Configurazione di un tunnel IPSec IKEv1 da sito a sito tra ASA e router Cisco IOS XE

Sommario

Introduzione

In questo documento viene descritto come configurare un tunnel IKEv1 da sito a sito tramite la CLI tra un'appliance Cisco ASA e un router con software Cisco IOS XE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS XE
- Cisco Adaptive Security Appliance (ASA)
- Concetti generali su IPSec

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASAv con software cisco versione 9.20(2)2
- Cisco CSRv con software Cisco IOS XE versione 17.03.03

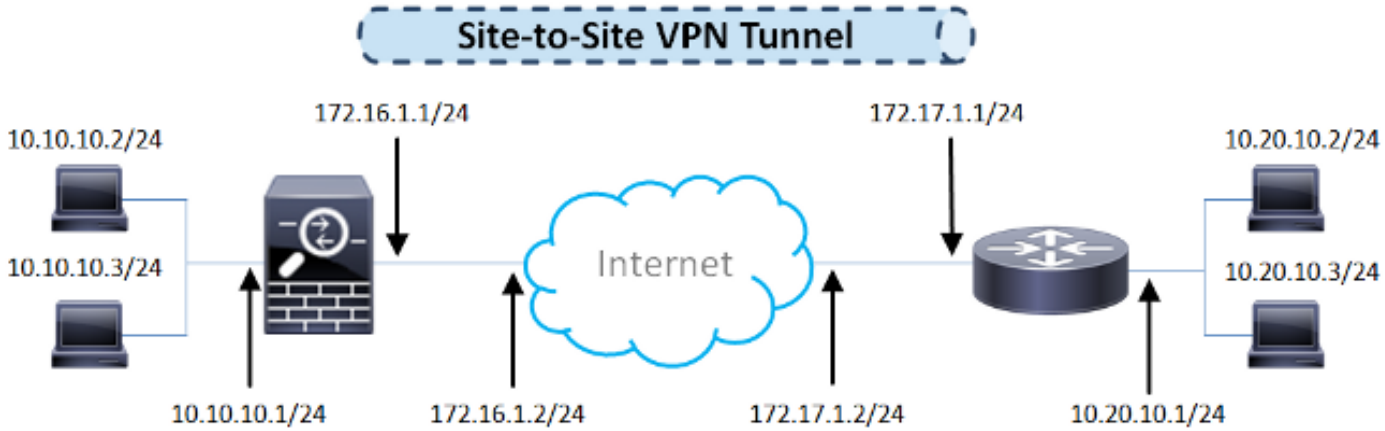
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

In questa sezione viene descritto come completare le configurazioni dell'interfaccia CLI del router ASA e Cisco IOS XE.

Esempio di rete

Per le informazioni di questo documento viene utilizzata la seguente configurazione della rete:



Configurazione ASA

Configurazione delle interfacce ASA

Se le interfacce ASA non sono configurate, verificare di configurare almeno gli indirizzi IP, i nomi delle interfacce e i livelli di sicurezza:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

Nota: per stabilire un tunnel VPN da sito a sito, verificare che sia disponibile una connettività sia alle reti interne che a quelle esterne, in particolare al peer remoto utilizzato. È possibile usare un comando ping per verificare la connettività di base.

Configurare il criterio IKEv1 e abilitare IKEv1 sull'interfaccia esterna

Per configurare i criteri ISAKMP (Internet Security Association and Key Management Protocol) per le connessioni IPSec Internet Key Exchange versione 1 (IKEv1), immettere il`crypto ikev1 policy` comando:

```
<#root>
crypto ikev1 policy 10


 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
```

Nota: esiste una corrispondenza di criteri IKEv1 quando entrambi i criteri dei due peer contengono gli stessi valori di autenticazione, crittografia, hash e parametro Diffie-Hellman. Per IKEv1, il criterio peer remoto deve inoltre specificare una durata minore o uguale alla durata del criterio inviato dall'iniziatore. Se le durate non sono identiche, l'appliance ASA usa la durata più breve.

Nota: se non si specifica un valore per un determinato parametro di criterio, viene applicato il valore predefinito.

È necessario abilitare IKEv1 sull'interfaccia che termina il tunnel VPN. In genere, si tratta dell'interfaccia esterna (o pubblica). Per abilitare IKEv1, immettere il`crypto ikev1 enable` comando in modalità di configurazione globale:

```
<#root>

crypto ikev1 enable outside
```

Configurazione del gruppo di tunnel (profilo di connessione LAN a LAN)

Per un tunnel da LAN a LAN, il tipo di profilo di connessione è`ipsec-l2l`. Per configurare la chiave già condivisa IKEv1, immettere la modalità di`tunnel-group ipsec-attributes`configurazione:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

Configurare l'ACL per il traffico VPN di interesse

L'appliance ASA utilizza gli Access Control Lists (ACL) per distinguere il traffico che deve essere protetto con la crittografia IPSec dal traffico che non deve essere protetto. Protegge i pacchetti in uscita che corrispondono a una voce ACE (Application Control Engine) dell'autorizzazione e garantisce la protezione dei pacchetti in entrata che corrispondono a una voce ACE dell'autorizzazione.

```
<#root>

object-group network

local-network


 network-object 10.10.10.0 255.255.255.0
object-group network
```

```
remote-network

 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group

local-network

 object-group

remote-network
```

Nota: un ACL per il traffico VPN usa gli indirizzi IP di origine e di destinazione dopo il protocollo NAT (Network Address Translation).

Nota: è necessario eseguire il mirroring di un ACL per il traffico VPN su entrambi i peer VPN.

Nota: se è necessario aggiungere una nuova subnet al traffico protetto, è sufficiente aggiungere una subnet/host al rispettivo gruppo di oggetti e completare una modifica di mirroring sul peer VPN remoto.

Configurare un'esenzione NAT

Nota: la configurazione descritta in questa sezione è facoltativa.

In genere, non deve essere eseguito alcun NAT sul traffico VPN. Per escludere il traffico, è necessario creare una regola NAT di identità. La regola NAT di identità traduce semplicemente un indirizzo nello stesso indirizzo.

```
<#root>

nat (inside,outside) source static

local-network local-network

 destination static

remote-network remote-network

 no-proxy-arp route-lookup
```

Configurare il set di trasformazioni IKEv1

Un set di trasformazioni IKEv1 è una combinazione di protocolli e algoritmi di sicurezza che definiscono il modo in cui l'appliance ASA protegge i dati. Durante le negoziazioni della Security Association (SA) IPSec, i peer devono identificare un set di trasformazioni o una proposta identica per entrambi i peer. L'ASA quindi applica il set di trasformazioni o la proposta di trasformazione corrispondente per creare un'associazione di protezione (SA) che protegga i flussi di dati nell'elenco degli accessi per la mappa crittografica.

Per configurare il set di trasformazioni IKEv1, immettere il`crypto ipsec ikev1 transform-set`comando:

```
<#root>

crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
```

Configurazione di una mappa crittografica e applicazione a un'interfaccia

Una mappa crittografica definisce un criterio IPSec da negoziare nell'associazione di protezione IPSec e include:

- Un elenco degli accessi per identificare i pacchetti consentiti e protetti dalla connessione IPSec
- Identificazione peer
- Indirizzo locale per il traffico IPSec
- Set di trasformazioni IKEv1
- Perfect Forward Secrecy (opzionale)

Di seguito è riportato un esempio:

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
```

È quindi possibile applicare la mappa crittografica all'interfaccia:

```
<#root>

crypto map outside_map interface outside
```

Configurazione finale ASA

Di seguito è riportata la configurazione finale dell'appliance ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
 object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
 static remote-network remote-network no-proxy-arp route-lookup
!
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
!
crypto ikev1 enable outside
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
crypto map outside_map interface outside
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
!
```

Configurazione CLI router Cisco IOS XE

Configurazione delle interfacce

Se le interfacce del router Cisco IOS XE non sono ancora configurate, è necessario configurare almeno le interfacce LAN e WAN. Di seguito è riportato un esempio:

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 no shutdown
```

Verificare la connettività alle reti interne ed esterne, in particolare al peer remoto utilizzato per stabilire un tunnel VPN da sito a sito. È possibile usare un comando ping per verificare la connettività di base.

Configurare il criterio ISAKMP (IKEv1)

Per configurare i criteri ISAKMP per le connessioni IKEv1, immettere il`crypto isakmp policy` comando in modalità di configurazione globale. Di seguito è riportato un esempio:

```
<#root>
crypto isakmp policy 10

 encryption aes 256
 hash sha
 authentication pre-share
 group 14
```

Nota: è possibile configurare più criteri IKE in ogni peer che partecipa a IPSec. All'inizio della negoziazione IKE, viene eseguito il tentativo di trovare un criterio comune configurato in entrambi i peer e viene avviato con i criteri con la priorità più alta specificati nel peer remoto.

Configurare una chiave ISAKMP crittografica

Per configurare una chiave di autenticazione già condivisa, immettere il comando nella`crypto isakmp key`modalità di configurazione globale:

<#root>

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configurazione di un ACL per il traffico VPN di interesse

Utilizzare l'elenco degli accessi esteso o con nome per specificare il traffico che deve essere protetto dalla crittografia. Di seguito è riportato un esempio:

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Nota: un ACL per il traffico VPN usa gli indirizzi IP di origine e destinazione dopo NAT.

Nota: è necessario eseguire il mirroring di un ACL per il traffico VPN su entrambi i peer VPN.

Configurare un'esenzione NAT

Nota: la configurazione descritta in questa sezione è facoltativa.

In genere, non deve essere eseguito alcun NAT sul traffico VPN. Se si usa il sovraccarico NAT, è necessario usare una route-map per esentare il traffico VPN di interesse dalla traduzione. Notare che nell'elenco degli accessi utilizzato nella route-map, il traffico VPN di interesse deve essere rifiutato.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

Configurare un set di trasformazioni

Per definire un set di trasformazioni IPSec (una combinazione accettabile di protocolli e algoritmi di sicurezza), immettere il comando`crypto ipsec transform-set`in modalità di configurazione globale. Di seguito è riportato un esempio:

<#root>

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

 mode tunnel
```

Configurazione di una mappa crittografica e applicazione a un'interfaccia

Per creare o modificare una voce della mappa crittografica e accedere alla modalità di configurazione della mappa crittografica, immettere il comando di configurazione globale crypto map. Affinché la voce della mappa crittografica sia completa, è necessario definire almeno alcuni aspetti:

- È necessario definire i peer IPsec a cui è possibile inoltrare il traffico protetto. Si tratta dei peer con cui è possibile stabilire un'associazione di protezione. Per specificare un peer IPSec in una voce della mappa crittografica, immettere il`set peer`comando.
- È necessario definire i set di trasformazioni che possono essere utilizzati con il traffico protetto. Per specificare i set di trasformazioni che possono essere utilizzati con la voce della mappa crittografica, immettere il`set transform-set`comando.
- È necessario definire il traffico da proteggere. Per specificare un elenco degli accessi estesi per una voce della mappa crittografica, immettere il`match address`comando.

Di seguito è riportato un esempio:

<#root>

```
crypto map outside_map 10 ipsec-isakmp

 set peer 172.16.1.1
 set transform-set ESP-AES256-SHA
 match address 110
```

Il passaggio finale è l'applicazione a un'interfaccia della mappa crittografica definita in precedenza.

Per applicare questa condizione, immettere il comando di configurazione dell'crypto mapinterfaccia:

<#root>

```
interface GigabitEthernet0/0

crypto map outside_map
```

Configurazione finale di Cisco IOS XE

Di seguito è riportata la configurazione finale della CLI del router Cisco IOS XE:

```
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES256-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
```

```
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

Verifica

Prima di verificare se il tunnel è attivo e se supera il traffico, è necessario verificare che il traffico di interesse sia inviato verso l'ASA o il router Cisco IOS XE.

Nota: sull'appliance ASA, è possibile usare lo strumento di traccia dei pacchetti che corrisponde al traffico di interesse per avviare il tunnel IPSec (ad esempio,packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed).

Verifica fase 1

Per verificare se IKEv1 fase 1 è attivo sull'appliance ASA, immettere il comando show crypto isakmp sa. L'output previsto è il seguenteMM_ACTIVEstato:

<#root>

```
ciscoasa#
```

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: 172.17.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Per verificare se IKEv1 Phase 1 è attivo su Cisco IOS XE, immettere ilshow crypto isakmp sacomando. L'output previsto è il seguenteACTIVEstato:

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           2003 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Verifica fase 2

Per verificare se IKEv1 fase 2 è attivo sull'appliance ASA, immettere il`show crypto ipsec sa`comando. Nell'output previsto verrà visualizzato l'indice dei parametri di sicurezza (SPI, Security Parameter Index) in entrata e in uscita. Se il traffico attraversa il tunnel, è necessario verificare l'incremento dei contatori encaps/decaps.

Nota: per ciascuna voce dell'ACL, viene creata un'associazione di protezione (SA) in entrata/in uscita distinta, che può generare un output di comando lungo`show crypto ipsec sa`(a seconda del numero di voci ACE nell'ACL crittografico).

Di seguito è riportato un esempio:

<#root>

```
ciscoasa#
```

show crypto ipsec sa peer 172.17.1.1

```
peer address: 172.17.1.1
    Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
   10.20.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 989, #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.: 172.17.1.1/0
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: 5397114D
current inbound spi : 9B592959

inbound esp sas:
spi: 0x9B592959 (2606311769)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFD7FF

outbound esp sas:
spi: 0x5397114D (1402409293)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa#
```

Per verificare se IKEv1 fase 2 è attivo su Cisco IOS XE, immettere il`show crypto ipsec sa`comando. L'output previsto consente di visualizzare l'indice SPI in entrata e in uscita. Se il traffico attraversa il tunnel, è necessario verificare l'incremento dei contatori encaps/decaps.

Di seguito è riportato un esempio:

<#root>

```
Router#
```

`show crypto ipsec sa peer 172.16.1.1`

```
interface: GigabitEthernet0/0
    Crypto map tag: outside_map, local addr 172.17.1.1

   protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
```

```
     PERMIT, flags={origin_is_acl,}
#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#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.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet3
current outbound spi: 0x9B592959(2606311769)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x5397114D(1402409293)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607857/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x9B592959(2606311769)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607901/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Router#
```

Verifica fase 1 e fase 2

In questa sezione vengono descritti i comandi che è possibile usare sull'appliance ASA o Cisco IOS XE per verificare i dettagli delle fasi 1 e 2.

Immettere il comando sull`show vpn-sessiondb`'appliance ASA per la verifica:

<#root>

```
ciscoasa#
```

show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

```
Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                       IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 98900                 Bytes Rx     : 134504
Login Time   : 06:15:52 UTC Fri Sep 6 2024
Duration     : 0h:15m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 2.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 84093 Seconds
  D/H Group    : 14
  Filter Name  :

IPsec:
  Tunnel ID    : 2.2
  Local Addr   : 10.10.10.0/255.255.255.0/0/0
  Remote Addr  : 10.20.10.0/255.255.255.0/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3293 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607901 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 26 Minutes
  Bytes Tx     : 98900                 Bytes Rx     : 134504
  Pkts Tx      : 989                   Pkts Rx      : 989

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 309 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :

ciscoasa#
```

Immettere il comando`show crypto session`su Cisco IOS XE per la verifica:

<#root>

```
Router#
```

show crypto session remote 172.16.1.1 detail

```
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 172.16.1.1
      Desc: (none)
  IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
  IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 989 drop 0 life (KB/Sec) 4449870/3383
        Outbound: #pkts enc'ed 989 drop 0 life (KB/Sec) 4449868/3383

Router#
```

Risoluzione dei problemi

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

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

Strumento di controllo IPSec da LAN a LAN

Per verificare automaticamente se la configurazione IPSec da LAN a LAN tra l'ASA e Cisco IOS XE è valida, è possibile usare lo strumento IPSec da LAN a LANChecker. Lo strumento è progettato in modo da accettare un comando`show tech`or`show running-config`da un router ASA o Cisco IOS XE. Esamina la configurazione e cerca di rilevare se è configurato un tunnel IPSec basato su mappa crittografica LAN a LAN. Se configurato, esegue un controllo della configurazione in più punti ed evidenzia gli eventuali errori di configurazione e le impostazioni per il tunnel che verrebbe negoziato.

Debug dell'ASA

Per risolvere i problemi di negoziazione del tunnel IPSec IKEv1 su un firewall ASA, è possibile utilizzare i seguenti`debug`comandi:

<#root>

debug crypto ipsec 127

```
debug crypto isakmp 127
debug ike-common 10
```

Nota: se il numero di tunnel VPN sull'appliance ASA è significativo, prima di abilitare i debug è necessario usare il`debug crypto condition peer A.B.C.D`comando per limitare gli output del debug in modo da includere solo il peer specificato.

Debug del router Cisco IOS XE

Per risolvere i problemi di negoziazione del tunnel IPSec IKEv1 su un router Cisco IOS XE, è possibile utilizzare i seguenti comandi di debug:

<#root>

```
debug crypto ipsec
debug crypto isakmp
```

Nota: se il numero di tunnel VPN su Cisco IOS XE è significativo, prima di abilitare i debug`debug crypto condition peer ipv4 A.B.C.D`deve essere utilizzato VPN per limitare gli output di debug in modo da includere solo il peer specificato.

Suggerimento: per ulteriori informazioni su come risolvere i problemi relativi a una VPN da sito a sito, consultare il documento sulle soluzioni più comuni per la risoluzione dei problemi relativi alle VPN IPSec da sito a sito Cisco.

Riferimenti

- Informazioni importanti sui comandi di debug
- Risoluzione dei problemi di sicurezza IP - Informazioni e uso dei comandi di debug
- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Controllo IPSec da LAN a LAN
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).