Esempio di configurazione della VPN ASA con scenari di sovrapposizione

Sommario

Introduzione

In questo documento viene descritta la procedura da utilizzare per tradurre il traffico VPN che viaggia su un tunnel IPsec LAN-to-LAN (L2L) tra due appliance ASA (Adaptive Security Appliance) in scenari sovrapposti e anche per il traffico Internet Port Address Translation (PAT).

Prerequisiti

Requisiti

Prima di procedere con questo esempio di configurazione, verificare di aver configurato Cisco Adaptive Security Appliance con gli indirizzi IP sulle interfacce e di disporre della connettività di base.

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

- Software Cisco Adaptive Security Appliance versione 8.3 e successive.

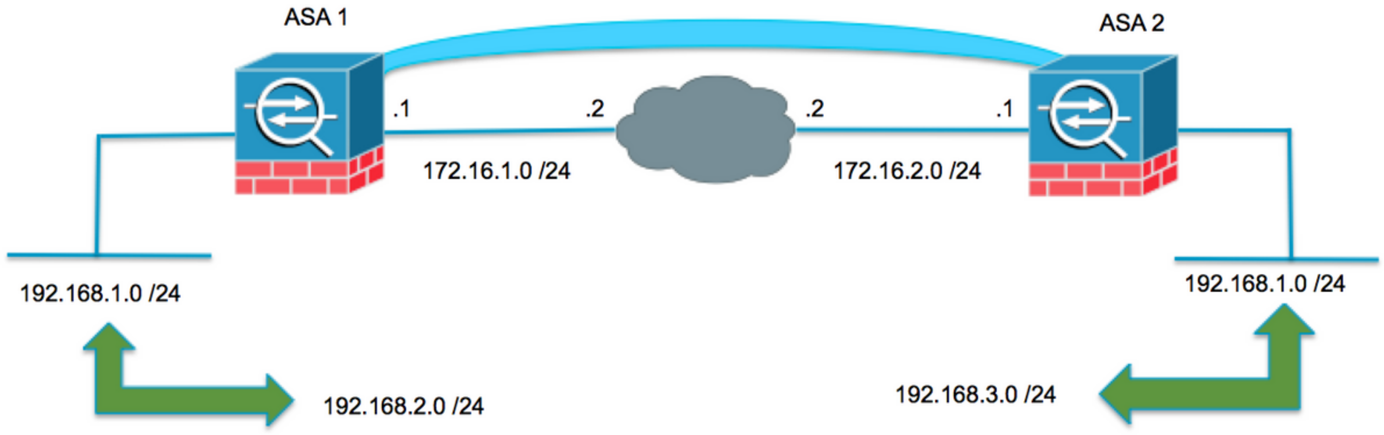
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Ciascun dispositivo è dotato di una rete privata protetta. In scenari di sovrapposizione, la comunicazione attraverso la VPN non avviene mai perché i pacchetti non lasciano mai la subnet locale poiché il traffico viene inviato a un indirizzo IP della stessa subnet. A tale scopo, è possibile utilizzare Network Address Translation (NAT), come spiegato nelle sezioni seguenti.

Traduzione su entrambi gli endpoint VPN

Quando le reti VPN protette si sovrappongono e la configurazione può essere modificata su entrambi gli endpoint; NAT può essere utilizzato per tradurre la rete locale in una subnet diversa quando si accede alla subnet tradotta in remoto.



ASA 1

Creare gli oggetti necessari per le subnet in 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
```

Configurare l'istruzione NAT

Crea un'istruzione manuale per convertire la rete locale in una subnet diversa solo quando si accede alla subnet remota (anche convertita)

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

Configurare l'ACL crittografico con le subnet tradotte

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

Configurazione crittografica rilevante

```
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

Creare gli oggetti necessari per le subnet in 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
```

Configurare l'istruzione NAT

Crea un'istruzione manuale per convertire la rete locale in una subnet diversa solo quando si accede alla subnet remota (anche convertita)

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

Configurare l'ACL crittografico con le subnet tradotte

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

Configurazione crittografica rilevante

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

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
```

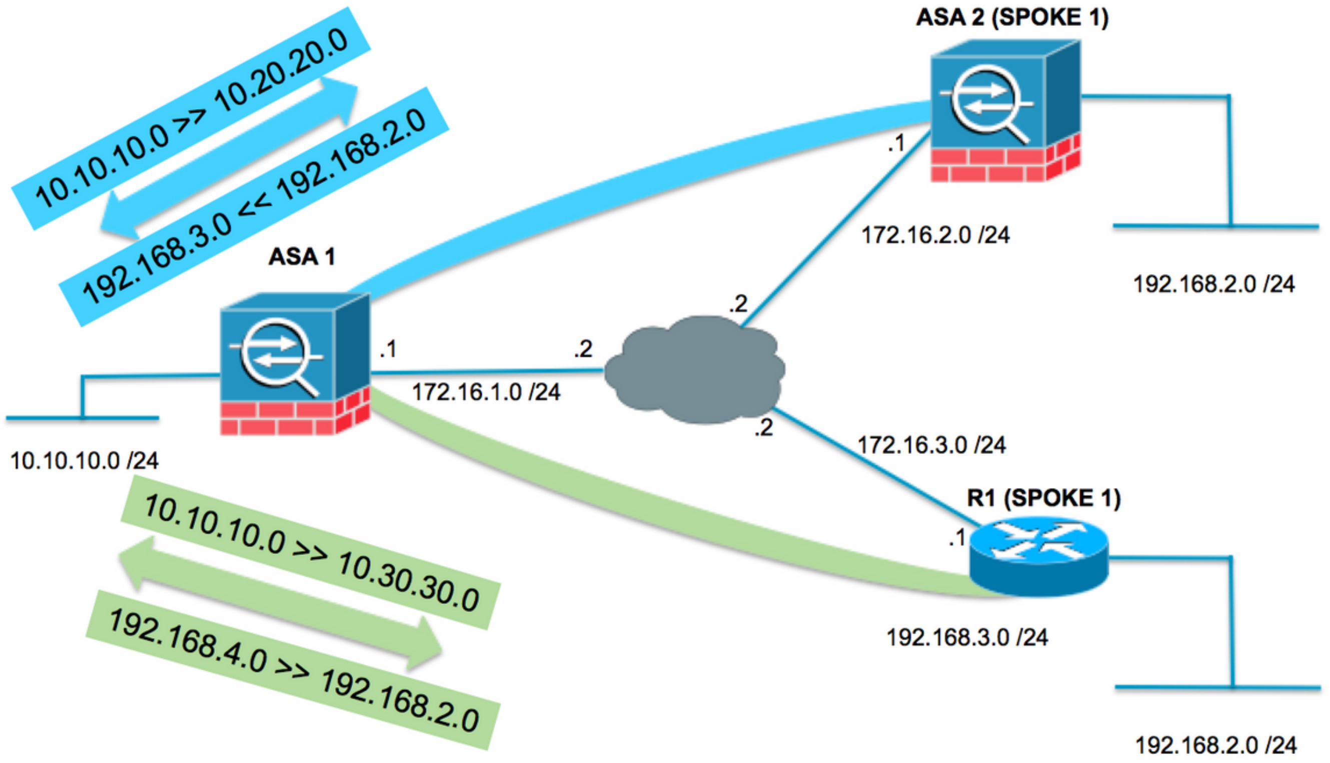
ASA 2

```
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
```

Topologia hub e spoke con spoke sovrapposti

Nella topologia seguente, entrambi i spoke hanno la stessa subnet che deve essere protetta tramite il tunnel IPsec verso l'hub. Per facilitare la gestione degli spoke, la configurazione NAT per risolvere il problema di sovrapposizione viene eseguita solo sull'hub.



ASA1

Creare gli oggetti necessari per le subnet in 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
```

Creare istruzioni manuali da tradurre:

- La rete locale da 10.10.10.0 /24 a 10.20.20.0 /24 quando si accede a SPOKE1 (192.168.2.0 /24).
- La rete SPOKE1 da 192.168.2.0 /24 a 192.168.3.0 /24 quando arriva a 10.20.20.0 /24.
- La rete locale da 10.10.10.0 /24 a 10.30.30.0 /24 quando si accede a SPOKE3 (192.168.2.0 /24).
- La rete SPOKE2 da 192.168.2.0 /24 a 192.168.4.0 /24 quando arriva 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
```

Configurare l'ACL crittografico con le subnet tradotte

```
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
```

Configurazione crittografica rilevante

```
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)

Configurare l'ACL crittografico che accede alla subnet tradotta (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
```

Configurazione crittografica rilevante

```
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)

Configurare l'ACL crittografico che accede alla subnet tradotta (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
```

Configurazione crittografica rilevante

```
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
```

Verifica

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 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)

```
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:
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Cancella associazioni di protezione

Quando si esegue la risoluzione dei problemi, assicurarsi di cancellare le associazioni di protezione esistenti dopo aver apportato una modifica. In modalità privilegiata di PIX, utilizzare i seguenti comandi:

- **clear crypto ipsec sa**: elimina le SA IPsec attive.
- **clear crypto isakmp sa**: elimina le associazioni di protezione IKE attive.

Verifica configurazione NAT

- **show nat detail** - Visualizza la configurazione NAT con gli oggetti/gruppi di oggetti espansi

Comandi per la risoluzione dei problemi

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi **show.** Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando **show**.

> **Nota:** consultare le informazioni importanti sui comandi di debug e sulla risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP della fase 1.

Informazioni correlate

- **Guida alla configurazione NAT**
- **Soluzioni per la risoluzione dei problemi più comuni di VPN IPsec L2L e ad accesso remoto**
- **Negoziazione IPSec/protocolli IKE**
- **Documentazione e supporto tecnico – Cisco Systems**