Configuring Cisco Adaptive Security Appliance for SIP Federation

June 18, 2013

Note Only Cisco Unified Presence Release 8.5(2) or later supports interdomain federation with Microsoft Lync. For Cisco Unified Presence Release 8.5(2) or later, any reference to interdomain federation with OCS also includes Microsoft Lync, unless explicitly stated otherwise.

Cisco Adaptive Security Appliance Unified Communication Wizard

If you deploy a **single** Cisco Unified Presence server in your interdomain federation deployment, you can use the Unified Communication wizard on Cisco Adaptive Security Appliance to configure the presence federation proxy between Cisco Adaptive Security Appliance and Cisco Unified Presence.

A configuration example showing the Unified Communication wizard is provided on the Cisco Unified Presence documentation wiki, see the URL below.

Related Topics

http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_8.x

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 (for example, 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 6-1

Procedure

Step 1 Enter config mode:

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

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

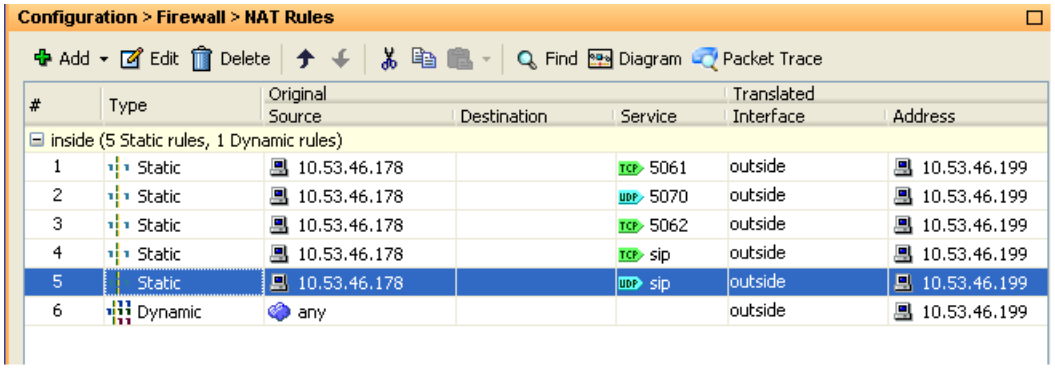
```
hostname(config)# route inside dest_ip mask gateway_ip
```

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 6-1 Viewing static routes via ASDM



What To Do Next

About Port Address Translation (PAT), page 6-3

About Port Address Translation (PAT)

Port Address Translation for This Integration

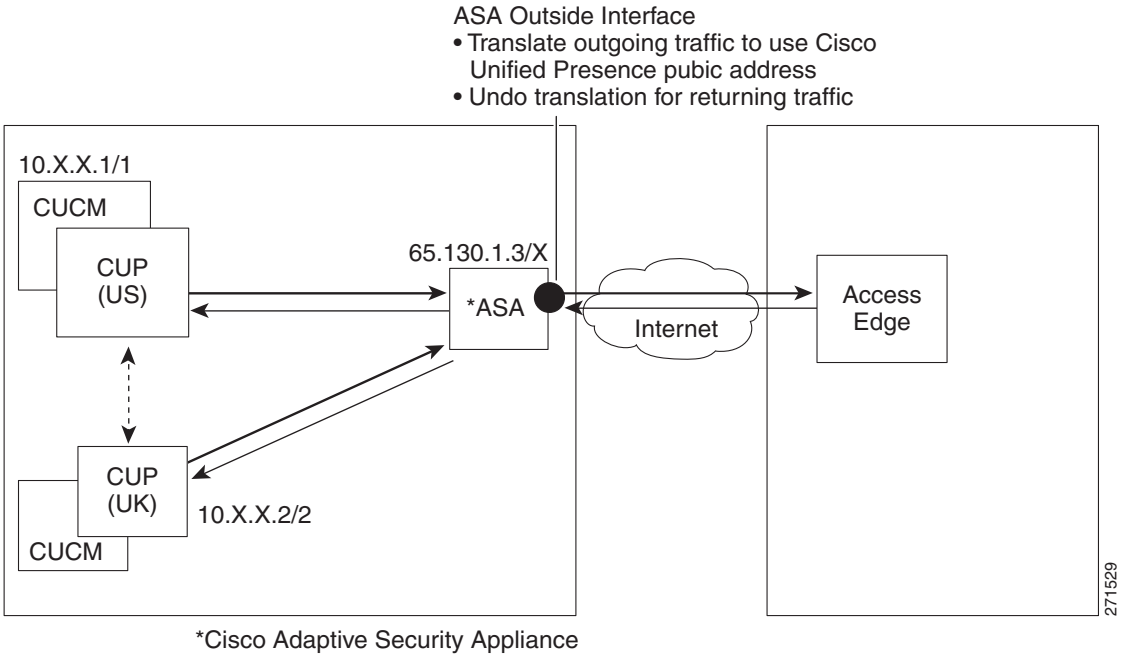
Note You also use Port Address Translation if you federate with another Cisco Unified Presence enterprise deployment in a foreign domain.

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 6-2.

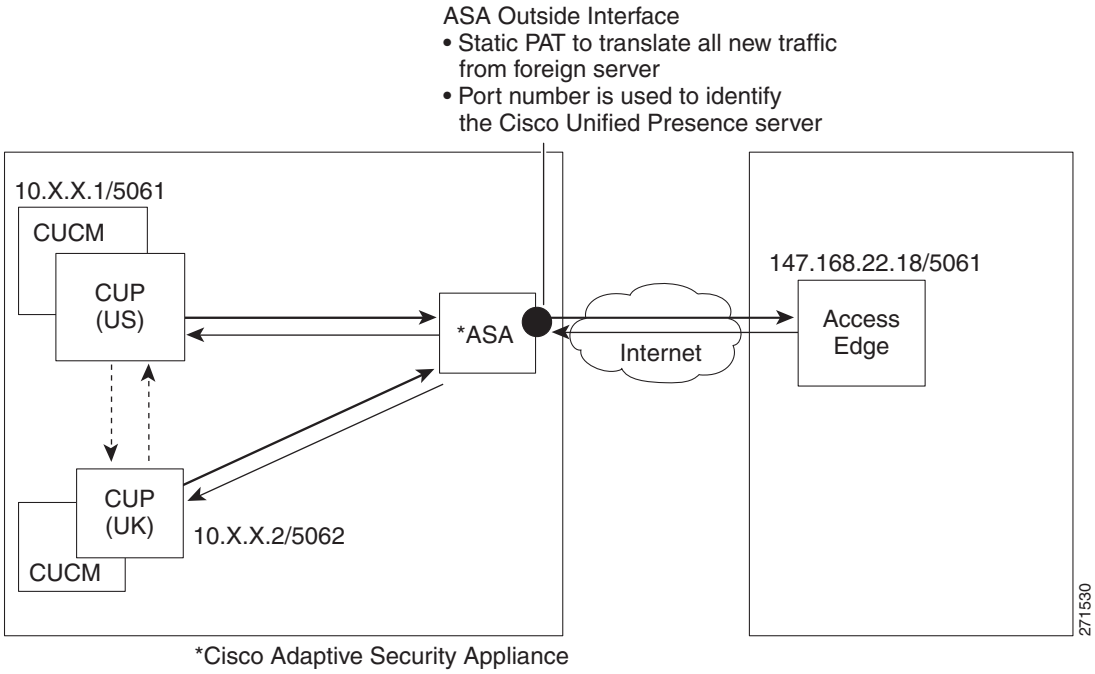
Figure 6-2 Example PAT for Messages Originating from Cisco Unified Presence to a Foreign Domain



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 6-3.

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 6-3 Static PAT for Messages Originating from a Foreign Domain



PAT for Private to Public Requests

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 Cisco Adaptive Security Appliance must apply a NAT action 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.

The following table provides sample global address translation commands for Cisco Adaptive Security Appliance Releases 8.2 and 8.3. The first row is mandatory for both a single Cisco Unified Presence deployment, and a multiple Cisco Unified Presence deployment. The second row is for single Cisco Unified Presence deployment only. The third row is for a multiple Cisco Unified Presence deployment.

Table 6-1 Sample global address translation commands

Sample Configuration	Cisco Adaptive Security Appliance Release 8.2 Global Command	Cisco Adaptive Security Appliance Release 8.3 Global Command

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`
		`object network obj_any`
		`host 0.0.0.0`
		`nat (inside,outside) dynamic <public cup address>`

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`
		`host <private cup address>`
		`nat (inside,outside) dynamic <public cup address>`
		
		`object network my_inside`
		`subnet 0.0.0.0 0.0.0.0`
		`nat (inside,outside) dynamic interface`

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`
		`object network obj_<private subnet>.0_255.255.255.0`
		`subnet <private subnet> 255.255.255.0`
		`nat (inside,outside) dynamic <public cup address>`
		
		`object network my_inside`
		`subnet 0.0.0.0 0.0.0.0`
		`nat (inside,outside) dynamic interface`

Note The sample configuration shown in the last row in Table 6-1 assumes that when there are multiple Cisco Unified Presence servers located behind Cisco Adaptive Security Appliance, and 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 6-3

Static PAT for New Requests

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

- Configure a static PAT command on TCP for the following ports: 5060, 5061, 5062 & 5080. Additionally if you have configured an intercluster connection with a Cisco Unified Presence Release 7.x node in your deployment, configure a TCP port for 5070.
- Configure a separate static PAT command on UDP for port 5080. Additionally if you have configured an intercluster connection with a Cisco Unified Presence Release 7.x node in your deployment, configure a UDP port for 5070.

This integration uses the following ports:

- 5060 - Cisco Adaptive Security Appliance uses this port for generic SIP inspection.
- 5061 - The SIP requests are sent to this port and this triggers the TLS handshake.
- 5062, 5070, 5080- Cisco Unified Presence uses these ports in the SIP VIA/CONTACT headers.

You only require PAT for port 5070 if you have an intercluster Cisco Unified Presence Release 7.x node in your Cisco Unified Presence Release 8.x cluster within the same domain. Cisco Unified Presence Release 8.x replaces port 5070 with port 5080.

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

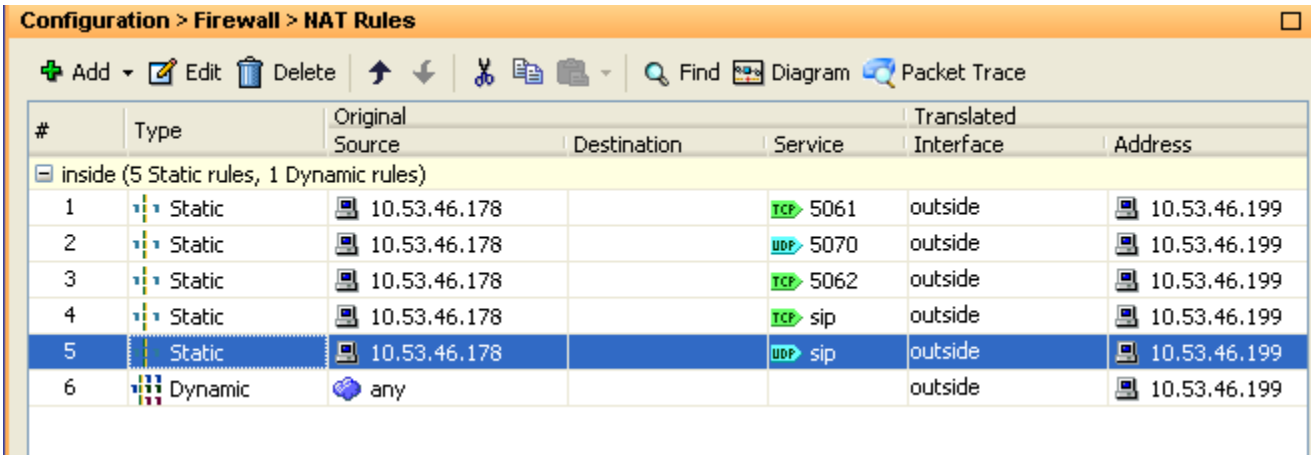
Related Topics

- About Sample Static PAT Commands, page 6-8
- Sample Cisco Adaptive Security Appliance Configuration, page A-1

NAT Rules in ASDM

You can view the NAT rules in ASDM by selecting **Configuration > Firewall > NAT Rules**. The first five NAT rules shown in Figure 6-4 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 6-4 Viewing PAT rules via ASDM



Related Topics

- About Sample Static PAT Commands, page 6-8
- Sample Cisco Adaptive Security Appliance Configuration, page A-1

About Sample Static PAT Commands

Note This section shows sample commands for Cisco Adaptive Security Appliance Release 8.3 and Release 8.2. You need to execute these commands when you configure a fresh configuration of Cisco Adaptive Security Appliance for federation.

- PAT Configuration for Routing Cisco Unified Presence Release 8.x Node, page 6-9
- PAT Configuration for Intercluster or Intracluster Cisco Unified Presence Release 8.x Nodes, page 6-10
- PAT Configuration for Intercluster Cisco Unified Presence Release 7.x Nodes, page 6-12

PAT Configuration for Routing Cisco Unified Presence Release 8.x Node

Table 6-2 shows the PAT commands for the routing Cisco Unified Presence Release 8.x node, where the peer auth listener port is 5062.

Note For Cisco Adaptive Security Appliance 8.3 configuration, you only need to define an object once and you can reference that object in multiple commands; you do not need to repeatedly define the same object.

Table 6-2 PAT commands for routing Cisco Unified Presence Release 8.x node

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Security Appliance Release 8.3 NAT Command

`static (inside,outside) tcp <public cup ip address> 5061 <routing cup private address> 5062 netmask 255.255.255.255`
 	
If the routing CUP peer auth listening port is 5061, use the command:
`static (inside,outside) tcp <public cup ip address> 5061 <routing cup private address> 5061 netmask 255.255.255.255`
	`Object network obj_host_<public cup ip address> (e.g. object network obj_host_10.10.10.10) #host <public cup ip address>`
	
	`object network obj_host_<routing cup private address> host <routing cup private address>`
	
	`object service obj_tcp_source_eq_5061 service tcp source eq 5061`
	
	`object service obj_tcp_source_eq_5062 service tcp source eq 5062`
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061`
	
	If the routing CUP peer auth listening port is 5061, use the command:
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5061 obj_tcp_source_eq_5061`

`static (inside,outside) tcp <public cup ip address> 5080 <routing cup private address> 5080 netmask 255.255.255.255`	`object service obj_tcp_source_eq_5080 service tcp source eq 5080`
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5080 obj_tcp_source_eq_5080`

`static (inside,outside) tcp <public cup ip address> 5060 <routing cup private address> 5060 netmask 255.255.255.255`	`object service obj_tcp_source_eq_5060 service tcp source eq 5060`
	Note 5060 displays as 'sip' in the service object.
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5060 obj_tcp_source_eq_5060`

`static (inside,outside) tcp <public cup ip address> 5062 <routing cup private address> 5062 netmask 255.255.255.255`	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_5062`

Related Topics

- Static PAT for New Requests, page 6-7
- PAT Configuration for Intercluster or Intracluster Cisco Unified Presence Release 8.x Nodes, page 6-10
- PAT Configuration for Intercluster Cisco Unified Presence Release 7.x Nodes, page 6-12

PAT Configuration for Intercluster or Intracluster Cisco Unified Presence Release 8.x Nodes

In a multi-node or an intercluster Cisco Unified Presence deployment, if the non-routing nodes in your Cisco Unified Presence Release 8.x clusters communicate directly with Cisco Adaptive Security Appliance, you must configure a set of static PAT commands for *each* of these nodes. The commands listed below are an example of a set of the static PAT commands you must configure for a single node.

You must use an unused arbitrary port. We recommend that you select a corresponding number, for example, 5080 uses the unused arbitrary port X5080 where X corresponds to a number that uniquely maps to a Cisco Unified Presence intercluster or intracluster server. For example 45080 uniquely maps to one node and 55080 uniquely maps to another node.

Table 6-3 shows the NAT commands for the non-routing Cisco Unified Presence Release 8.x nodes. Repeat the commands for each non-routing Cisco Unified Presence Release 8.x node.

Note For Cisco Adaptive Security Appliance 8.3 configuration, you only need to define an object once and you can reference that object in multiple commands; you do not need to repeatedly define the same object.

Table 6-3 NAT commands for non-routing Cisco Unified Presence Release 8.x nodes

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Security Appliance Release 8.3 NAT Command

`static (inside,outside) tcp <public CUP address> 45062 <intercluster cup8 private address> 5062 netmask 255.255.255.255`
 	
If the intercluster Cisco Unified Presence peer auth listening port is 5061, use the command:
 	
`static (inside,outside) tcp <public CUP address> 45061 <intercluster cup8 private address> 5061 netmask 255.255.255.255`
	`object network obj_host_<intercluster cup8 private address>`
	`host <intercluster cup8 private address>`
	
	`object service obj_tcp_source_eq_45062`
	`service tcp source eq 45062`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_45062`
	
	If the intercluster Cisco Unified Presence peer auth listening port is 5061, use the command:
	
	`object service obj_tcp_source_eq_45061`
	`service tcp source eq 45061`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5061 obj_tcp_source_eq_45061`

`static (inside,outside) tcp <public cup ip address> 45080 <intercluster cup8 private address> 5080 netmask 255.255.255.255`	`object service obj_tcp_source_eq_45080`
	`service tcp source eq 45080`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5080 obj_tcp_source_eq_45080`

`static (inside,outside) tcp <public cup ip address> 45060 <intercluster cup8 private address> 5060 netmask 255.255.255.255`	`object service obj_tcp_source_eq_45060`
	`service tcp source eq 45060`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5060 obj_tcp_source_eq_45060`

Related Topics

- Static PAT for New Requests, page 6-7
- PAT Configuration for Routing Cisco Unified Presence Release 8.x Node, page 6-9
- PAT Configuration for Intercluster Cisco Unified Presence Release 7.x Nodes, page 6-12

PAT Configuration for Intercluster Cisco Unified Presence Release 7.x Nodes

In a multi-node or an intercluster Cisco Unified Presence deployment, if nodes in your Cisco Unified Presence Release 7.x clusters communicate directly with Cisco Adaptive Security Appliance, you must configure a set of static PAT commands for *each* of these nodes. The commands listed below are an example of a set of the static PAT commands you must configure for a single node.

You must use an unused arbitrary port. We recommend that you select a corresponding number, for example, 5070 uses the unused arbitrary port X5070 where X corresponds to a number that uniquely maps to a Cisco Unified Presence intercluster or intracluster server. For example 65070 uniquely maps to one node and 75070 uniquely maps to another node.

Table 6-4 shows the NAT commands for intercluster Cisco Unified Presence Release 7.x nodes. Repeat the commands for each node.

Note For Cisco Adaptive Security Appliance 8.3 configuration, you only need to define an object once and you can reference that object in multiple commands; you do not need to repeatedly define the same object.

Table 6-4 NAT commands for intercluster Cisco Unified Presence Release 7.x nodes

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Security Appliance Release 8.3 NAT Command

`static (inside,outside) tcp <public CUP address> 55062 <intercluster cup7 private address> 5062 netmask 255.255.255.255`
 	
If the intercluster CUP peer auth listening port is 5061, use the command:
 	
`static (inside,outside) tcp <public CUP address> 55061 <intercluster cup7 private address> 5061 netmask 255.255.255.255`
	`object network obj_host_<intercluster cup7 private address>`
	`#host <intercluster cup7 private address>`
	
	`object service obj_tcp_ source_eq_55062`
	`# service tcp source eq 55062`
	
	`nat (inside,outside) source static obj_host_<intercluster cup7 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_55062`
	
	If the intercluster Cisco Unified Presence peer auth listening port is 5061, use the command:
	
	`object service obj_tcp_ source_eq_55061`
	`# service tcp source eq 55061`
	`nat (inside,outside) source static obj_host_<intercluster cup7 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5061 obj_tcp_source_eq_55061`

Table 6-4 NAT commands for intercluster Cisco Unified Presence Release 7.x nodes

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Security Appliance Release 8.3 NAT Command

`static (inside,outside) tcp <public cup ip address> 55070 <intercluster cup7 private address> 5070 netmask 255.255.255.255`	`object service obj_tcp_source_eq_55070`
	`# service tcp source eq 55070`
	
	`nat (inside,outside) source static obj_host_<intercluster cup7 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5070 obj_tcp_source_eq_55070`

`static (inside,outside) udp <public cup ip address> 55070 <intercluster cup7 private address> 5070 netmask 255.255.255.255`	`object service obj_udp_source_eq_55070`
	`# service udp source eq 55070`
	
	`nat (inside,outside) source static obj_host_<intercluster cup7 private address> obj_host_<public cup ip address>`

There is a limitation with intercluster deployments and SIP federation with AOL, refer to Intercluster Deployments and SIP Federation with AOL, page 1-4 for details.

Related Topics

- Static PAT for New Requests, page 6-7
- PAT Configuration for Routing Cisco Unified Presence Release 8.x Node, page 6-9
- PAT Configuration for Intercluster or Intracluster Cisco Unified Presence Release 8.x Nodes, page 6-10
- Intercluster Deployments and SIP Federation with AOL, page 1-4

Cisco Adaptive Security Appliance Upgrade Options for Existing Deployments

If you upgrade from Cisco Adaptive Security Appliance Release 8.2 to Release 8.3, Cisco Adaptive Security Appliance migrates the existing commands seamlessly during the upgrade.

Note Once you upgrade to Cisco Unified Presence Release 8.x, you must open port 5080 on Cisco Adaptive Security Appliance for each Cisco Unified Presence 8.x node located behind Cisco Adaptive Security Appliance. This is independent of whether you have upgraded Cisco Adaptive Security Appliance also.

Use one of the following upgrade procedures when you upgrade both Cisco Unified Presence and Cisco Adaptive Security Appliance in your existing federation deployment:

Upgrade Procedure Option 1:

1. Upgrade Cisco Unified Presence to Release 8.x.
2. Configure NAT rules for port 5080 on Cisco Adaptive Security Appliance.
3. Confirm that federation is working in your deployment after the Cisco Unified Presence upgrade.
4. Upgrade Cisco Adaptive Security Appliance to Release 8.3.
5. Confirm that federation is working in your deployment after the Cisco Adaptive Security Appliance upgrade.

Upgrade Procedure Option 2:

1. Upgrade both Cisco Unified Presence nodes to Release 8.x and Cisco Adaptive Security Appliance to Release 8.3.
2. After both upgrades, configure NAT rules for port 5080 on Cisco Adaptive Security Appliance.
3. Confirm that federation is working in your deployment.

These are the commands you require to open port 5080 for each Cisco Unified Presence Release 8.x node that sits behind Cisco Adaptive Security Appliance:

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Security Appliance Release 8.3 NAT Command

`static (inside,outside) tcp <public cup ip address> 5080 <routing cup private address> 5080 netmask 255.255.255.255`
 	
`static (inside,outside) tcp <public cup ip address> 45080 <intercluster cup8 private address> 5080 netmask 255.255.255.255`
 	
Note Configure these commands for each intercluster Cisco Unified Presence 8.x server, and use a different arbitrary port for each.
	`object service obj_tcp_source_eq_5080`
	`# service tcp source eq 5080`
	
	`nat (inside,outside) source static obj_host_<routing cupprivate address> obj_host_<public cup ip address> serviceobj_tcp_source_eq_5080 obj_tcp_source_eq_5080`
	
	`object service obj_tcp_source_eq_45080`
	`# service tcp source eq 45080`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address>service obj_tcp_source_eq_5080 obj_tcp_source_eq_45080`
	
	Note Configure these commands for each intercluster Cisco Unified Presence 8.x server, and use a different arbitrary port for each.