

オーバーラップ シナリオが付いている ASA VPN の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[両 VPN エンドポイントの変換](#)

[ASA1](#)

[使用中のサブネットのための必要なオブジェクトを作成して下さい](#)

[NAT の設定例を設定して下さい](#)

[変換されたサブネットで暗号 ACL を設定して下さい](#)

[関連した暗号構成](#)

[ASA2](#)

[使用中のサブネットのための必要なオブジェクトを作成して下さい](#)

[NAT の設定例を設定して下さい](#)

[変換されたサブネットで暗号 ACL を設定して下さい](#)

[関連した暗号構成](#)

[確認](#)

[ASA1](#)

[ASA2](#)

[オーバーラップ スポークとのハブ・アンド・スポーク トポロジー](#)

[ASA1](#)

[使用中のサブネットのための必要なオブジェクトを作成して下さい](#)

[変換するために手動文を作成して下さい:](#)

[変換されたサブネットで暗号 ACL を設定して下さい](#)

[関連した暗号構成](#)

[ASA2 \(SPOKE1 \)](#)

[設定して下さい変換されたサブネット \(10.20.20.0 /24 \) に行く暗号 ACL を](#)

[関連した暗号構成](#)

[R1 \(SPOKE2 \)](#)

[設定して下さい変換されたサブネット \(10.30.30.0 /24 \) に行く暗号 ACL を](#)

[関連した暗号構成](#)

[確認](#)

[ASA1](#)

[ASA2 \(SPOKE1 \)](#)

[R1 \(SPOKE2 \)](#)

[トラブルシューティング](#)

[セキュリティ アソシエーションのクリア](#)

[NAT 設定を検討して下さい](#)

概要

この資料は VPN トラフィックを変換するのに使用されるステップを記述したものです LAN-to-LAN な (L2L) IPSecトンネルにオーバーラップシナリオおよびまたポート アドレス変換 (PAT) の 2 適応型セキュリティ アプライアンス (ASA) の間でインターネットトラフィック移動する。

前提条件

要件

設定例に進む前に、Cisco 適応型セキュリティ アプライアンスにインターフェイスの IP アドレスが設定され、基本的な接続が確立されていることを確認します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア ソフトウェア バージョン 8.3 およびそれ以降。

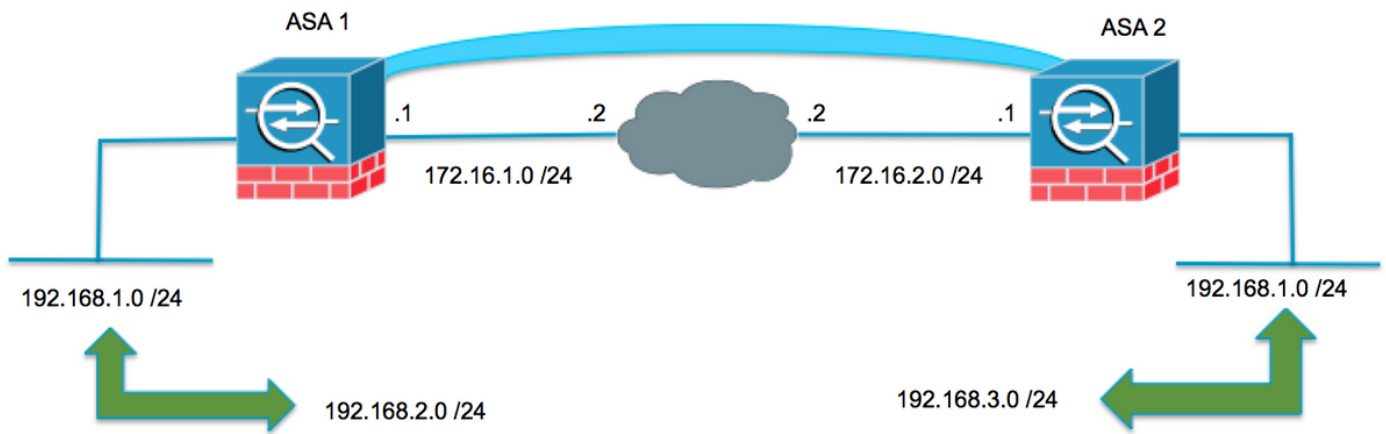
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

各デバイスに private が、その後ろの保護されたネットワークあります。オーバーラップシナリオでは、VPN を渡る通信は決してトラフィックが同じサブネットの IP アドレスに送信されるのでパケットが決してローカルサブネットを去らないので起こりません。これは以降のセクションで説明されているようにネットワーク アドレス変換 (NAT) と達成することができます。

両 VPN エンドポイントの変換

VPN 保護されたネットワークがおよびオーバーラップするとき設定は両エンドポイントで修正することができます; 遠隔に行くときサブネットを変換した NAT が別のサブネットにローカルネットワークを変換するのに使用することができます。



ASA1

使用中のサブネットのための必要なオブジェクトを作成して下さい

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.3.0 255.255.255.0
```

NAT の設定例を設定して下さい

だけリモート サブネットに行った場合だけ別のサブネットにローカルネットワークを変換するために手動文を作成して下さい (また変換される)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

変換されたサブネットで暗号 ACL を設定して下さい

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE
```

関連した暗号構成

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

ASA2

使用中のサブネットのための必要なオブジェクトを作成して下さい

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.2.0 255.255.255.0
```

NAT の設定例を設定して下さい

だけリモート サブネットに行った場合だけ別のサブネットにローカルネットワークを変換するために手動文を作成して下さい (また変換される)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

変換されたサブネットで暗号 ACL を設定して下さい

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rel
```

関連した暗号構成

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

確認

ここでは、設定が正常に動作していることを確認します。

ASA1

```
ASA1(config)# sh cry isa sa
```

```
IKEv1 SAs:
```

```
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 172.16.2.1
   Type    : L2L                Role    : initiator
   Rekey   : no                 State   : MM_ACTIVE
```

```
There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
```

```

interface: outside
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

  access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0
  255.255.255.0
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer: 172.16.2.1

  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
  path mtu 1500, ipsec overhead 74(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: F90C149A
  current inbound spi : 6CE656C7

inbound esp sas:
  spi: 0x6CE656C7 (1827034823)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000003FF

outbound esp sas:
  spi: 0xF90C149A (4178318490)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

ASA2

```
ASA2(config)# show crypto isa sa
```

```
IKEv1 SAs:
```

```

Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 172.16.1.1
   Type    : L2L                Role    : responder
   Rekey   : no                 State   : MM_ACTIVE

```

```

There are no IKEv2 SAs
ASA2(config)# show crypto ipsec sa
interface: outside

```

Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

```
access-list VPN-TRAFFIC extended permit ip 192.168.3.0 255.255.255.0 192.168.2.0
255.255.255.0
```

```
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 6CE656C7
current inbound spi : F90C149A
```

inbound esp sas:

```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28684)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003FF
```

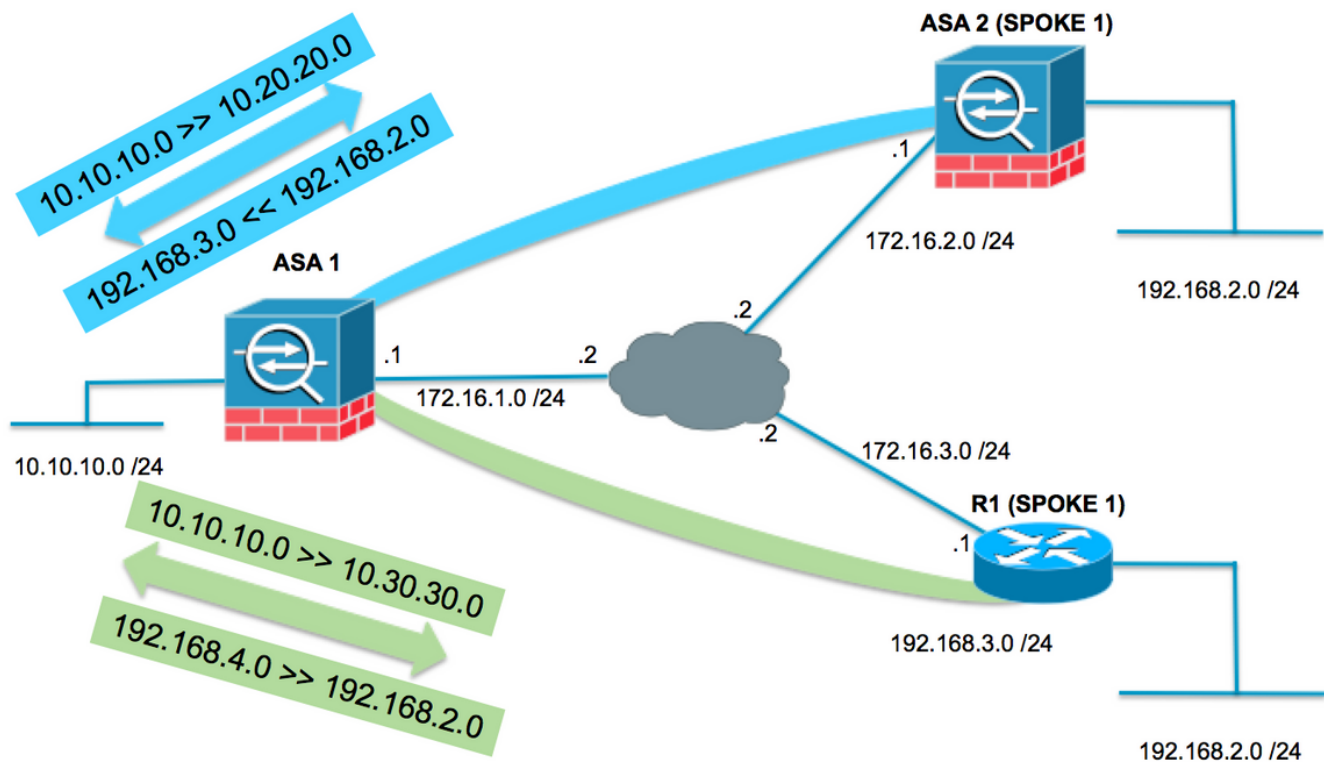
outbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28683)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

オーバーラップ スポークとのハブ・アンド・スポーク トポロジ

—

following トポロジでは、スポークに両方ともハブの方の IPsec トンネルに保護される必要がある
同じサブネットワークがあります。スポークの管理を NAT 設定はハブだけで回避策に促進するために
オーバーラップ問題行われます。



ASA1

使用中のサブネットのための必要なオブジェクトを作成して下さい

```
object network LOCAL
  subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
  subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
  subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
  subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
  subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
  subnet 192.168.4.0 255.255.255.0
```

変換するために手動文を作成して下さい:

- SPOKE1 (192.168.2.0 /24) に行く場合の 10.20.20.0 /24 へのローカルネットワーク 10.10.10.0 /24。
- 10.20.20.0 /24 に来る場合の 192.168.3.0 /24 への SPOKE1 ネットワーク 192.168.2.0 /24。
- SPOKE3 (192.168.2.0 /24) に行く場合の 10.30.30.0 /24 へのローカルネットワーク 10.10.10.0 /24。
- 10.30.30.0 /24 に来る場合の 192.168.4.0 /24 への SPOKE2 ネットワーク 192.168.2.0 /24。

```
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-SPOKE1 SPOKES-NETWORK
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-SPOKE2 SPOKES-NETWORK
```

変換されたサブネットで暗号 ACL を設定して下さい

```
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS
```

関連した暗号構成

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

ASA2 (SPOKE1)

設定して下さい変換されたサブネット (10.20.20.0 /24) に行く暗号 ACL を

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
```

関連した暗号構成

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

R1 (SPOKE2)

設定して下さい変換されたサブネット (10.30.30.0 /24) に行く暗号 ACL を

```
ip access-list extended VPN-TRAFFIC
```



```
permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```

関連した暗号構成

```
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2
```

```
crypto isakmp key secure_PSK address 172.16.1.1
```

```
crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
  mode tunnel
```

```
crypto map MYMAP 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set AES256-SHA
  match address VPN-TRAFFIC
```

```
interface GigabitEthernet0/1
  ip address 172.16.3.1 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  crypto map MYMAP
```

確認

ASA1

```
ASA1(config)# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
  Active SA: 2
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
```

```
1  IKE Peer: 172.16.3.1
   Type    : L2L           Role    : responder
   Rekey   : no           State   : MM_ACTIVE
2  IKE Peer: 172.16.2.1
   Type    : L2L           Role    : responder
   Rekey   : no           State   : MM_ACTIVE
```

```
There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
```

```
interface: outside
```

```
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1
```

```
  access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0
  255.255.255.0
```

```
    local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
```

```
    remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
    current_peer: 172.16.2.1
```

```
  #pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
```

```
  #pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

```
  #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
```

```
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
  #TFC rcvd: 0, #TFC sent: 0
```

#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 79384296
current inbound spi : 2189BF7A

inbound esp sas:

spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF

outbound esp sas:

spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: MYMAP, seq num: 20, local addr: 172.16.1.1

access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0
255.255.255.0

local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.3.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.3.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 65FDF4F5
current inbound spi : 05B7155D

inbound esp sas:

spi: 0x05B7155D (95884637)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes

```
replay detection support: Y
Anti replay bitmap:
  0x00000000 0x0000001F
outbound esp sas:
  spi: 0x65FDF4F5 (1711142133)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 8192, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/2883)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

ASA2 (SPOKE1)

```
ASA2(config)# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1  IKE Peer: 172.16.1.1
   Type      : L2L                Role      : initiator
   Rekey     : no                 State     : MM_ACTIVE
```

```
There are no IKEv2 SAsASA2(config)# show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1
```

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0
255.255.255.0
```

```
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
```

```
current_peer: 172.16.1.1
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
```

```
path mtu 1500, ipsec overhead 74(44), media mtu 1500
```

```
PMTU time remaining (sec): 0, DF policy: copy-df
```

```
ICMP error validation: disabled, TFC packets: disabled
```

```
current outbound spi: 2189BF7A
```

```
current inbound spi : 79384296
```

```
inbound esp sas:
```

```
spi: 0x79384296 (2033730198)
```

```
transform: esp-aes-256 esp-sha-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv1, }
```

```
slot: 0, conn_id: 8192, crypto-map: MYMAP
```

```
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Anti replay bitmap:
  0x00000000 0x000003FF
outbound esp sas:
  spi: 0x2189BF7A (562675578)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 8192, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (4373999/28494)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

R1 (SPOKE2)

```
R3lshow crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	status
172.16.1.1	172.16.3.1	QM_IDLE	1001	ACTIVE

```
IPv6 Crypto ISAKMP SAR1#show crypto ipsec sa
```

```
interface: GigabitEthernet0/1
```

```
  Crypto map tag: MYMAP, local addr 172.16.3.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
```

```
current_peer 172.16.1.1 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
```

```
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
```

```
current outbound spi: 0x5B7155D(95884637)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
  spi: 0x65FDF4F5(1711142133)
```

```
  transform: esp-256-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP
```

```
  sa timing: remaining key lifetime (k/sec): (4188495/2652)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
  spi: 0x5B7155D(95884637)
```

```
  transform: esp-256-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
```

```
  sa timing: remaining key lifetime (k/sec): (4188495/2652)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

セキュリティ アソシエーションのクリア

トラブルシューティングを行う際には、変更を加えた後、既存の SA を必ずクリアしてください。PIX の特権モードで、次のコマンドを使用します。

- `clear crypto ipsec sa` : アクティブな IPSec SA を削除します。
- `clear crypto isakmp sa` : アクティブな IKE SA を削除します。

確認 NAT 設定

- `show nat` 詳細-拡張されるオブジェクト/オブジェクト グループとの NAT 設定を表示します

トラブルシューティングのためのコマンド

ここでは、設定が正常に動作していることを確認します。

[Cisco CLI アナライザ](#) ([登録ユーザ専用](#)) は、特定の `show` コマンドをサポートしています。`show` コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

注: `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』および『[IP Security のトラブルシューティング : debug コマンドの説明と使用](#)』を参照してください。

- `debug crypto ipsec` : フェーズ 2 の IPSec ネゴシエーションを表示します。
- `debug crypto isakmp` : フェーズ 1 の ISAKMP ネゴシエーションを表示します。

関連情報

- [NAT コンフィギュレーション ガイド](#)
- [一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)