on your ACE. In this SNAT example, packets that ingress the ACE from the 19.168.12.0 network are translated to one of the IP addresses in the NAT pool defined on VLAN 200 by the `nat-pool` command. The `pat` keyword indicates that ports higher than 1024 are also translated.

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0 255.255.255.0 1 72.27.16.0 255.255.255.0 eq http

class-map match-any NAT_CLASS
    match access-list NAT_ACCESS

class-map match-any NAT_CLASS
    match access-list NAT_ACCESS

policy-map multi-match NAT_POLICY
    class NAT_CLASS
        nat dynamic 1 vlan 200

interface vlan 100
    mtu 1500
    ip address 192.168.1.100 255.255.255.0
    service-policy input NAT_POLICY
    no shutdown

interface vlan 200
    mtu 1500
    ip address 172.27.16.2 255.255.255.0
    nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0 pat
    no shutdown
```
Static Port Redirection (DNAT) Configuration Example

The following DNAT configuration example shows those sections of the running configuration related to the commands necessary to configure static port redirection on your ACE. Typically, this configuration is used for DNAT, where HTTP packets that are destined to 192.0.0.0/8 and ingressing the ACE on VLAN 101 are translated to 10.0.0.0/8 and port 8080. In this example, the servers are hosting HTTP on custom port 8080.

```
access-list acl1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any

class-map match-any NAT_CLASS
    match access-list acl1

policy-map multi-match NAT_POLICY
    class NAT_CLASS
        nat static 192.0.0.0 255.0.0.0 80 vlan 101

interface vlan 100
    mtu 1500
    ip address 192.168.1.100 255.255.255.0
    service-policy input NAT_POLICY
    no shutdown

interface vlan 101
    mtu 1500
    ip address 172.27.16.100 255.255.255.0
    no shutdown
```
Example of SNAT with Cookie Load Balancing

The following configuration example shows those sections of the running configuration related to the commands necessary to configure SNAT (dynamic NAT) with cookie load balancing. Any source host that sends traffic to the VIP 20.11.0.100 is translated to one of the free addresses in the NAT pool in the range 30.11.100.1 to 30.11.200.1, inclusive. If you want to use PAT instead of NAT, replace “nat dynamic 1 vlan 2021” with “nat dynamic 2 vlan 2021” in the L7SLBCookie policy map.

```
server host http
    ip address 30.11.0.10
    inservice
serverfarm host httpsf
    rservers http
    inservice

class-map match-any vip4
    2 match virtual-address 20.11.0.100 tcp eq www
class-map type http loadbalance match-any L7SLB_Cookie
    3 match http cookie JG cookie-value ".*"

policy-map type loadbalance first-match L7SLB_Cookie
    class L7SLB_Cookie
    serverfarm httpsf
Policy-map multi-match L7SLBCookie
    class vip4
        loadbalance vip inservice
        loadbalance L7SLB_Cookie
        nat dynamic 1 vlan 2021

interface vlan 2020
    ip address 20.11.0.2 255.255.0.0
    alias 20.11.0.1 255.255.0.0
    peer ip address 20.11.0.3 255.255.0.0
    service-policy input L7SLBCookie
    no shutdown

interface vlan 2021
    ip address 30.11.0.2 255.255.0.0
    alias 30.11.0.1 255.255.0.0
    peer ip address 30.11.0.3 255.255.0.0
    fragment min-mtu 68
    nat-pool 2 30.11.201.1 30.11.201.1 netmask 255.255.255.255 pat
    nat-pool 1 30.11.100.1 30.11.200.1 netmask 255.255.255.255
    no shutdown
```