

Ejemplo de configuración de ASA VPN con los escenarios que solapan

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Traducción en ambos puntos finales de VPN](#)

[ASA 1](#)

[Cree los objetos necesarios para las subredes funcionando](#)

[Configure la sentencia NAT](#)

[Configure el ACL crypto con las subredes traducidas](#)

[Configuración de criptografía relevante](#)

[ASA 2](#)

[Cree los objetos necesarios para las subredes funcionando](#)

[Configure la sentencia NAT](#)

[Configure el ACL crypto con las subredes traducidas](#)

[Configuración de criptografía relevante](#)

[Verificación](#)

[ASA 1](#)

[ASA 2](#)

[Topología Hub y Spoke con el spokes que solapa](#)

[ASA1](#)

[Cree los objetos necesarios para las subredes funcionando](#)

[Cree las declaraciones manuales para traducir:](#)

[Configure el ACL crypto con las subredes traducidas](#)

[Configuración de criptografía relevante](#)

[ASA2 \(SPOKE1\)](#)

[Configure el ACL crypto que va a la subred traducida \(10.20.20.0 /24\)](#)

[Configuración de criptografía relevante](#)

[R1 \(SPOKE2\)](#)

[Configure el ACL crypto que va a la subred traducida \(10.30.30.0 /24\)](#)

[Configuración de criptografía relevante](#)

[Verificación](#)

[ASA 1](#)

[ASA2 \(SPOKE1\)](#)

[R1 \(SPOKE2\)](#)

[Troubleshooting](#)

[Borre las asociaciones de seguridad](#)

[Revise la configuración del NAT](#)

Introducción

Este documento describe los pasos usados para traducir el tráfico VPN que viaja sobre un túnel IPsec del LAN a LAN (L2L) entre dos dispositivos de seguridad adaptantes (ASA) en los escenarios que solapan y también el Port Address Translation (PAT) el tráfico de Internet.

Prerrequisitos

Requisitos

Asegúrese de haber configurado el dispositivo de seguridad adaptante de Cisco con los IP Addresses en las interfaces, y tenga conectividad básica antes de que usted proceda con este ejemplo de configuración.

Componentes Utilizados

La información de este documento se basa en esta versión del software:

- Versión de software adaptante 8.3 del dispositivo de seguridad de Cisco y posterior.

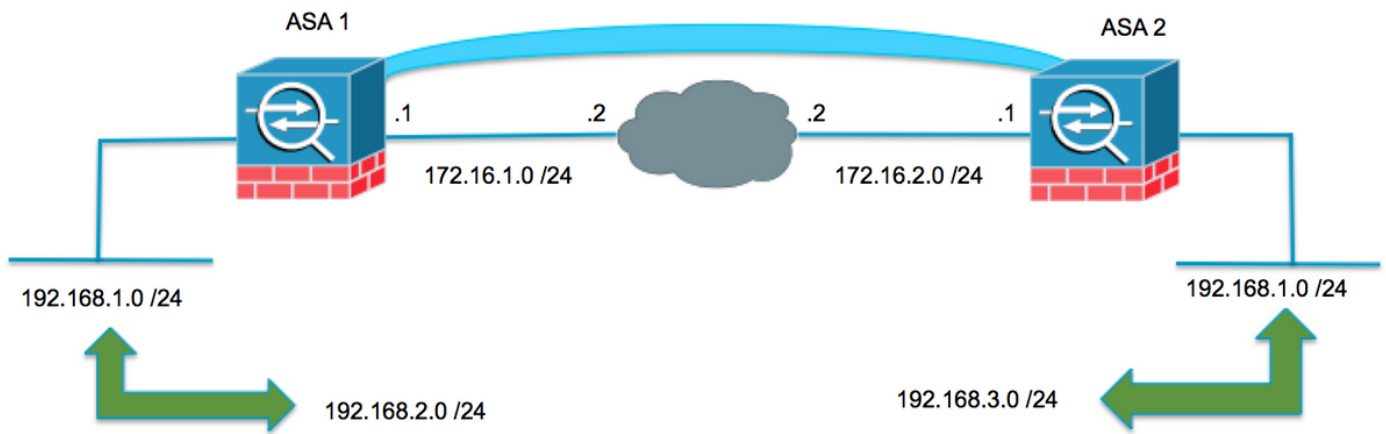
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Cada dispositivo tiene un soldado, red protegida detrás de él. En los escenarios que solapan, la comunicación a través del VPN nunca sucede porque los paquetes nunca salen de la subred local puesto que el tráfico se envía a una dirección IP de la misma subred. Esto se puede lograr con el Network Address Translation (NAT) como se explica en las secciones siguientes.

Traducción en ambos puntos finales de VPN

Cuando las redes protegidas VPN solapan y la configuración se puede modificar en ambos puntos finales; El NAT se puede utilizar para traducir la red local a una diversa subred al ir a la subred traducida remota.



ASA 1

Cree los objetos necesarios para las subredes funcionando

```
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
```

Configure la sentencia NAT

Cree una declaración manual para traducir la red local a una diversa subred solamente al ir a la subred remota (también traducida)

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

Configure el ACL crypto con las subredes traducidas

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

Configuración de criptografía relevante

```
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
```

ASA 2

Cree los objetos necesarios para las subredes funcionando

```
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
```

Configure la sentencia NAT

Cree una declaración manual para traducir la red local a una diversa subred solamente al ir a la subred remota (también traducida)

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

Configure el ACL crypto con las subredes traducidas

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

Configuración de criptografía relevante

```
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

ASA 1

```
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

```

ASA 2

```
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:

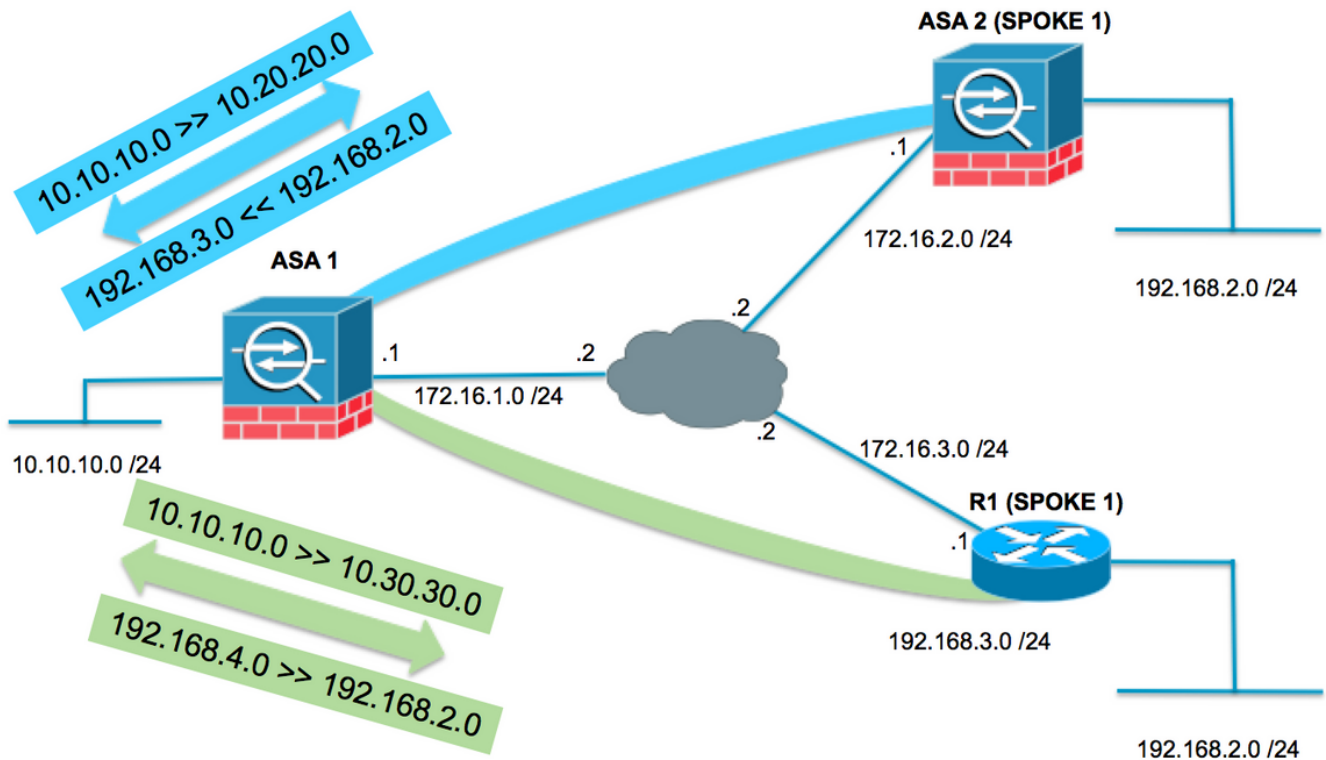
```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28684)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF
```

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
```

Topología Hub y Spoke con el spokes que solapa

En la topología following, ambos spokes tienen la misma subred que necesita ser protegida sobre el túnel IPsec hacia el concentrador. Para facilitar la Administración en el spokes la configuración del NAT a la solución alternativa el problema que solapa se realiza en el concentrador solamente.



ASA1

Cree los objetos necesarios para las subredes funcionando

```

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

```

Cree las declaraciones manuales para traducir:

- La red local 10.10.10.0 /24 a 10.20.20.0 /24 al ir al SPOKE1 (192.168.2.0 /24).
- La red 192.168.2.0 /24 del SPOKE1 a 192.168.3.0 /24 al venir a 10.20.20.0 /24.
- La red local 10.10.10.0 /24 a 10.30.30.0 /24 al ir al SPOKE3 (192.168.2.0 /24).
- La red 192.168.2.0 /24 del SPOKE2 a 192.168.4.0 /24 al venir a 10.30.30.0 /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

```

Configure el ACL crypto con las subredes traducidas

```

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
```

Configuración de criptografía relevante

```
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)

Configure el ACL crypto que va a la subred traducida (10.20.20.0 /24)

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

Configuración de criptografía relevante

```
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)

Configure el ACL crypto que va a la subred traducida (10.30.30.0 /24)

```
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```


Configuración de criptografía relevante

```
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
```

Verificación

ASA 1

```
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 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 192.168.2.0 255.255.255.0 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 pcp 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:

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Borre las asociaciones de seguridad

Cuando usted Troubleshooting, esté seguro de borrar los SA existentes después de que usted realice un cambio. En el modo privilegiado del PIX, utilice estos comandos:

- **clear crypto ipsec sa** - Borra el IPsec activo SA.
- **clear crypto isakmp sa** - Borra el IKE activo SA.

Configuración del NAT del estudio

- **muestre el detalle nacional** - Visualiza la configuración del NAT con los objetos/

Comandos para resolución de problemas

Use esta sección para confirmar que su configuración funciona correctamente.

[El analizador del CLI de Cisco](#) ([clientes registrados solamente](#)) apoya los ciertos comandos show. Utilice el analizador del CLI de Cisco para ver una análisis de la salida del comando show.

Nota: Consulte [Información Importante sobre Comandos Debug](#) y [Troubleshooting de Seguridad IP - Comprensión y Uso de Comandos debug](#) antes de usar los comandos **debug**

- **IPsec del debug crypto** - Visualiza los IPsec Negotiations de la fase 2.
- **debug crypto isakmp** - Muestra las negociaciones ISAKMP para la fase 1.

Información Relacionada

- [Guía de configuración del NAT](#)
- [La mayoría del IPsec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)