Sample Cisco Adaptive Security Appliance Configuration

This section provides information on Sample Cisco Adaptive Security Appliance Configuration.

Sample PAT Commands and Access List Configuration for SIP Federation

This section provides a sample configuration for a IM and Presence Service node that is federating with an external OCS enterprise deployment. There are two additional intercluster IM and Presence Service nodes in the local enterprise deployment.

The following values are used in this sample configuration:

- Public IM and Presence Service IP Address = 10.10.10.10
- Private Routing IM and Presence Service IP Address = 1.1.1.1
- Private Second IM and Presence Service IP Address = 2.2.2.2
- Private Third IM and Presence Service IP Address = 3.3.3.3
- Peer Auth Listener Port on IM and Presence Service = 5062
- Netmask = 255.255.255.255
- External Domain = abc.com
- Microsoft OCS External Interface = 20.20.20.20

These PAT commands are defined for the (routing) IM and Presence Service node:

(Cisco Adaptive Security Appliance Release 8.2:)

```
static (inside,outside) tcp 10.10.10.10 5061 1.1.1.1 5062 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 5080 1.1.1.1 5080 netmask 255.255.255.255
```

```
static (inside,outside) tcp 10.10.10.10 5060 1.1.1.1 5060 netmask 255.255.255.255
```

(Cisco Adaptive Security Appliance Release 8.3:)

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5061 obj_tcp_source_eq_5062

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5080 obj_tcp_source_eq_5080

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5060 obj_tcp_source_eq_5060
```

These PAT commands are defined for the two additional intercluster IM and Presence Service nodes in the enterprise deployment:

(Cisco Adaptive Security Appliance Release 8.2:)

```
static (inside,outside) tcp 10.10.10.10 45080 2.2.2.2 5080 netmask 255.255.255.255

static (inside,outside) udp 10.10.10.10 55070 3.3.3.3 5070 netmask 255.255.255.255

static (inside,outside) tcp 10.10.10.10 55070 3.3.3.3 5070 netmask 255.255.255.255

static (inside,outside) udp 10.10.10.10 45062 2.2.2.2 5062 netmask 255.255.255.255

static (inside,outside) tcp 10.10.10.10 55062 3.3.3.3 5062 netmask 255.255.255.255
```

(Cisco Adaptive Security Appliance Release 8.3:)

```
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5080 obj_tcp_source_eq_45080

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5070 obj_tcp_source_eq_55070

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_udp_source_eq_5070 obj_udp_source_eq_55070

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5062 obj_tcp_source_eq_45062

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5062 obj_tcp_source_eq_55062
```

The corresponding access lists for this configuration are provided below. Note that for each external domain that you federate with, you must add access lists similar to these access lists for the domain abc.com.

(Cisco Adaptive Security Appliance Release 8.2:)

```
access-list ent_imp_to_abc extended permit tcp host 1.1.1.1 host 20.20.20.20 eq 5061

access-list ent_abc_to_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq 5061

access-list ent_second_imp_to_abc extended permit tcp host 2.2.2.2 host 20.20.20.20 eq 5061

access-list ent_third_imp_to_abc extended permit tcp host 3.3.3.3 host 20.20.20.20 eq 5061

access-list ent_abc_to_second_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq
45061

access-list ent_abc_to_third_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq
55061
```

(Cisco Adaptive Security Appliance Release 8.3:)

```
access-list ent_imp_to_abc extended permit tcp host 1.1.1.1 host 20.20.20.20 eq 5061
access-list ent_abc_to_imp extended permit tcp host 20.20.20.20 host 1.1.1.1 eq 5062
access-list ent_second_imp_to_abc extended permit tcp host 2.2.2.2 host 20.20.20.20 eq 5061
access-list ent_third_imp_to_abc extended permit tcp host 3.3.3.3 host 20.20.20.20 eq 5061
access-list ent_abc_to_second_imp extended permit tcp host 20.20.20.20 host 2.2.2.2 eq 5062
access-list ent_abc_to_third_imp extended permit tcp host 20.20.20.20 host 3.3.3.3 eq 5062
```

Associate each of your access lists with the a class map:

```
class-map ent_imp_to_abc
match access-list ent_imp_to_abc
class-map ent_abc_to_imp
match access-list ent_abc_to_imp
class-map ent_second_imp_to_abc
match access-list ent_second_imp_to_abc
class-map ent_third_imp_to_abc
match access-list ent_third_imp_to_abc
class-map ent_abc_to_second_imp
match access-list ent_abc_to_second_imp
class-map ent_abc_to_third_imp
match access-list ent_abc_to_third_imp
```

Update the global policy map for each class map you created. In this example, the TLS proxy instance for TLS connections initiated by the IM and Presence Service is called “imp_to_external”, and the TLS proxy instance for TLS connections initiated by an external domain is called "external_to_imp".

```
policy-map global_policy
class ent_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external
policy-map global_policy
class ent_abc_to_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp
policy-map global_policy
class ent_second_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external
policy-map global_policy
class ent_third_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external
```

```
policy-map global_policy
class ent_abc_to_second_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp
policy-map global_policy
class ent_abc_to_third_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp
```

Sample Access List Configuration for XMPP Federation

Note The examples in this section apply to the Cisco Adaptive Security Appliance Release 8.3.

Any Address Access to any Address on Port 5269

This example access list configuration allows from any address to any address on port 5269:

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

Any Address Access to any Single XMPP Federation Node on Port 5269

This example access list configuration allows from any address to any single XMPP federation node on port 5269. The following values are used in this example:

- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- XMPP federation listening port = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
```

Any Address Access to Specific XMPP Federation Nodes Published in DNS

This example access list configuration allows from any address to specific XMPP federation nodes published in DNS.

Note The public addresses are published in DNS, but the private addresses are configured in the access-list command.

The following values are used in this sample configuration:

- • Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- • Private second IM and Presence Service Release 9.x IP address= 2.2.2.2
- • Private third IM and Presence Service Release 9.x IP address = 3.3.3.3

• • XMPP federation listening port = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
access-list ALLOW-ALL extended permit tcp any host 2.2.2.2 eq 5269
access-list ALLOW-ALL extended permit tcp any host 3.3.3.3 eq 5269
```

Specific Federated Domain Only Access to Specific XMPP Federation Nodes Published in DNS

This example access list configuration allows only from a specific federated domain interface to specific XMPP federation nodes published in DNS.

Note The public addresses are published in DNS, but the private addresses are configured in the access-list command.

The following values are used in this sample configuration:

- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3
- XMPP federation listening port = 5269
- External interface of the external XMPP enterprise = 100.100.100.100

```
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 1.1.1.1 eq 5269
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 2.2.2.2 eq 5269
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 3.3.3.3 eq 5269
```

Sample NAT Configuration for XMPP Federation

Example 1: Single node with XMPP federation enabled

The following values are used in this sample configuration:

- Public IM and Presence Service IP address = 10.10.10.10
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- XMPP federation listening port = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
```

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

Example 2: Multiple nodes with XMPP federation, each with a public IP address in DNS

The following values are used in this sample configuration:

- Public IM and Presence Service IP addresses = 10.10.10.10, 20.20.20.20, 30.30.30.30
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3
- XMPP federation listening port = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_20.20.20.20 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_20.20.20.20 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_30.30.30.30 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_30.30.30.30 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

Example 3: Multiple nodes with XMPP federation, but a single public IP address in DNS with arbitrary ports published in DNS (PAT).

The following values are used in this sample configuration:

- Public IM and Presence Service IP Address = 10.10.10.10
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1, port 5269
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2, arbitrary port 25269
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3, arbitrary port 35269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_25269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_35269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_35269
```