

Ejemplo de Configuración de ASA VPN con Escenarios de Superposición

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Traducción en ambos terminales VPN](#)

[ASA 1](#)

[Crear los objetos necesarios para las subredes en uso](#)

[Configuración de la Declaración NAT](#)

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

[Configuración criptográfica relevante](#)

[ASA 2](#)

[Crear los objetos necesarios para las subredes en uso](#)

[Configuración de la Declaración NAT](#)

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

[Configuración criptográfica relevante](#)

[Verificación](#)

[ASA 1](#)

[ASA 2](#)

[Topología de radios y concentradores con radios superpuestas](#)

[ASA1](#)

[Crear los objetos necesarios para las subredes en uso](#)

[Cree instrucciones manuales para traducir:](#)

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

[Configuración criptográfica relevante](#)

[ASA2 \(SPOKE1\)](#)

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

[Configuración criptográfica relevante](#)

[R1 \(SPOKE2\)](#)

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

[Configuración criptográfica relevante](#)

[Verificación](#)

[ASA 1](#)

[ASA2 \(SPOKE1\)](#)

[R1 \(SPOKE2\)](#)

[Troubleshoot](#)

[Despeje las asociaciones de seguridad](#)

[Revisar configuración NAT](#)

Introducción

Este documento describe los pasos utilizados para traducir el tráfico VPN que viaja a través de un túnel IPsec de LAN a LAN (L2L) entre dos dispositivos de seguridad adaptables (ASA) en escenarios superpuestos y también la Traducción de direcciones de puerto (PAT) en el tráfico de Internet.

Prerequisites

Requirements

Asegúrese de haber configurado el dispositivo de seguridad adaptable de Cisco con direcciones IP en las interfaces y de tener conectividad básica antes de continuar con este ejemplo de configuración.

Componentes Utilizados

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

- Cisco Adaptive Security Appliance Software versión 8.3 y posteriores.

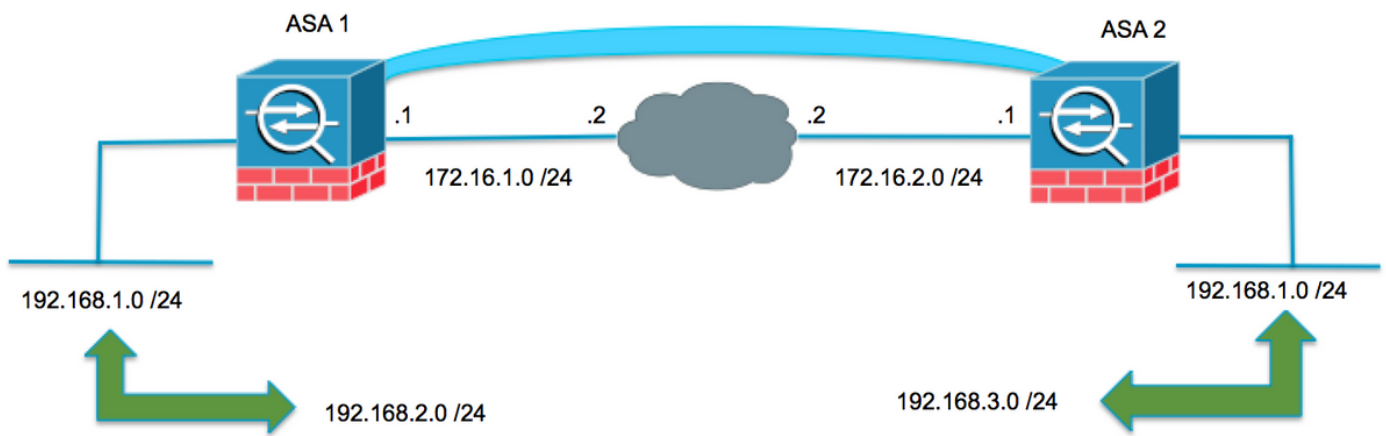
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Cada dispositivo tiene una red privada protegida detrás de ella. En escenarios superpuestos, la comunicación a través de la VPN nunca ocurre porque los paquetes nunca salen de la subred local ya que el tráfico se envía a una dirección IP de la misma subred. Esto se puede lograr con la traducción de direcciones de red (NAT), como se explica en las secciones siguientes.

Traducción en ambos terminales VPN

Cuando las redes protegidas por VPN se superponen y la configuración se puede modificar en ambos extremos; NAT se puede utilizar para traducir la red local a una subred diferente cuando se va a la subred traducida remota.



ASA 1

Crear los objetos necesarios para las subredes en uso

```
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
```

Configuración de la Declaración NAT

Cree una instrucción manual para traducir la red local a una subred diferente sólo cuando vaya a la subred remota (también traducida)

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

Configure la ACL crypto con las subredes traducidas

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

Configuración criptográfica 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

Crear los objetos necesarios para las subredes en uso

```
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
```

Configuración de la Declaración NAT

Cree una instrucción manual para traducir la red local a una subred diferente sólo cuando vaya a la subred remota (también traducida)

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

Configure la ACL crypto con las subredes traducidas

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

Configuración criptográfica 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 SAs
```

```
ASA1(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)
```

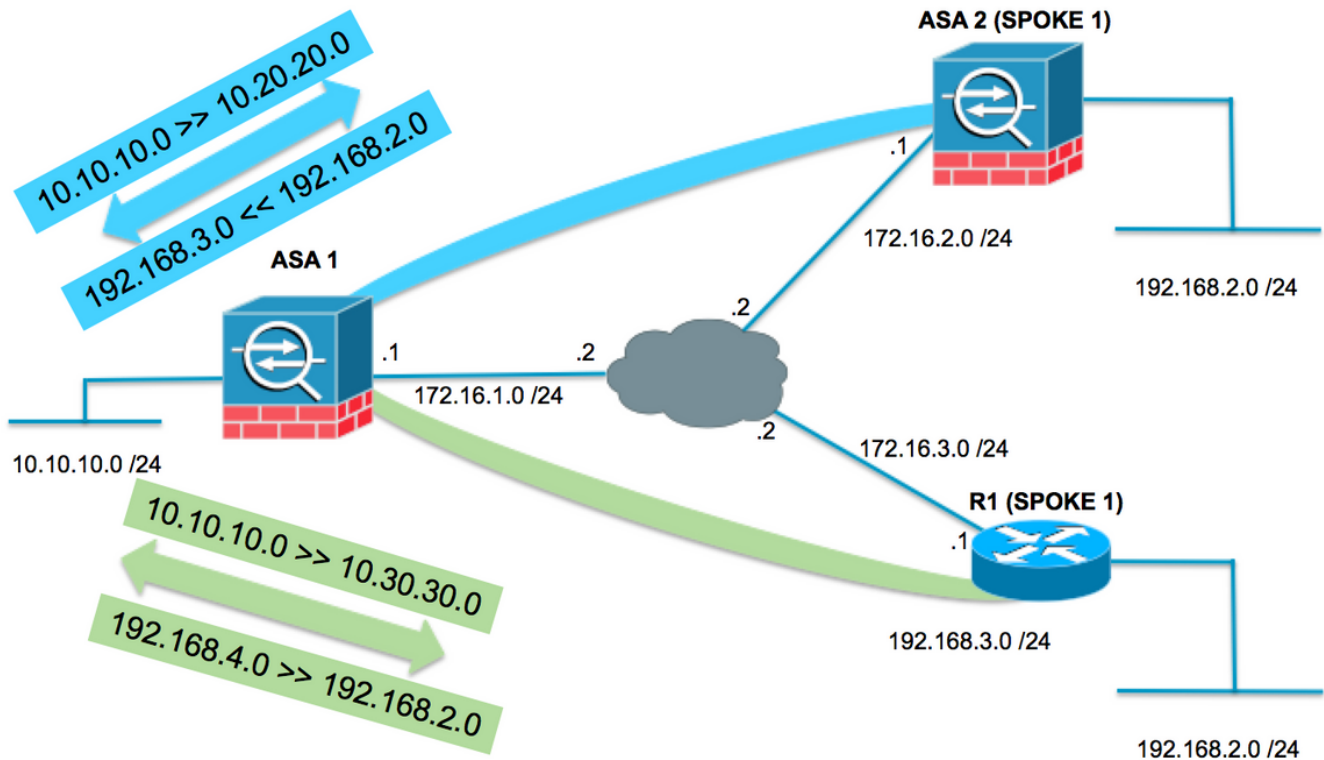
```
IV size: 16 bytes
```

```
replay detection support: Y
```

Anti replay bitmap:
0x00000000 0x00000001

Topología de radios y concentradores con radios superpuestas

En la siguiente topología, ambos radios tienen la misma subred que debe protegerse sobre el túnel IPsec hacia el concentrador. Para facilitar la administración en los radios, la configuración NAT para solucionar el problema de superposición se realiza solamente en el Hub.



ASA1

Crear los objetos necesarios para las subredes en uso

```
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 instrucciones manuales para traducir:

- La red local 10.10.10.0 /24 a 10.20.20.0 /24 cuando se dirige a SPOKE1 (192.168.2.0 /24).
- La red SPOKE1 192.168.2.0 /24 a 192.168.3.0 /24 cuando llega a 10.20.20.0 /24.
- La red local 10.10.10.0 /24 a 10.30.30.0 /24 cuando se va a SPOKE3 (192.168.2.0 /24).
- La red SPOKE2 192.168.2.0 /24 a 192.168.4.0 /24 cuando llega 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 la 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 criptográfica 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 la 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 criptográfica 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 la 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 criptográfica 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 SAs

```
ASA1(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 0x0000003FF
```

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)

```
R31show 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 SA
```

```
R1#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:
```

Troubleshoot

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

Despeje las asociaciones de seguridad

Cuando resuelva problemas, asegúrese de borrar las SA existentes después de realizar un cambio. En el modo privilegiado del PIX, use estos comandos:

- **clear crypto ipsec sa** - Elimina las SAs IPsec activas.
- **clear crypto isakmp sa** - Elimina las SA IKE activas.

Revisar configuración NAT

- **show nat detail** - Muestra la configuración de NAT con los objetos / grupos de objetos expandidos

Comandos para resolución de problemas

Use esta sección para confirmar que su configuración funciona correctamente.

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show. Utilice el Analizador de Cisco CLI para ver un análisis de los resultados 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](#)

.

- `debug crypto ipsec` - Muestra los IPsec Negotiations de la Fase 2.
- `debug crypto isakmp` - Muestra las negociaciones ISAKMP para la fase 1.

Información Relacionada

- [Guía de configuración de NAT](#)
- [Soluciones y Troubleshooting para los Problemas más Comunes con VPN IPsec de Acceso Remoto y L2L](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)