Cisco Adaptive Security Appliance（ASA）の設定例

SIP フェデレーションの PAT コマンドとアクセス リスト設定の例

ここでは、外部 OCS 企業配置とフェデレーションを実行する IM and Presence サーバの設定例を示します。 ローカルな企業配置の場合、さらに 2 つのクラスタ間 IM and Presence サーバがあります。

この設定例では、次の値が使用されます。

- IM and Presence のパブリック IP アドレス = 10.10.10.10
- IM and Presence のプライベート ルーティング IP アドレス = 1.1.1.1
- IM and Presence のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence のプライベート サード IP アドレス = 3.3.3.3
- IM and Presence のピア認証リスナー ポート = 5062
- ネットマスク = 255.255.255.255
- 外部ドメイン = abc.com
- Microsoft OCS 外部インターフェイス = 20.20.20.20

次の PAT コマンドが（ルーティング）IM and Presence サーバ用に定義されています。

（Cisco Adaptive Security Appliance Release 8.2：）

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

企業配置の場合、さらに 2 つのクラスタ間 IM and Presence サーバ用に次の PAT コマンドを定義します。

（Cisco Adaptive Security Appliance Release 8.2：）

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

この設定に対応するアクセスリストを次に示します。フェデレーションを行う外部ドメインごとに、ドメイン abc.com 用に次のようなアクセス リストを追加する必要があります。

（Cisco Adaptive Security Appliance Release 8.2：）

```
access-list ent_cup_to_abc extended permit tcp host 1.1.1.1 host
20.20.20.20 eq 5061access-list ent_abc_to_cup extended permit tcp host
20.20.20.20 host 10.10.10.10 eq 5061
```

```
access-list ent_secondcup_to_abc extended permit tcp host 2.2.2.2 host
20.20.20.20 eq 5061
access-list ent_thirdcup_to_abc extended permit tcp host 3.3.3.3 host
20.20.20.20 eq 5061
access-list ent_abc_to_secondcup extended permit tcp host 20.20.20.20
host 10.10.10.10 eq 45061
access-list ent_abc_to_thirdcup 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_cup_to_abc extended permit tcp host 1.1.1.1 host
20.20.20.20 eq 5061access-list ent_abc_to_cup extended permit tcp host
20.20.20.20 host 1.1.1.1 eq 5062
access-list ent_secondcup_to_abc extended permit tcp host 2.2.2.2 host
20.20.20.20 eq 5061
access-list ent_thirdcup_to_abc extended permit tcp host 3.3.3.3 host
20.20.20.20 eq 5061
access-list ent_abc_to_secondcup extended permit tcp host 20.20.20.20
host 2.2.2.2 eq 5062
access-list ent_abc_to_thirdcup 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_cup_to_abc
match access-list ent_cup_to_abc

class-map ent_abc_to_cup match
access-list ent_abc_to_cup

class-map ent_secondcup_to_abc
match access-list ent_secondcup_to_abc

class-map ent_thirdcup_to_abc
match access-list ent_thirdcup_to_abc

class-map ent_abc_to_secondcup
match access-list ent_abc_to_secondcup

class-map ent_abc_to_thirdcup
match access-list ent_abc_to_thirdcup
```

作成した各クラス マップのグローバル ポリシー マップを更新します。 この例では、IM and Presence から開始される TLS 接続の TLS プロキシ インスタンスは “cup_to_foreign” です。また、外部ドメインから開始される TLS 接続の TLS プロキシ インスタンスは "foreign_to_cup" です。

```
policy-map global_policy
class ent_cup_to_abc
inspect sip sip_inspect tls-proxy ent_cup_to_foreign

policy-map global_policy
class ent_abc_to_cup
inspect sip sip_inspect tls-proxy ent_foreign_to_cup

policy-map global_policy
class ent_secondcup_to_abc
inspect sip sip_inspect tls-proxy ent_cup_to_foreign
```

```
policy-map global_policy
class ent_thirdcup_to_abc
inspect sip sip_inspect tls-proxy ent_cup_to_foreign

policy-map global_policy
class ent_abc_to_secondcup
inspect sip sip_inspect tls-proxy ent_foreign_to_cup

policy-map global_policy
class ent_abc_to_thirdcup
inspect sip sip_inspect tls-proxy ent_foreign_to_cup
```

XMPP フェデレーション用のアクセス リストの設定例

（注） このセクションの例は、Cisco Adaptive Security Appliance Release 8.3 に適用できます。

例 1：このアクセス リストの設定例では、ポート 5269 上で任意のアドレスから任意のアドレスへの転送が許可されます。

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

例 2：このアクセス リストの設定例では、ポート 5269 上で任意のアドレスから任意のシングル XMPP フェデレーション ノードへの転送が許可されます。 この例では、次の値が使用されます。

- XMPP フェデレーション IM and Presence Release 9.x のプライベート IP アドレス = 1.1.1.1
- XMPP フェデレーションのリスニング ポート = 5269

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

例 3：このアクセス リストの設定例では、任意のアドレスから、DNS で公開された特定の XMPP フェデレーション ノードへの転送が許可されます。

（注） これらのパブリック アドレスは DNS で公開されますが、access-list コマンドにはプライベート アドレスが設定されます。

この設定例では、次の値が使用されます。

- XMPP フェデレーション IM and Presence Release 9.x のプライベート IP アドレス = 1.1.1.1
- IM and Presence Release 9.x のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence Release 9.x のプライベート サード IP アドレス = 3.3.3.3
- XMPP フェデレーションのリスニング ポート = 5269

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

例 4：このアクセス リストの設定例では、特定のフェデレーテッド ドメイン インターフェイスから、DNS で公開された特定の XMPP フェデレーション ノードへの転送だけが許可されます。

（注） これらのパブリック アドレスは DNS で公開されますが、access-list コマンドにはプライベート アドレスが設定されます。

この設定例では、次の値が使用されます。

- XMPP フェデレーション IM and Presence Release 9.x のプライベート IP アドレス = 1.1.1.1
- IM and Presence Release 9.x のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence Release 9.x のプライベート サード IP アドレス = 3.3.3.3
- XMPP フェデレーションのリスニング ポート = 5269
- 外部の XMPP 企業の外部インターフェイス = 100.100.100.100

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

XMPP フェデレーション用の NAT の設定例

例 1：XMPP フェデレーションがイネーブルのシングル ノード

この設定例では、次の値が使用されます。

- IM and Presence のパブリック IP アドレス = 10.10.10.10
- XMPP フェデレーション IM and Presence Release 9.x のプライベート IP アドレス = 1.1.1.1
- XMPP フェデレーションのリスニング ポート = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1
obj_host_10.10.10.10
serviceobj_udp_source_eq_5269obj_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
```

例 2：XMPP フェデレーションが設定され、それぞれが DNS 内のパブリック IP アドレスを持つ複数のノード

この設定例では、次の値が使用されます。

- IM and Presence のパブリック IP アドレス = 10.10.10.10、20.20.20.20, 30.30.30.30
- XMPP フェデレーション IM and Presence Release 9.x のプライベート IP アドレス = 1.1.1.1
- IM and Presence Release 9.x のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence Release 9.x のプライベート サード IP アドレス = 3.3.3.3
- XMPP フェデレーションのリスニング ポート = 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
```

例 3：XMPP フェデレーションが設定されているが、DNS 内のパブリック IP アドレスは単一で、DNS で公開された任意のポートを持つ

複数のノード（PAT）。

この設定例では、次の値が使用されます。

- IM and Presence のパブリック IP アドレス = 10.10.10.10
- XMPP フェデレーション IM and Presence Release 9.x のプライベート IP アドレス = 1.1.1.1、ポート 5269
- IM and Presence Release 9.x のプライベート セカンド IP アドレス = 2.2.2.2、任意のポート 25269
- IM and Presence Release 9.x のプライベート サード IP アドレス = 3.3.3.3、任意のポート 35269

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