Cisco Adaptive Security Appliance Configuration for SIP Federation

This section provides information on Cisco Adaptive Security Appliance Configuration for SIP Federation.

Cisco Adaptive Security Appliance Unified Communication Wizard

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

A configuration example showing the Unified Communication wizard is provided on the Adaptive Security Appliance documentation wiki, see the URL below.

Related Information

Cisco Unified Presence 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 external domain servers (for example, Microsoft Access Edge/Access Proxy).
- Use the second interface as the inside or internal interface. This is the interface to the IM and Presence Service 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 the Cisco Adaptive Security Appliance sets the security level to 100 by default.
- Please refer to the *CiscoSecurity Appliance Command Line Configuration Guide* for details on configuring the external and internal interfaces through 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 choosing **Configuration** > **Device Setup** > **Interfaces**.

Configure Static IP Routes

The 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 the 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 the Cisco Adaptive Security Appliance, refer to the *CiscoSecurity Appliance Command Line Configuration Guide*.

Before you begin

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

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

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

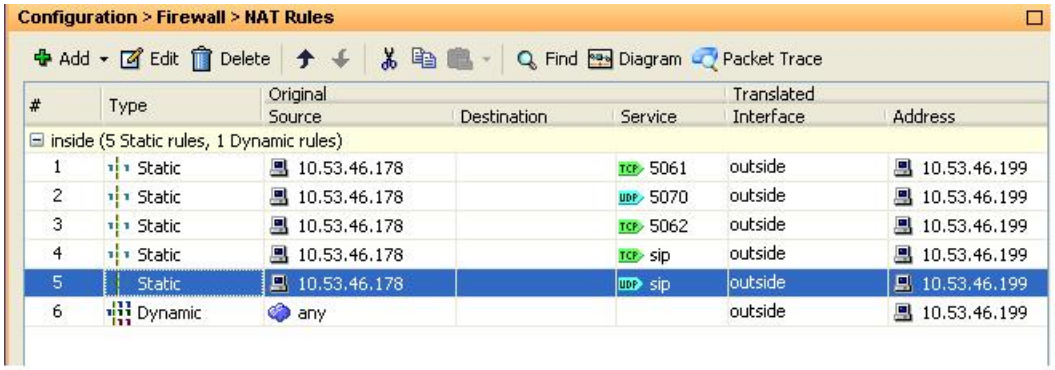
```
hostname(config)# route inside dest_ip mask gateway_ip
```

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 choosing **Configuration** > **Device Setup** > **Routing** > **Static routes**.

Figure 1: Viewing Static Routes Through ASDM



What to do next

Port Address Translation (PAT), on page 3

Port Address Translation (PAT)

This section explains the concept of Port Address Translation.

Port Address Translation for This Integration

Note You also use Port Address Translation if you federate with another IM and Presence Service enterprise deployment in an external domain.

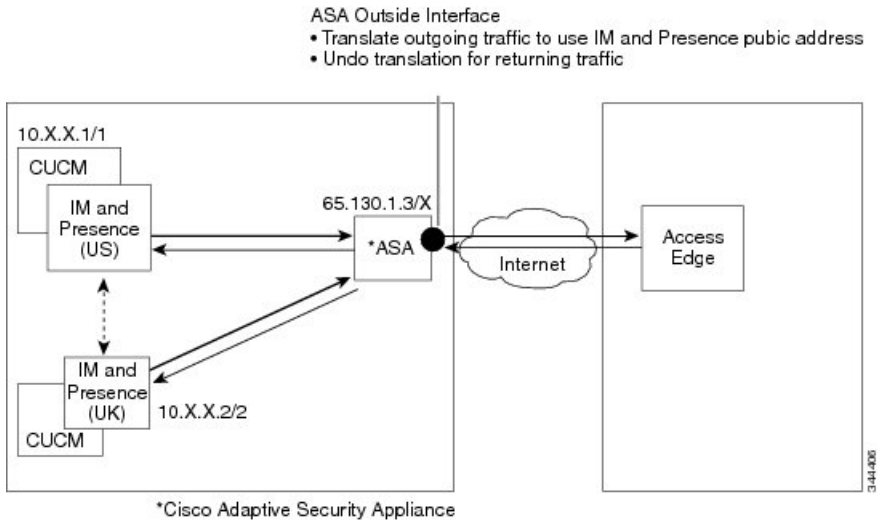
For this integration, Cisco Adaptive Security Appliance uses Port Address Translation (PAT) and static PAT for message address translation. Cisco Adaptive Security Appliance does not use Network Address Translation (NAT) for this integration.

This integration uses PAT to translate messages sent from the IM and Presence Service to an external 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 can be routed 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.

The Cisco Adaptive Security Appliance translates messages sent from the IM and Presence Service to an external domain (private to public messages) by changing the private IP address and port on the IM and Presence Service to a public IP address and one or more public port(s). Therefore, a local IM and Presence Service domain only uses one public IP address. The Cisco IM and Presence Service 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 the following figure.

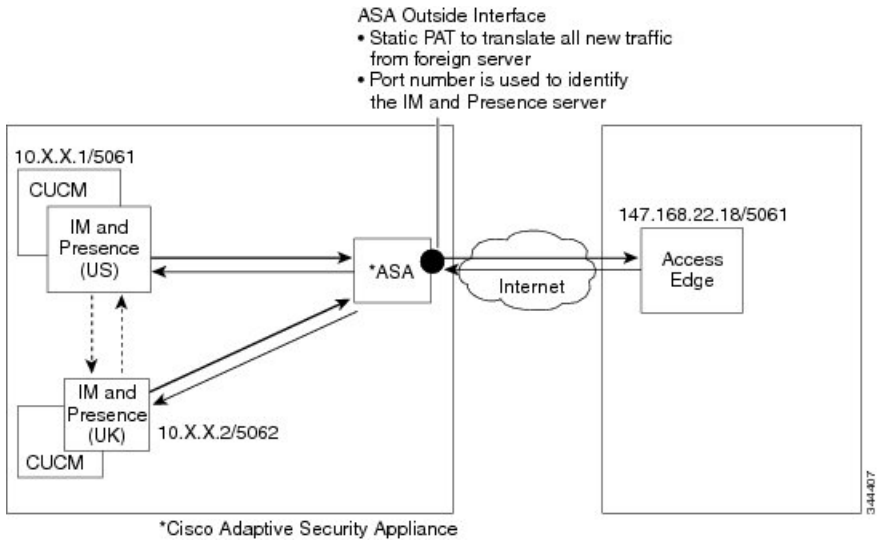
Figure 2: Example PAT for Messages Originating from the IM and Presence Service to an External Domain



For new messages sent from an external domain to the IM and Presence Service, the Cisco Adaptive Security Appliance uses static PAT to map any message sent to the public IP address and port for the IM and Presence Service to a designated IM and Presence Service node. 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 IM and Presence Service node to handle the message request, as shown in the following figure.

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

Figure 3: Static PAT for Messages Originating From an External 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 the 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 through 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 IM and Presence Service public address.

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

Table 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 IM and Presence Service nodes on the inside interface, with no other firewall traffic.	**global (outside) 1** *public_imp_address* **nat (inside) 1 0 0**	**object network obj_any host 0.0.0.0 nat (inside,outside) dynamic** *public_imp_address*

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 is one IM and Presence Service node on the inside interface, with other firewall traffic.	**global (outside) 1** *public_imp_address* **nat (inside) 1** *private_imp_address* **255.255.255.255 global (outside) 2 interface nat (inside) 2 0 0**	**host** *private_imp_address* **nat (inside,outside) dynamic** *public_imp_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 IM and Presence Service nodes on the inside interface, with other firewall traffic.	**global (outside) 1** *public_imp_ip* **nat (inside) 1** *private_imp_net private_imp_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_imp_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 of the table assumes that when there are multiple IM and Presence Service nodes located behind the Cisco Adaptive Security Appliance, and these IM and Presence Service nodes are all on the same subnet. Specifically, if all the inside IM and Presence Service nodes are on the 2.2.2.x/24 network, the NAT command is: **nat (inside) 1 2.2.2.0 255.255.255.0**

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 and 5080.
- Configure a separate static PAT command on UDP for port 5080.

This integration uses the following ports:

- 5060 - the 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, 5080 - The IM and Presence Service uses these ports in the SIP VIA/CONTACT headers.

Note You can check the peer auth listener port on the IM and Presence Service by logging in to **Cisco Unified CM IM and Presence Administration** and choosing **System** > **Application Listeners**.

Related Information -

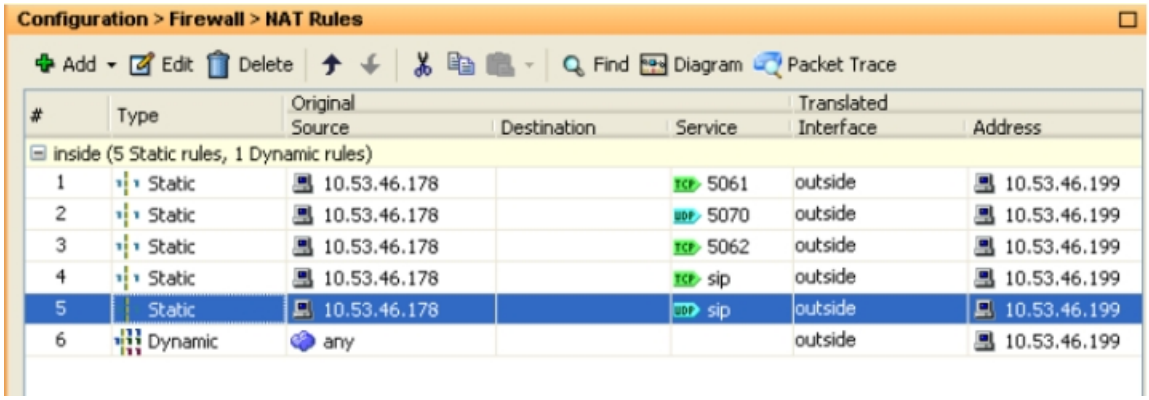
Sample Static PAT Commands

Sample Cisco Adaptive Security Appliance Configuration

NAT Rules in ASDM

You can view the NAT rules in ASDM by choosing **Configuration** > **Firewall** > **NAT Rules**. The first five NAT rules shown in the following figure are the static PAT entries, and the final dynamic entry is the outgoing PAT configuration that maps any outgoing traffic to the public IM and Presence Service IP address and port.

Figure 4: Viewing NAT Rules in ASDM



Related Information

Sample Static PAT Commands

Sample Cisco Adaptive Security Appliance Configuration

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 the IM and Presence Service Node

The following table shows the PAT commands for the routing the IM and Presence Service 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 2: PAT Commands for Routing the IM and Presence Service Node

Cisco Adaptive Security Appliance Release 8.2 Static Commands	Cisco Adaptive Security Appliance Release 8.3 NAT
static (inside,outside) tcp *public_imp_ip_address* **5061** *routing_imp_private_address* **5062 netmask 255.255.255.255** If the routing IM and Presence Service peer auth listening port is 5061, use the command: **static (inside,outside) tcp** *public_imp_ip_address* **5061** *routing_imp_private_address* **5061 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **5060** *routing_imp_private_address* **5060 netmask 255.255.255.255**	**object network** *obj_host_public_imp_ip_addres* **network** *obj_host_10.10.10.10*) **#host** *public_i* **object network** *obj_host_routing_imp_private_* *routing_imp_private_address* **object service** *obj_tcp_source_eq_5061* **servic** **object service** *obj_tcp_source_eq_5062* **servic** **nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_host_* **service** *obj_tcp_source_eq_5062 obj_tcp_sourc* If the routing IM and Presence Service peer auth liste command: **nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_host_* **service** *obj_tcp_source_eq_5061 obj_tcp_sourc*
--	**object service** *obj_tcp_source_eq_5080* **servic** **nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_host_* **service** *obj_tcp_source_eq_5080 obj_tcp_sourc*
--	**object service** *obj_tcp_source_eq_5060* **servic** **Note** 5060 displays as "sip" in the service obj **nat (inside,outside) source static** *obj_host_routing_imp_private_addr* *obj_host_public_imp_ip_address* **se** *obj_tcp_source_eq_5060 obj_tcp_so*
static (inside,outside) tcp *public_imp_ip_address* **5062** *routing_imp_private_address* **5062 netmask 255.255.255.255**	**nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_host_* **service obj_tcp_source_eq_5062 obj_tcp_sourc**

PAT Configuration for Intercluster or Intracluster IM and Presence Service Nodes

In a multinode or an intercluster IM and Presence Service deployment, if the non-routing nodes in the IM and Presence Service clusters communicate directly with the 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 an IM

and Presence Service intercluster or intracluster server. For example 45080 uniquely maps to one node and 55080 uniquely maps to another node.

The following table shows the NAT commands for the non-routing IM and Presence Service nodes. Repeat the commands for each non-routing IM and Presence Service 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 3: NAT Commands for Non-Routing IM and Presence Service Nodes

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Security Appliance Release 8.3 NA
static (inside,outside) tcp *public_imp_address* **45062** *intercluster_imp_private_address* **5062 netmask 255.255.255.255** If the intercluster IM and Presence Service peer auth listening port is 5061, use the command: **static (inside,outside) tcp** *public_imp_address* **45061** *intercluster_imp_private_address* **5061 netmask 255.255.255.255**	**object network** *obj_host_intercluster_imp_p intercluster_imp_private_address* **object service** *obj_tcp_source_eq_45062* **serv** **nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj obj_tcp_source_eq_45062* If the intercluster IM and Presence Service peer aut the command: **object service** *obj_tcp_source_eq_45061* **serv nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj obj_tcp_source_eq_45061*
static (inside,outside) tcp *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255**	**object service** *obj_tcp_source_eq_45080* **serv nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj obj_tcp_source_eq_45080*
static (inside,outside) tcp *public_imp_ip_address* **45060** *intercluster_imp_private_address* **5060 netmask 255.255.255.255**	**object service** *obj_tcp_source_eq_45060* **serv nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj obj_tcp_source_eq_45060*

Related Information -

Static PAT for New Requests

PAT Configuration for Routing the IM and Presence Service Node

Cisco Adaptive Security Appliance Upgrade Options for Existing Deployments

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

Note Once you upgrade to IM and Presence Service Release 9.0, you must open port 5080 on the Cisco Adaptive Security Appliance for each IM and Presence Service 9.0 node located behind the Cisco Adaptive Security Appliance. This is independent of whether you have upgraded the Cisco Adaptive Security Appliance also.

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

Upgrade Procedure Option 1:

1. Upgrade the IM and Presence Service to Release 9.0.
2. Configure NAT rules for port 5080 on the Cisco Adaptive Security Appliance.
3. Confirm that federation is working in your deployment after the IM and Presence Service upgrade.
4. Upgrade the 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 the IM and Presence Service nodes to Release 9.0 and Cisco Adaptive Security Appliance to Release 8.3.
2. After both upgrades, configure NAT rules for port 5080 on the 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 IM and Presence Service Release 9.0 node that sits behind Cisco Adaptive Security Appliance.

Table 4: Cisco ASA commands to open port 5080

Cisco Adaptive Security Appliance Release 8.2 Static Command	Cisco Adaptive Secur
static (inside,outside) tcp *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255** **Note** Configure these commands for each intercluster IM and Presence Service 9.0 node, and use a different arbitrary port for each.	**object service** *obj* **nat (inside,outsid** *obj_host_public_im* **object service** *obj* **nat (inside,outsid** *obj_host_public_im* **Note** Configure a differen