Configure IPSec sitio a sitio un túnel IKEv1 entre un ASA y un router del Cisco IOS

Contenido

Introducción

Este documento describe cómo configurar un túnel de la versión 1 del intercambio de claves de Internet del IPSec del sitio a localizar (LAN a LAN) (IKEv1) vía el CLI entre un dispositivo de seguridad adaptante de Cisco (ASA) y un router que funcione con el software del ® del Cisco IOS.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- IOS de Cisco
- Cisco ASA
- Conceptos generales del IPSec

Componentes Utilizados

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

- Cisco 5512-X Series ASA que funcionan con la versión de software 9.4(1)
- Router de los Servicios integrados de las Cisco 1941 Series (ISR) esa versión del Cisco IOS Software 15.4(3)M2 de los funcionamientos

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

Configurar

Esta sección describe cómo completar las configuraciones CLI ASA y del router IOS.

Diagrama de la red

La información en este documento utiliza esta configuración de la red:

Configuración ASA

Configure las interfaces ASA

Si las interfaces ASA no se configuran, asegúrese de que usted configure por lo menos los IP Addresses, interconecte los nombres, 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 al interno y a las redes externas, y especialmente al peer remoto que será utilizado para establecer un túnel del VPN de sitio a sitio. Usted puede utilizar un ping para verificar la conectividad básica.

Configure la directiva IKEv1 y habilite IKEv1 en la interfaz exterior

Para configurar las directivas del Internet Security Association and Key Management Protocol (ISAKMP) para las conexiones IKEv1, ingrese el comando **crypto del <priority> de la directiva ikev1**:

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

> **Nota:** Una coincidencia de la directiva IKEv1 existe cuando ambas directivas de los dos pares contienen la misma autenticación, cifrado, hash, y Valores de parámetro de Diffie Hellman. Para IKEv1, la directiva del peer remoto debe también especificar un curso de la vida inferior o igual el curso de la vida en la directiva que el iniciador envía. Si los cursos de la vida no son idénticos, después el ASA utiliza el curso de la vida más corto.

> **Nota:** Si usted no especifica un valor para un parámetro dado de la directiva, el valor predeterminado es aplicado.

Usted debe habilitar IKEv1 en la interfaz que termina el túnel VPN. Típicamente, ésta es la interfaz del exterior (o *público*). Para habilitar IKEv1, ingrese el **ikev1 crypto habilitan <interface name> el** comando en el modo de configuración global:

```
crypto ikev1 enable outside
```

Configure el grupo de túnel (el perfil de la conexión de LAN a LAN)

Para un túnel de LAN a LAN, el tipo del perfil de la conexión es **ipsec-l2l**. Para configurar la clave del preshared IKEv1, ingrese al modo de configuración de los IPSec-*atributos del grupo de túnel*:

```
tunnel-group 172.17.1.1 type ipsec-l2l
```

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

Configure el ACL para el tráfico VPN del interés

El ASA utiliza el Listas de control de acceso (ACL) para distinguir el tráfico que se debe proteger con la encripción de IPSec contra el tráfico que no requiere la protección. Protege los paquetes salientes que hacen juego un motor del control de la aplicación del permiso (ACE) y se asegura de que los paquetes de entrada que hacen juego un permiso ACE tenga 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:** Un ACL para el tráfico VPN utiliza los IP Address de origen y de destino después del Network Address Translation (NAT).

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

> **Nota:** Si hay una necesidad de agregar una nueva subred al tráfico protegido, de agregar simplemente una subred/un host al objeto-grupo respectivo y de completar un cambio del espejo en el par del telecontrol VPN.

Configure una exención de NAT

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

Típicamente, no debe haber NAT realizado en el tráfico VPN. Para eximir ese tráfico, usted debe crear una regla de la identidad NAT. La regla de la identidad NAT traduce simplemente un direccionamiento al mismo direccionamiento.

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

Configure el IKEv1 transforman el conjunto

Un IKEv1 transforma el conjunto es una combinación de protocolos de Seguridad y los algoritmos que define la manera que el ASA protege los datos. Durante las negociaciones de la asociación de seguridad IPSec (SA), los pares deben identificar una transformación fijada o la oferta que sean lo mismo para ambos pares. El ASA entonces aplica correspondido con transforma el conjunto o la oferta para crear un SA que proteja los flujos de datos en la lista de acceso para esa correspondencia de criptografía.

Para configurar el IKEv1 transforme el conjunto, ingresan el comando **crypto del transforme el conjunto del IPSec ikev1**:

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

Configure una correspondencia de criptografía y apliqúela a una interfaz

Una correspondencia de criptografía define una política IPSec que se negociará en IPSec SA y la incluye:

- Una lista de acceso para identificar los paquetes que conexión IPSec los permisos y protege
- Identificación del par
- Una dirección local para el tráfico IPSec
- Los IKEv1 transforman los conjuntos

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
```

Usted puede entonces aplicar la correspondencia de criptografía a la interfaz:

```
crypto map outside_map interface outside
```

Configuración final ASA

Aquí está la configuración final en el 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 IOS

Configure las interfaces

Si las interfaces del router IOS todavía no se configuran, después por lo menos el LAN y las interfaces de WAN deben ser configurados. 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 al interno y a las redes externas, y especialmente al peer remoto que será utilizado para establecer un túnel del VPN de sitio a sitio. Usted puede utilizar un ping para verificar la conectividad básica.

Configure la directiva ISAKMP (IKEv1)

Para configurar las políticas isakmp para las conexiones IKEv1, ingrese el comando **crypto del <priority> de la política isakmp** en el modo de configuración global. Aquí tiene un ejemplo:

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

> **Nota:** Usted puede configurar las políticas IKE múltiples en cada par que participe en el IPSec. Cuando la negociación IKE comienza, intenta encontrar una directiva común que se configure en ambos pares, y comienza con las directivas más prioritarias que se especifican en el peer remoto.

Configure una clave Crypto ISAKMP

Para configurar una clave de autenticación del *preshared*, ingrese el **comando crypto isakmp key** en el modo de configuración global:

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

Configure un ACL para el tráfico VPN del interés

Utilice el extendido o la lista de acceso denominada para especificar el tráfico que se debe proteger por el 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:** Un ACL para el tráfico VPN utiliza los IP Address de origen y de destino después del NAT.

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

Configure una exención de NAT

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

Típicamente, no debe haber NAT realizado en el tráfico VPN. Si se utiliza la sobrecarga NAT, después un route-map se debe utilizar para eximir el tráfico VPN del interés de la traducción. Note que en la lista de acceso que se utiliza en el route-map, el tráfico VPN del interés debe ser negado.

```
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
```

Configure un conjunto de la transformación

Para definir un IPSec transforme el conjunto (una combinación aceptable de protocolos y de algoritmos de Seguridad), ingresan el **comando 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
```

Configure una correspondencia de criptografía y apliqúela a una interfaz

Para crear o modificar una entrada de correspondencia de criptografía y ingresar al modo de configuración de la correspondencia de criptografía, ingrese el comando global configuration de la **correspondencia de criptografía**. Para que la entrada de correspondencia de criptografía sea completa, allí son algunos aspectos que se deben definir en un mínimo:

- Los peeres IPSec a quienes el tráfico protegido puede ser remitido deben ser definidos. Éstos son los pares con quienes un SA puede ser establecido. Para especificar a un peer IPSec en una entrada de correspondencia de criptografía, ingrese el **comando set peer**.
- Los conjuntos de la transformación que son aceptables para el uso con el tráfico protegido deben ser definidos. Para especificar los conjuntos de la transformación que se pueden utilizar con la entrada de correspondencia de criptografía, ingrese el **comando set transform-set**.
- El tráfico que debe ser protegido debe ser definido. Para especificar una lista de acceso ampliada para una entrada de correspondencia de criptografía, ingrese el **comando address del emparejamiento**.

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 último paso es aplicar el conjunto previamente definido de la correspondencia de criptografía a una interfaz. Para aplicar esto, ingrese el comando interface configuration de la **correspondencia de criptografía**:

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

Configuración final IOS

Aquí está la configuración CLI final del router 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 que usted lo verifique si el túnel sea ascendente y ése pase el tráfico, usted debe asegurarse de que el tráfico del interés esté enviado hacia el ASA o el router IOS.

Nota: En el ASA, la herramienta del paquete-trazalíneas que hace juego el tráfico del interés se puede utilizar para iniciar el túnel IPsec (tal como paquete-**trazalíneas entrado dentro de tcp 10.10.10.10 12345 10.20.10.10 80 detallado** por ejemplo).

Verificación de la fase 1

Para verificar si IKEv1 la fase 1 esté para arriba en el ASA, ingrese el **comando show crypto isakmp sa**. El resultado esperado es considerar **MM_ACTIVE el** 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 la fase 1 esté para arriba en el IOS, ingrese el **comando show crypto isakmp sa**. El resultado esperado es considerar el estado **ACTIVO**:

```
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#
```

Verificación de la fase 2

Para verificar si IKEv1 la fase 2 esté para arriba en el ASA, ingrese el **comando show crypto ipsec sa**. El resultado esperado es considerar el Security Parameter Index entrante y saliente (SPI). Si el tráfico pasa a través del túnel, usted debe ver el encaps/los contadores de los decaps incrementar.

Nota: Para cada entrada ACL hay un SA entrante/saliente separado creado, que pudo dar lugar a una salida larga del **comando show crypto ipsec sa** (dependiente sobre el número de entradas de ACE en el 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 la fase 2 esté para arriba en el IOS, ingrese el **comando show crypto ipsec sa**. El resultado esperado es considerar SPI entrante y saliente. Si el tráfico pasa a través del túnel, usted debe ver el encaps/los contadores de los decaps incrementar.

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#
```

Fase 1 y verificación 2

Esta sección describe los comandos que usted puede utilizar en el ASA o el IOS para verificar los detalles por ambas fases 1 y 2.

Ingrese el comando de **VPN-sessiondb de la demostración** 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#
```

Ingrese el comando de **sesión de criptografía de la demostración** en el IOS 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#
```

Troubleshooting

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

> **Nota:** Refiera a la información importante en los comandos Debug y el Troubleshooting de IP Security - entendiendo y con los documentos de Cisco de los comandos debug antes de

que usted utilice los **comandos debug**.

Herramienta del inspector del LAN a LAN del IPSec

Para verificar automáticamente si la configuración de LAN a LAN del IPSec entre el ASA y el IOS sea válida, usted puede utilizar la herramienta del inspector del LAN a LAN del IPSec. Se diseña la herramienta de modo que valide una **tecnología** o un **comando show running-config de la demostración de un** ASA o del router IOS. Examina la configuración e intenta detectar si una correspondencia de criptografía basada túnel ipsec de LAN a LAN está configurada. Si está configurado, realiza un control de múltiples puntos de la configuración y resalta cualesquiera Errores de configuración y configuraciones para el túnel que sería negociado.

Debugs ASA

Para resolver problemas la negociación de túnel del IPSec IKEv1 en un Firewall ASA, usted puede utilizar estos **comandos debug**:

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

> **Nota:** Si el número de VPN hace un túnel en el ASA es significativo, el **par de la condición del debug crypto que** utilizan al **comando a.b.c.d** debe antes de que usted permita a los debugs para limitar las salidas de los debugs para incluir solamente al par especificado.

Debugs del router IOS

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

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

> **Nota:** Si el número de VPN hace un túnel en el IOS es significativo, el **par de la condición del debug crypto que A.B.C.D** se utiliza **ipv4 debe** antes de que usted permita a los debugs para limitar las salidas de los debugs para incluir solamente al par especificado.

> Consejo: Refiera al L2L más común y al IPSec VPN del Acceso Remoto que resuelve problemas el documento de Cisco de las soluciones para más información sobre cómo resolver problemas un 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
- Inspector del LAN a LAN del IPSec
- Soporte Técnico y Documentación - Cisco Systems