CHAPTER 5

Configuring Cisco Adaptive Security Appliance for this Integration

January 26, 2009

External and Internal Interface Configuration

On the Cisco Adaptive Security Appliance you must configure two interfaces as follows:

- Use one interface as the "**outside**" or external interface. This is the interface to the internet and to the foreign domain servers (Microsoft Access Edge/Access Proxy).
- Use the second interface as the"**inside**" or internal interface. This is the interface to Cisco Unified Presence or to the Load Balancer, depending on your deployment.
- When configuring an interface, you need to refer it with an **interface type**, for example Ethernet or Gigabit Ethernet, and an **interface slot.** The Cisco Adaptive Security Appliance has four embedded Ethernet or Gigabit Ethernet ports on slot 0. You may optionally add an SSM-4GE module in slot 1 to obtain an additional four Gigabit Ethernet ports on slot 1.
- For each interface to route traffic, you need to configure an **interface name** and an **IP address**. The internal and external interface IP addresses must be in different subnets, which means they must have different submasks.
- Each interface must have a security level ranging from zero to 100 (from lowest to highest). A security level value of 100 is the most secure interface (inside interface). A security level value of zero is the least secure interface. If you do not explicitly set the security level for the inside or outside interface, then Cisco Adaptive Security Appliance sets the security level to 100 by default.
- Please refer to the *Cisco Security Appliance Command Line Configuration Guide* for details on configuring the external and internal interfaces via the CLI.

Note You can configure the internal and external interfaces using the ASDM startup wizard. You can also view or edit an interface in ASDM by selecting **Configuration > Device Setup > Interfaces**.

Configuring the Static IP Routes

Cisco Adaptive Security Appliance supports both static routes and dynamic routing protocols such as OSPF, RIP and EIGRP. For this integration you need to configure static routes that define the next hop address for IP traffic routed to the inside interface and for traffic routed to the outside interface of Cisco Adaptive Security Appliance. In the procedure below, the *dest_ip mask* is the IP address for the destination network and the *gateway_ip* value is the address of the next-hop router or gateway.

For a detailed description on setting up default and static routes on Cisco Adaptive Security Appliance, refer to the *Cisco Security Appliance Command Line Configuration Guide*.

Before You Begin

Complete the steps in External and Internal Interface Configuration, page 5-1

Procedure

Step 1 Enter config mode:

```
>Enable
>password
>config t
```

Step 2 Enter this command to add a static route for the inside interface:

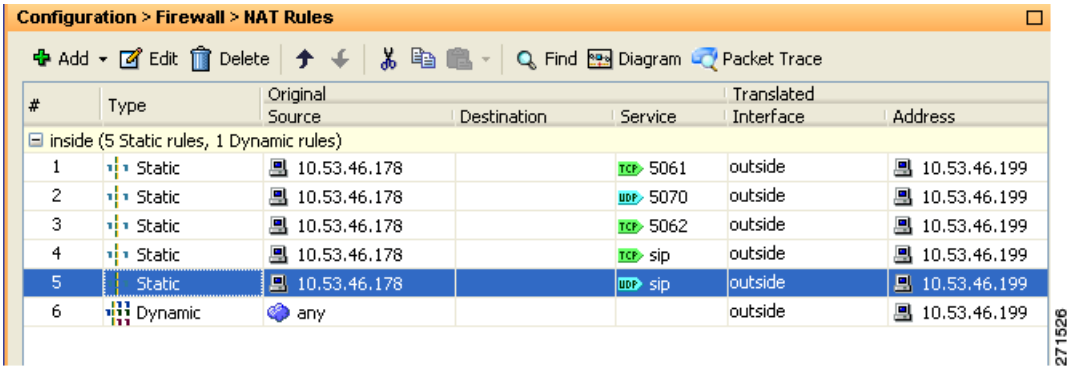
```
hostname(config)# route inside dest_ip mask gateway_ip
```

Step 3 Enter this command to add a static route for the outside interface:

```
hostname(config)# route outside dest_ip mask gateway_ip
```

Note You can also view and configure the static routes from ASDM by selecting **Configuration > Device Setup > Routing > Static routes.**

Figure 5-1 Viewing static routes via ASDM



What To Do Next

About Port Address Translation (PAT), page 5-3

About Port Address Translation (PAT)

Port Address Translation for This Integration

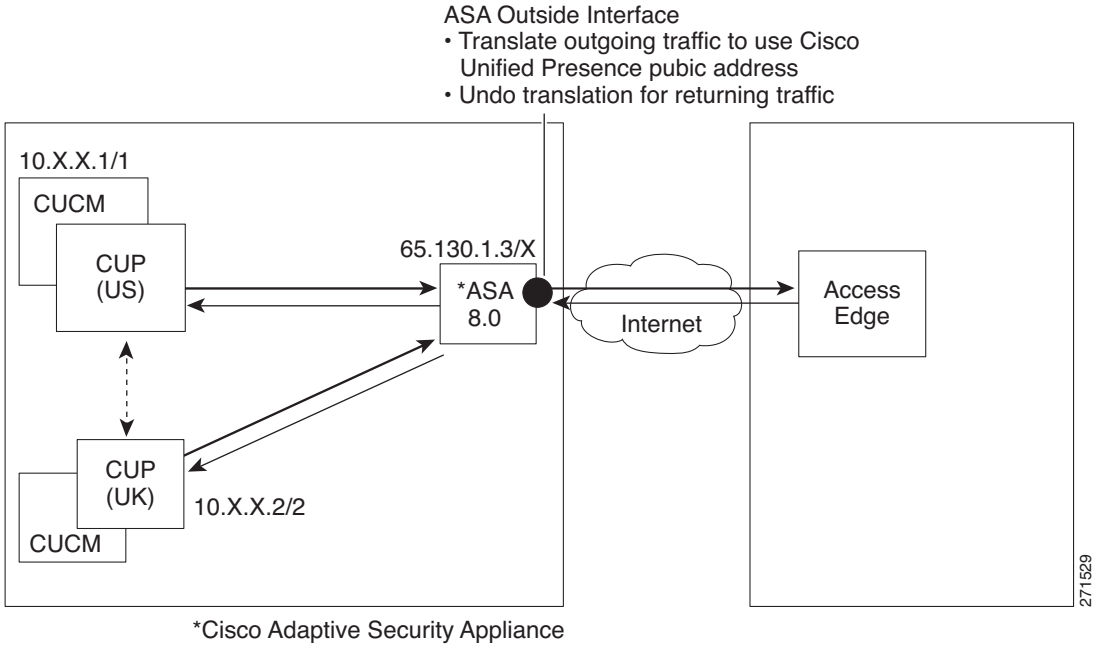
Note You also use Port Address Translation if you are federating with another Cisco Unified Presence enterprise deployment in a foreign domain.

For this integration, Cisco Adaptive Security Appliance uses Port Address Translation (PAT) and static PAT for message address translation. Cisco Adaptive Security Appliance does not use Network Address Translation (NAT) for this integration.

This integration uses PAT to translate messages sent from Cisco Unified Presence to a foreign domain (private to public messages). Port Address Translation (PAT) means the real address and source port in a packet is substituted with a mapped address and unique port that is routable on the destination network. This translation method uses a two step process that translates the real IP address and port to a mapped IP address and port, and then the translation is "undone" for returning traffic.

Cisco Adaptive Security Appliance translates messages sent from Cisco Unified Presence to a foreign domain (private to public messages) by changing the private IP address and port on Cisco Unified Presence to a public IP address and one or more public port(s). Therefore, a local Cisco Unified Presence domain only uses one public IP address. Cisco Adaptive Security Appliance assigns a NAT command to the outside interface and translates the IP address and port of any message received on that interface as illustrated in Figure 5-2.

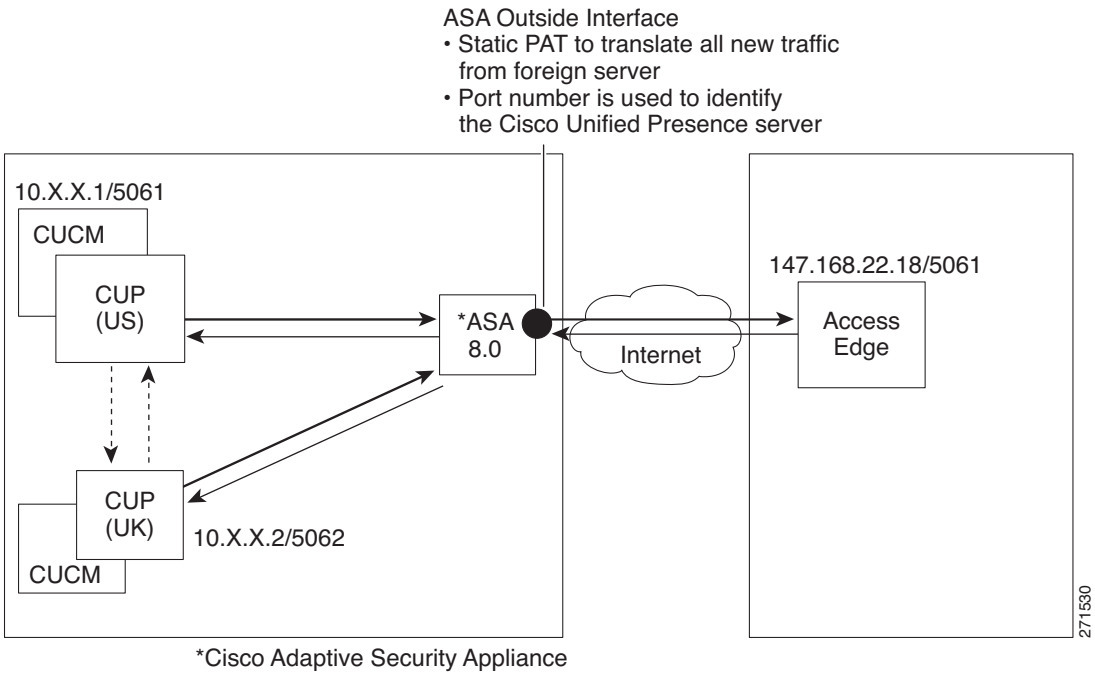
Figure 5-2 PAT for Messages Originating from Cisco Unified Presence to a Foreign Domain



For new messages sent from a foreign domain to Cisco Unified Presence, Cisco Adaptive Security Appliance uses static PAT to map any message sent to the public IP address and port for Cisco Unified Presence to a designated Cisco Unified Presence server. Using static PAT allows you to translate the real IP address to a mapped IP address, and the real port number to a mapped port number. You can translate the real port number to the same port number or to a different port number. In this case, the port number identifies the correct Cisco Unified Presence server to handle the message request, as shown in Figure 5-3.

Note If a user does not exist on the Cisco Unified Presence server, the Cisco Unified Presence routing server uses intercluster routing to redirect the message. All responses are sent to Cisco Adaptive Security Appliance from the Cisco Unified Presence routing server.

Figure 5-3 Static PAT for Messages Originating from a Foreign Domain



PAT for Private to Public Messages

For this integration, the address translation for private to public messages involves the following configuration:

- Define a NAT rule to identify the real IP address and port number that you wish to translate. In this case, configure a NAT rule that states that a NAT action must be applied to any message received on the internal interface.
- Configure a global NAT action to specify the mapped addresses to use for messages exiting via the external (outside) interface. For this integration, specify only one address (because it uses PAT). The NAT action maps the IP address (of messages received on the internal interface) to the Cisco Unified Presence public address.

You can use this sample NAT configuration in a deployment where there are one or more Cisco Unified Presence servers on the inside interface, with no other firewall traffic.

```
global (outside) 1 <public_cup_address>
nat (inside) 1 0 0
```

You can use this sample NAT configuration in a deployment where there is one Cisco Unified Presence server on the inside interface, with other firewall traffic.

```
global (outside) 1 <public_cup_address>
nat (inside) 1 <private_cup_address> 255.255.255.255

global (outside) 2 interface
nat (inside) 2 0 0
```

You can use this sample NAT configuration in a deployment where there are multiple Cisco Unified Presence servers on the inside interface, with other firewall traffic.

```
global (outside) 1 <public cup ip>
nat (inside) 1 <private_cup_net> <private_cup_netmask>

global (outside) 2 interface
nat (inside) 2 0 0
```

Note The configuration example above assumes that when there are multiple Cisco Unified Presence servers located behind Cisco Adaptive Security Appliance, these Cisco Unified Presence servers are all on the same subnet. Specifically, if all the inside Cisco Unified Presence servers are on the 2.2.2.x/24 network, the NAT command is: `nat (inside) 1 2.2.2.0 255.255.255.0`

Related Topics

Port Address Translation for This Integration, page 5-3

Static PAT for New Messages

For this integration the address translation for private to public messages involves the following configuration:

- Configure a static PAT command for the following ports: 5060, 5061, 5070, and 5062.
- Configure a separate static PAT command for port 5070 to allow TCP, or UDP connections, or both, to be established before the translated messages are sent.

This integration uses the following ports:

- 5060 - Cisco Adaptive Security Appliance uses this port for generic SIP inspection.
- 5061 - The SIP SUBSCRIBE message is sent to this port and this triggers the TLS handshake.
- 5062, 5070 - Cisco Unified Presence uses these ports in the SIP VIA/CONTACT headers.

Note You can check the peer auth listener port on Cisco Unified Presence by selecting **Cisco Unified Presence Administration > System > Application Listeners**.

See the sample configuration below for the PAT commands for the routing Cisco Unified Presence, where the peer auth listener port is 5062.

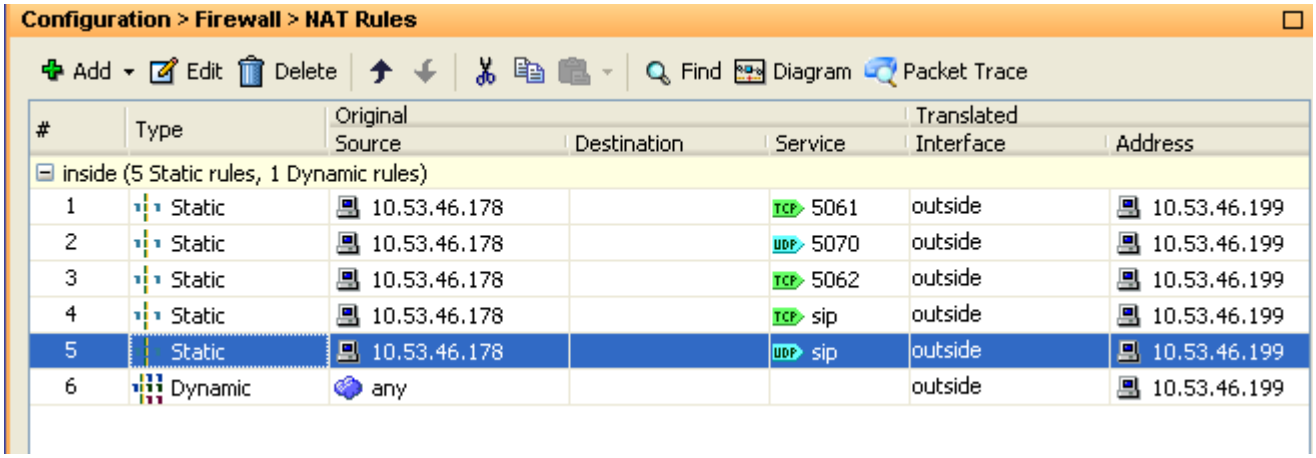
```
static (inside,outside) tcp <public cup ip address> 5061 <routing private cup address>
5062 netmask 255.255.255.255
static (inside,outside) udp <public cup ip address> 5070 <routing private cup address>
5070 netmask 255.255.255.255
static (inside,outside) tcp <public cup ip address> 5070 <routing private cup address>
5070 netmask 255.255.255.255
static (inside,outside) tcp <public cup ip address> 5060 <routing private cup address>
5060 netmask 255.255.255.255
static (inside,outside) tcp <public cup ip address> 5062 <routing private cup address>
5061 netmask 255.255.255.255
```

For an multi-node cluster or an intercluster Cisco Unified Presence deployment, if you have Cisco Unified Presence clusters communicating directly with Cisco Adaptive Security Appliance, for *each* Cisco Unified Presence node you must configure a set of static PAT commands such as those listed below. Note that you must use an unused arbitrary port, and we recommend selecting a corresponding number, for example, 5070 use the unused arbitrary port 45070.

```
static (inside,outside) tcp <public CUP address> 50000 <intercluster private cup address>
5062 netmask 255.255.255.255

static (inside,outside) udp <public CUP address> 55070 <private cup address> 5070 netmask
255.255.255.255

static (inside,outside) tcp <public CUP address> 55070 <private cup address> 5070 netmask
255.255.255.255

static (inside,outside) tcp <public CUP address> 55060 <private cup address> 5060 netmask
255.255.255.255

static (inside,outside) tcp <public CUP address> 40000 <private cup address> 5061 netmask
255.255.255.255
```

You can view the NAT rules in ASDM by selecting **Configuration > Firewall > NAT Rules**. The first five NAT rules shown in Figure 5-4 are the static PAT entries, and the final dynamic entry is the outgoing PAT configuration that maps any outgoing traffic to the public Cisco Unified Presence IP address and port.

Figure 5-4 Viewing PAT rules via ASDM



Related Topics

- Sample Cisco Adaptive Security Appliance Configuration, page A-1
- Port Address Translation for This Integration, page 5-3

Failover on Cisco Adaptive Security Appliance

For a detailed description of configuring failover for Cisco Adaptive Security Appliance, refer to the *Cisco Security Appliance Command Line Configuration Guide*. If you are considering deploying failover for Cisco Adaptive Security Appliance in your federated network, note the following:

- Failover is supported using the active/standby mode. With active/standby failover, only one Cisco Adaptive Security Appliance router passes traffic while the other router waits in a standby state.
- In terms of hardware requirements, the two Cisco Adaptive Security Appliances in a failover deployment must have the exact same hardware configuration.
- In terms of software requirements, the two Cisco Adaptive Security Appliances in a failover configuration must be in the operating mode, and must have the same software version.
- In terms of licensing, for active/standby mode you will require a security plus license, and unrestricted (UR) licence.

Note Cisco Adaptive Security Appliance does not support a TLS stateful or graceful failover. Existing TLS connections must be reestablished following a failover to the standby Cisco Adaptive Security Appliance.