Configuración de un túnel IPSec de IKEv1 de sitio a sitio entre ASA y un router Cisco IOS

Contenido

Introducción

Este documento describe cómo configurar un túnel IKEv1 de sitio a sitio (de LAN a LAN) a través de la CLI entre un Cisco ASA y un router que ejecuta el software Cisco IOS®.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IOS de Cisco
- Dispositivo de seguridad Cisco Adaptive Security Appliance (ASA)
- Conceptos generales de IPSec

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA serie 5512-X que ejecuta la versión de software 9.4(1)
- Cisco 1941 Series Integrated Services Router (ISR) que ejecuta la versión 15.4(3)M2 del software Cisco IOS

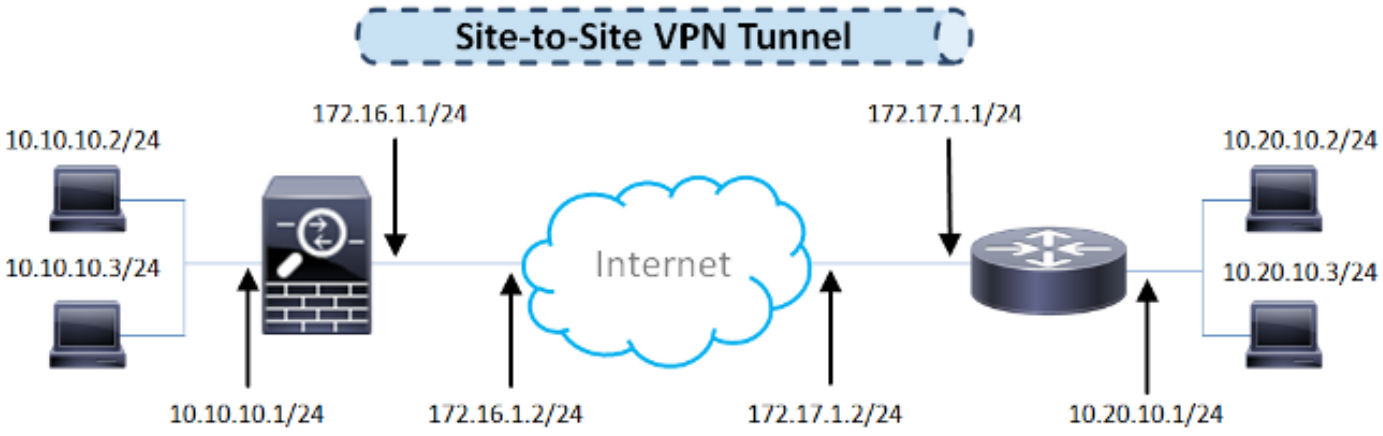
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En esta sección se describe cómo completar las configuraciones CLI de los routers ASA y Cisco IOS.

Diagrama de la red

La información de este documento utiliza esta configuración de red:



Configuración de ASA

Configuración de las interfaces ASA

Si las interfaces ASA no están configuradas, asegúrese de configurar al menos las direcciones IP, los nombres de interfaz y los niveles de seguridad:

```
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**: Asegúrese de que haya conectividad tanto con las redes internas como externas, especialmente con el peer remoto que se utiliza para establecer un túnel VPN de sitio a sitio. Puede utilizar un ping para verificar la conectividad básica.

Configuración de la política IKEv1 y activación de IKEv1 en la interfaz externa

Para configurar las directivas ISAKMP (Internet Security Association and Key Management Protocol) para las conexiones IKEv1 (Internet Key Exchange Version 1, Intercambio de claves de Internet IPSec), introduzca el `crypto ikev1 policy` comando:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **Nota:** Existe una coincidencia de política IKEv1 cuando ambas políticas de los dos peers contienen los mismos valores de parámetro de autenticación, cifrado, hash y Diffie-Hellman. Para IKEv1, la política de peer remoto también debe especificar una duración menor o igual a la duración en la política que envía el iniciador. Si las duraciones no son idénticas, el ASA utiliza la duración más corta.

> **Nota:** Si no especifica un valor para un parámetro de política determinado, se aplica el valor por defecto.

Debe habilitar IKEv1 en la interfaz que termina el túnel VPN. Normalmente, se trata de la interfaz externa (o pública). Para habilitar IKEv1, ingrese el `crypto ikev1 enable` comando en el modo de configuración global:

```
crypto ikev1 enable outside
```

Configuración del grupo de túnel (perfil de conexión de LAN a LAN)

Para un túnel de LAN a LAN, el tipo de perfil de conexión es ipsec-l2l . Para configurar la clave precompartida IKEv1, introduzca el tunnel-group ipsec-attributes modo de configuración global:

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

Configuración de la ACL para el Tráfico de Interés de VPN

ASA utiliza listas de control de acceso (ACL) para diferenciar el tráfico que debe protegerse con cifrado IPSec del tráfico que no requiere protección. Protege los paquetes salientes que coinciden con un permit Application Control Engine (ACE) y garantiza que los paquetes entrantes que coinciden con un permit ACE tengan protección.

```
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:** Una ACL para el tráfico VPN utiliza las direcciones IP de origen y de destino después de la traducción de direcciones de red (NAT).

> **Nota:** Una ACL para el tráfico VPN se debe duplicar en ambos pares VPN.

> **Nota:** Si es necesario agregar una nueva subred al tráfico protegido, simplemente agregue una subred/host al grupo de objetos respectivo y complete un cambio de reflejo en el par VPN remoto.

Configuración de una exención de NAT

> **Nota**: La configuración que se describe en esta sección es opcional.

Normalmente, no debe realizarse ninguna NAT en el tráfico VPN. Para eximir ese tráfico, debe crear una regla de identidad NAT. La regla de identidad NAT simplemente traduce una dirección a la misma dirección.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

Configuración del conjunto de transformación IKEv1

Un conjunto de transformación IKEv1 es una combinación de protocolos y algoritmos de seguridad que definen la forma en que ASA protege los datos. Durante las negociaciones de la Asociación de seguridad IPSec (SA), los pares deben identificar un conjunto o una propuesta de transformación que sea la misma para ambos pares. A continuación, ASA aplica el conjunto o la propuesta de transformación coincidente para crear una SA que proteja los flujos de datos en la lista de acceso para ese mapa criptográfico.

Para configurar el conjunto de transformación IKEv1, introduzca el `crypto ipsec ikev1 transform-set` comando:

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

Configurar un mapa criptográfico y aplicarlo a una interfaz

Un mapa criptográfico define una política IPSec que se negociará en la SA IPSec e incluye:

- Una lista de acceso para identificar los paquetes que la conexión IPSec permite y protege
- Identificación de pares
- Una dirección local para el tráfico IPSec
- Los conjuntos de transformación IKEv1

Aquí tiene un ejemplo:

```
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-AES-SHA
```

A continuación, puede aplicar el mapa criptográfico a la interfaz:

```
crypto map outside_map interface outside
```

Configuración final de ASA

Esta es la configuración final del 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 ipsec ikev1 transform-set ESP-AES-SHA esp-aes 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-AES-SHA
crypto map outside_map interface outside
```

Configuración CLI del router Cisco IOS

Configuración de las interfaces

Si las interfaces del router Cisco IOS aún no están configuradas, deben configurarse al menos las interfaces LAN y WAN. Aquí tiene un ejemplo:

```
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
```

Asegúrese de que haya conectividad tanto con las redes internas como externas, especialmente con el peer remoto que se utiliza para establecer un túnel VPN de sitio a sitio. Puede utilizar un ping para verificar la conectividad básica.

Configuración de la política ISAKMP (IKEv1)

Para configurar las políticas ISAKMP para las conexiones IKEv1, ingrese el `crypto isakmp policy` en el modo de configuración global. Aquí tiene un ejemplo:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

> **Nota:** Puede configurar varias políticas IKE en cada par que participa en IPSec. Cuando comienza la negociación IKE, intenta encontrar una política común que se configura en

ambos peers, y comienza con las políticas de mayor prioridad que se especifican en el peer remoto.

Configurar una clave ISAKMP de cifrado

Para configurar una clave de autenticación previamente compartida, ingrese el crypto isakmp key comando en el modo de configuración global:

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

Configuración de una ACL para el tráfico de interés de VPN

Utilice la lista de acceso ampliada o con nombre para especificar el tráfico que debe protegerse mediante cifrado. Aquí tiene un ejemplo:

```
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: Una ACL para el tráfico VPN utiliza las direcciones IP de origen y de destino después de NAT.

Nota: Una ACL para el tráfico VPN se debe duplicar en ambos pares VPN.

Configuración de una exención de NAT

Nota: La configuración que se describe en esta sección es opcional.

Normalmente, no debe realizarse ninguna NAT en el tráfico VPN. Si se utiliza la sobrecarga NAT, se debe utilizar un route-map para eximir de la traducción el tráfico VPN de interés. Observe que en la lista de acceso que se utiliza en el route-map, se debe denegar el tráfico VPN de interés.

```
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
```

Configuración de un conjunto de transformación

Para definir un conjunto de transformación IPSec (una combinación aceptable de protocolos y algoritmos de seguridad), introduzca el crypto ipsec transform-set en el modo de configuración global. Aquí tiene un ejemplo:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

Configurar un mapa criptográfico y aplicarlo a una interfaz

Para crear o modificar una entrada de mapa criptográfico e ingresar al modo de configuración de mapa criptográfico, ingrese el comando de configuración global **crypto map**. Para que la entrada de mapa criptográfico esté completa, hay algunos aspectos que deben definirse como mínimo:

- Se deben definir los pares IPsec a los que se puede reenviar el tráfico protegido. Estos son los pares con los que se puede establecer una SA. Para especificar un peer IPSec en una entrada de mapa criptográfico, ingrese el set peer comando.
- Se deben definir los conjuntos de transformación que son aceptables para su uso con el tráfico protegido. Para especificar los conjuntos de transformación que se pueden utilizar con la entrada de mapa criptográfico, ingrese el set transform-set comando.
- Se debe definir el tráfico que se debe proteger. Para especificar una lista de acceso ampliada para una entrada de mapa criptográfico, ingrese el match address comando.

Aquí tiene un ejemplo:

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

El paso final es aplicar el conjunto de mapas criptográficos previamente definido a una interfaz. Para aplicar esto, ingrese el crypto map comando de configuración de interfaz:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Configuración final de Cisco IOS

Esta es la configuración final de la CLI del router Cisco IOS:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
```

```
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-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
```

Verificación

Antes de verificar si el túnel está activo y que pasa el tráfico, debe asegurarse de que el tráfico de interés se envía hacia el ASA o el router Cisco IOS.

> **Nota:** En ASA, la herramienta de seguimiento de paquetes que coincide con el tráfico de interés se puede utilizar para iniciar el túnel IPSec (como packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed por ejemplo).

Fase 1 Verificación

Para verificar si IKEv1 Phase 1 está activo en el ASA, ingrese el comando **show crypto isakmp sa**. El resultado esperado es ver el MM_ACTIVE estado:

```
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#
```

Para verificar si IKEv1 Phase 1 está activo en el IOS de Cisco, ingrese el show crypto isakmp sa comando. El resultado esperado es ver el ACTIVE estado:

```
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           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Fase 2 Verificación

Para verificar si IKEv1 Phase 2 está activo en el ASA, ingrese el show crypto ipsec sa comando. El resultado esperado es ver el Índice de parámetros de seguridad (SPI) entrante y saliente. Si el tráfico pasa a través del túnel, debe ver el incremento de los contadores encaps/decaps.

> **Nota:** Para cada entrada de ACL, se crea una SA entrante/saliente independiente, que puede dar como resultado una show crypto ipsec sa resultado del comando (depende del número de entradas ACE en la ACL crypto).

Aquí tiene un ejemplo:

```
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: 1005, #pkts encrypt: 1005, #pkts digest: 1005
     #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #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: 8A9FE619
     current inbound spi : D8639BD0

inbound esp sas:
     spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
     spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

Para verificar si IKEv1 Phase 2 está activo en el IOS de Cisco, ingrese el show crypto ipsec sa comando. El resultado esperado es ver el SPI entrante y saliente. Si el tráfico pasa a través del túnel, debe ver el incremento de los contadores encaps/decaps.

Aquí tiene un ejemplo:

```
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: 2024, #pkts encrypt: 2024, #pkts digest: 2024
   #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
     spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

outbound esp sas:
     spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

Verificación de las fases 1 y 2

Esta sección describe los comandos que puede utilizar en ASA o Cisco IOS para verificar los detalles para las fases 1 y 2.

Escriba el show vpn-sessiondb en el ASA para la verificación:

```
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)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m: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   : AES128                 Hashing      : SHA1
 Rekey Int (T): 86400 Seconds          Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 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   : AES128                 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     : 100500                 Bytes Rx     : 101400
 Pkts Tx      : 1005                   Pkts Rx      : 1014

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#
```

Escriba el show crypto session en el IOS de Cisco para la verificación:

```
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 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

Troubleshoot

Esta sección proporciona información que puede utilizar para resolver problemas de su configuración.

> **Nota:** Refiérase a los documentos de Información Importante sobre Comandos de Debug y Troubleshooting de Seguridad IP - Comprensión y Uso de los Comandos debug de Cisco

antes de utilizar debug comandos.

Herramienta IPSec LAN-to-LAN Checker

Para verificar automáticamente si la configuración IPSec de LAN a LAN entre ASA y Cisco IOS es válida, puede utilizar la herramienta IPSec LAN a LANChecker. La herramienta está diseñada para que acepte un show tech or show running-config desde un router ASA o Cisco IOS. Examina la configuración e intenta detectar si se ha configurado un túnel IPSec de LAN a LAN basado en mapa criptográfico. Si se configura, realiza una verificación multipunto de la configuración y resalta cualquier error de configuración y configuración para el túnel que se negociaría.

Depuraciones de ASA

Para resolver problemas de negociación de túnel IKEv1 IPSec en un firewall ASA, puede utilizar estos debug comandos:

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

> **Nota:** Si el número de túneles VPN en el ASA es significativo, el debug crypto condition peer A.B.C.D se debe utilizar antes de habilitar los debugs para limitar los resultados de debug de modo que incluyan solamente el peer especificado.

Depuraciones del router Cisco IOS

Para resolver problemas de negociación de túnel IPSec IKEv1 en un router Cisco IOS, puede utilizar estos comandos debug:

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

> **Nota:** Si el número de túneles VPN en el IOS de Cisco es significativo, el debug crypto condition peer ipv4 A.B.C.D se debe utilizar antes de habilitar los debugs para limitar los resultados de debug para incluir solamente el peer especificado.

> **Sugerencia**: Consulte el documento L2L y Soluciones de Troubleshooting de VPN IPSec de Acceso Remoto más Comunes de Cisco para obtener más información sobre cómo resolver problemas de una VPN de sitio a sitio.

Referencias

- Información importante sobre los Comandos de depuración
- Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración

- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Verificador IPSec de LAN a LAN
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).