Solucione problemas comunes con VPN IPSec L2L y de acceso remoto

Contenido

Introducción

Antecedentes

Prerequisites

La Configuración de VPN IPSec no Funciona

Los clientes VPN no pueden conectarse con ASA

La conexión del cliente VPN se corta con frecuencia en el primer intento o "Security Connection terminated by peer. Reason 433." o "Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)"

El acceso remoto y los usuarios del EZVPN conectan con el VPN pero no pueden acceder a los recursos externos

Incapaz de conectar a más de tres usuarios del cliente de VPN

Incapaz de iniciar la sesión o una aplicación y de reducir la transferencia después del establecimiento del túnel

No se puede iniciar el túnel VPN desde ASA

Incapaz de pasar el tráfico a través del túnel VPN

Configure el par de respaldo para el túnel VPN en el mismo mapa criptográfico

Inhabilitar/túnel del reinicio VPN

Algunos túneles no cifrados

Error:- %ASA-5-713904: Grupo = DefaultRAGroup, IP = x.x.x.x, ...versión v2 del modo de transacción no compatible.Túnel finalizado.

Error:- %ASA-6-722036: grupo de clientes del grupo de usuarios xxxx IP x.x.x.x que transmite el paquete grande 1220 (umbral 1206)

Mensaje de error cuando QoS se habilita en un extremo del túnel VPN

ADVERTENCIA: entrada de mapa criptográfico incompleta

Error:- %ASA-4-400024: IDS:2151 Paquete ICMP grande de a en interfaz externa

Error:- %ASA-4-402119: IPSEC: se ha recibido un paquete de protocolo (SPI=spi, número de secuencia= número_seq) de remote_IP (nombre de usuario) a local_IP que no ha superado la comprobación de bloqueo de reproducción.

Mensaje de error - %ASA-4-407001: Denegar tráfico para nombre_interfaz_host:dirección_interna, límite de número de licencia excedido

Mensaje de error - %VPN_HW-4-PACKET_ERROR:

Mensaje de error: Comando rechazado: elimine primero la conexión crypto entre VLAN XXXX y XXXX.

Mensaje de error - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Paquete descartado - Opción de ampliación de ventana no válida para la sesión x.x.x.x:27331 a x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

%ASA-5-305013: reglas NAT asimétricas coincidentes para reenvío e inversión . Poner al día por favor los flujos de este problema

%ASA-5-713068: mensaje de notificación no rutinario recibido: notify_type

%ASA-5-720012: (VPN-Secondary) Error al actualizar los datos de tiempo de ejecución de conmutación por error de IPSec en la unidad en espera (o) %ASA-6-720012: (VPN-unit) Error al actualizar los datos de tiempo de ejecución de conmutación por error de IPsec en la unidad en espera

Error:- %ASA-3-713063: dirección de par IKE no configurada para destino 0.0.0.0

Error: %ASA-3-752006: el Administrador de túneles no pudo enviar un mensaje KEY_ACQUIRE.

Error: %ASA-4-402116: IPSEC: se recibió un paquete ESP (SPI= 0x99554D4E, número de secuencia= 0x9E) de XX.XX.XX.XX (usuario= XX.XX.XX.XX) a YY.YY.YY.YY

No podido iniciar el instalador 64-bit VA para habilitar el adaptador virtual debido al error 0xffffffff

El Cisco VPN Client no trabaja con el indicador luminoso LED amarillo de la placa muestra gravedad menor de datos en Windows 7

Alerta: "Es posible que la funcionalidad VPN no funcione en absoluto"

Error de Padding de IPSec

El Túnel VPN se Desconecta Después de 18 Horas de Actividad

El Flujo de Tráfico no se Mantiene Después de que el Túnel LAN-LAN se Renegocie

Mensaje de Error que Indica que se ha Alcanzado el Ancho de Bando de la Funcionalidad Crypto

Problema: el tráfico de cifrado saliente en un túnel IPsec falla, incluso si el tráfico de descifrado entrante funciona.

Miscelánea

Información Relacionada

Introducción

Este documento contiene las soluciones más comunes para los problemas de VPN de IPSec.

Antecedentes

Las soluciones que se describen aquí provienen directamente de solicitudes de servicio que el soporte técnico de Cisco ha resuelto.

Muchas de estas soluciones se implementan antes de la resolución de problemas detallada de una conexión VPN IPsec.

Este documento proporciona un resumen de los procedimientos comunes que debe probar antes de comenzar a resolver problemas de una conexión.

Aunque los ejemplos de configuración en este documento son para uso en routers y dispositivos de seguridad, casi todos estos conceptos también son aplicables a VPN 3000 .

Consulte Solución de Problemas de Seguridad IP - Comprensión y Uso de los Comandos debug para obtener una explicación de los comandos debug comunes que se utilizan para resolver problemas de IPSec en el software Cisco IOS® y en .

Nota: ASA no pasa el tráfico multicast sobre los túneles IPsec VPN.

Advertencia: Muchas de las soluciones presentadas en este documento pueden conducir a una pérdida temporal de toda la conectividad VPN IPsec en un dispositivo.

Se recomienda que estas soluciones se implementen con precaución y de acuerdo con su política

del control de cambios.

Prerequisites

Requirements

Cisco recomienda conocer la configuración de VPN IPsec en estos dispositivos de Cisco:

- Cisco ASA 5500 Series Security Appliance
- Routers Cisco IOS®

Componentes Utilizados

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

- Cisco ASA 5500 Series Security Appliance
- IOS® de Cisco

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.

Convenciones

Consulte el documento Cisco Technical Tips Conventions (Convenciones sobre consejos técnicos de Cisco) para obtener más información sobre las convenciones de los documentos.

La Configuración de VPN IPSec no Funciona

Problema

Una solución recientemente configurada o modificada de VPN IPSec no funciona.

Una configuración de VPN IPSec ya no funciona.

Soluciones

Esta sección contiene las soluciones para la mayoría de los problemas de VPN IPSec.

Aunque no se enumeran en ningún orden concreto, estas soluciones se pueden utilizar como una lista de comprobación de elementos que se deben verificar o probar antes de llevar a cabo una remediación exhaustiva.

Todas estas soluciones provienen directamente de las solicitudes de servicio del TAC y han resuelto numerosos problemas.

- Habilitar NAT-Traversal (Problema de VPN RA n.º 1)
- Probar la Conectividad Correctamente
- Habilitar ISAKMP
- Habilitar/Inhabilitar PFS
- Despejar las Asociaciones de Seguridad Antiguas o Existentes (Túneles)
- Verificar la duración de ISAKMP
- Habilitar o Inhabilitar los Keepalives de ISAKMP
- Volver a Ingrese o Recuperar Claves Previamente Compartidas
- Clave Previamente Compartida No Coincidente
- Quitar y Volver a Aplicar Mapas Crypto
- Verifique que los Comandos sysopt estén Presentes (/ASA Only)
- Verificar la identidad ISAKMP
- Verificar el Tiempo de Espera de la Sesión/Inactividad
- Verificar que las ACL sean Correctas y Estén Enlazadas al Mapa Crypto
- Verificar las Políticas ISAKMP
- Verificar que el Ruteo sea Correcto
- Verificar que Transform-Set sea Correcto
- Verifocar el Nombre y los Números de Secuencia del Mapa Crypto
- Verificar que la Dirección IP sea Correcta
- Verificar el Grupo de Túnel y los Nombres de Grupo
- Inhabilitar XAUTH para los Peers L2L
- Agotamiento Progresivo del Conjunto VPN
- Problemas con el Tiempo de Espera para el Tráfico del Cliente VPN

Nota: Algunos de los comandos de estas secciones se han reducido a una segunda línea debido a consideraciones espaciales.

Habilitar NAT-Traversal (Problema de VPN RA n.º 1)

NAT-Traversal (o NAT-T) permite que el tráfico VPN pase a través de dispositivos NAT o PAT, como un router SOHO de Linksys.

Si NAT-T no está habilitado, los usuarios de VPN Client a menudo parecen conectarse al ASA sin problemas, pero no pueden acceder a la red interna detrás del dispositivo de seguridad.

Si no habilita NAT-T en el dispositivo NAT/PAT, puede recibir el mensaje de error **`error de creación de traducción regular para el protocolo 50 src inside:10.0.1.26 dst outside:10.9.69.4`** en el ASA.

Del mismo modo, si no puede realizar el inicio de sesión simultáneo desde la misma dirección IP, **`el cliente finalizará localmente la conexión VPN segura. Motivo 412: el par remoto ya no responde.`**aparece un mensaje de error.

Habilite NAT-T en el dispositivo de VPN headend para resolver este error.

Nota: Con Cisco IOS® Software Release 12.2(13)T y posteriores, NAT-T se habilita de forma predeterminada en Cisco IOS®.

Este es el comando para habilitar NAT-T en un Dispositivo de Seguridad de Cisco. El valor veinte (20) de este ejemplo es el tiempo de keepalive (predeterminado).

ASA

<#root>

```
securityappliance(config)#
```

`crypto isakmp nat-traversal 20`

Para que funcione, los clientes también deben ser modificados.

En Cisco VPN Client, navegue hastaConnection Entries y haga clic en Modify. Se abre una nueva ventana en la que debe seleccionar la fichaTransporte.

En esta ficha, haga clic en el botón de opción Enable Transparent Tunneling y theIPSec over UDP (NAT / PAT). A continuación, haga clic enGuardar y probar la conexión.

Es importante permitir el UDP 4500 para los puertos NAT-T, UDP 500 y ESP mediante la configuración de una ACL porque el ASA actúa como un dispositivo NAT.

Consulte Configuración de un Túnel IPsec a través de un Firewall con NAT para obtener más información para aprender más sobre la configuración de ACL en ASA.

Probar la Conectividad Correctamente

Idealmente, la conectividad VPN se prueba desde dispositivos detrás de los dispositivos terminales que realizan el cifrado, pero muchos usuarios prueban la conectividad VPN con el comando pingen los dispositivos que realizan el cifrado.

Mientras que el ping generalmente funciona para este propósito, es importante obtener su ping de la interfaz correcta.

Si el ping se origina incorrectamente, puede parecer que la conexión VPN ha fallado cuando realmente funciona. Este es un ejemplo:

Crypto ACL de Router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Crypto ACL de Router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

En esta situación, la paginación debe originarse en la red interna detrás de cualquier router. Esto es así porque las ACL crypto solo están configuradas para cifrar el tráfico con esas direcciones de origen.

Las aplicaciones originadas en las interfaces externas de cualquiera de los routers no están cifradas. Utilice las opciones extendidas del comando ping en el modo EXEC privilegiado para obtener un ping desde la interfaz interna de un router:

<#root>

```
routerA#
ping
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
```

```
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
```

Packet sent with a source address of 192.168.100.1

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

Imagine que los routers de este diagrama se han sustituido por dispositivos de seguridad ASA. El sonido que se utiliza para probar la conectividad también se puede obtener de la interfaz interna con la palabra clave insidekeyword:

<#root>

```
securityappliance#
```

ping inside 192.168.200.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

No se recomienda dirigirse a la interfaz interna de un dispositivo de seguridad con suping.

Si debe dirigirse a la interfaz interior con yourping, debe habilitar management-access en esa interfaz o el dispositivo no contestará.

<#root>

```
securityappliance(config)#
```

management-access inside

Cuando existe un problema con la conectividad, incluso la fase uno (1) de VPN no funciona.

En el ASA, si falla la conectividad, la salida de SA es similar a este ejemplo, que indica una posible configuración incorrecta del peer crypto y/o una configuración incorrecta de la propuesta ISAKMP:

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
```

```
    Rekey   : no              State   : MM_WAIT_MSG2
```

El estado puede ser de MM_WAIT_MSG2 a MM_WAIT_MSG5, que denota la falla del intercambio de estado en cuestión en modo principal (MM).

La salida SA crypto cuando la fase 1 está activa es similar a este ejemplo:

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Habilitar ISAKMP

Si no hay ninguna indicación de que un túnel VPN IPsec funcione, es posible que ISAKMP no se haya habilitado. Asegúrese de haber habilitado ISAKMP en sus dispositivos.

Utilice uno de estos comandos para habilitar ISAKMP en sus dispositivos:

IOS® de Cisco

<#root>

```
router(config)#
```

crypto isakmp enable

Cisco ASA (reemplazofuera con la interfaz que desee)

<#root>

```
securityappliance(config)#
```

crypto isakmp enable outside

También puede obtener este error cuando habilita ISAKMP en la interfaz exterior:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

La causa del error puede ser que el cliente detrás de ASA obtiene PAT al puerto udp 500 antes de que isakmp se pueda habilitar en la interfaz. Una vez que se quita esa traducción de PAT (despejar xlate), isakmp puede ser habilitado.

Verifique que los números de puerto UDP 500 y 4500 estén reservados para la negociación de conexiones ISAKMP con el par.

Cuando ISAKMP no esté habilitado en la interfaz, el cliente VPN muestra un mensaje de error similar a este mensaje:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

Para resolver este error, habilite ISAKMP en la interfaz crypto del gateway de VPN.

Habilitar/Inhabilitar PFS

En las negociaciones de IPSec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior.

Active o desactive PFS en ambos pares de túnel; de lo contrario, el túnel IPsec de LAN a LAN (L2L) no se establece en el router ASA/Cisco IOS®.

Perfect Forward Secrecy (PFS) es propiedad de Cisco y no es soportado en otros dispositivos de terceros.

ASA:

PFS se inhabilita de forma predeterminada. Para habilitar PFS, utilice el comando pfscon la palabra clave enable en el modo de configuración de política de grupo. Para inhabilitar PFS, ingrese la palabra clave disable (inhabilitar).

<#root>

```
hostname(config-group-policy)#
```

pfs {enable | disable}

Para quitar el atributo PFS de la configuración, ingrese la forma no de este comando.

Una política de grupo puede heredar un valor para PFS de otra política de grupo. Ingrese la forma no de este comando para evitar la transferencia de un valor.

<#root>

```
hostname(config-group-policy)#
no pfs
```

Router Cisco IOS®:

Para especificar que IPSec debe solicitar PFS cuando se soliciten nuevas Asociaciones de Seguridad para esta entrada de mapa criptográfico, utilice el comando set pfsen el modo de configuración de mapa criptográfico.

Para especificar que IPSec requiere PFS cuando recibe solicitudes para nuevas Asociaciones de Seguridad, utilice el comando set pfsen el modo de configuración de mapa criptográfico.

Para especificar que IPSec no debe solicitar a PFS, utilice la forma no de este comando. De forma predeterminada, PFS no se solicita. Si no se especifica ningún grupo con este comando, como valor predeterminado se utiliza group1.

```
set pfs [group1 | group2]
no set pfs
```

Para el comando set pfs:

- group1: Especifica que IPSec debe utilizar el grupo de módulos primos Diffie Hellman de 768 bits cuando se ejecuta el nuevo intercambio Diffie-Hellman.
- group2: Especifica que IPSec debe utilizar el grupo de módulos primos Diffie Hellman de 1024 bits cuando se ejecuta el nuevo intercambio Diffie-Hellman.

Ejemplo:

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
set pfs group2
```

Borrar asociaciones de seguridad antiguas o actuales (túneles)

Si este mensaje de error aparece en el router Cisco IOS®®, el problema es que la SA ha expirado o se ha borrado.

El dispositivo de extremo de túnel remoto no sabe que utiliza una SA expirada para enviar un paquete (no un paquete de establecimiento de SA).

Cuando se ha establecido una nueva SA, la comunicación se reanuda y se inicia el tráfico interesante a través del túnel para crear una nueva SA y restablecer el túnel.

<#root>

%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x has no SA

Despejar las asociaciones de seguridad ISAKMP (Fase I) e IPSec (Fase II) (SA) es la solución más simple y, a menudo, la mejor solución para resolver los problemas de VPN IPSec.

Si usted despeja las SA, puede solucionar frecuentemente una amplia variedad de mensajes de error y de conductas extrañas sin la necesidad de tener que resolver problemas.

Si bien esta técnica se puede utilizar fácilmente en cualquier situación, casi siempre es un requisito despejar las SA después de cambiar o agregar a la configuración de IPSec VPN actual.

Por otra parte, si bien es posible despejar solo asociaciones de seguridad específicas, el mayor beneficio se obtiene cuando despeja las SA en forma global en el dispositivo.

Una vez que las asociaciones de seguridad han sido despejadas, puede ser necesario enviar el tráfico a través del túnel para restablecerlas.

Advertencia: a menos que especifique qué asociaciones de seguridad debe borrar, los comandos que aparecen aquí pueden borrar todas las asociaciones de seguridad del dispositivo. Proceda con cautela si otros túneles de VPN IPSec están en uso.

1. Vea las asociaciones de seguridad antes de despejarlas.

    a. Cisco IOS®

    <#root>

    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa

    b. Dispositivos de seguridad Cisco ASA

    <#root>

    securityappliance#

    show crypto isakmp sa

    securityappliance#

```
show crypto ipsec sa
```

2. Despeje las asociaciones de seguridad. Cada comando se puede ingresar como se muestra en negrita o con las opciones que aparecen con ellos.

    a. IOS® de Cisco

        a. ISAKMP (Fase I)

<#root>

```
router#

clear crypto isakmp

 ?
  <0 - 32766>  connection id of SA
  <cr>
```

        b. IPSec (Fase II)

<#root>

```
router#

clear crypto sa

 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

    b. Dispositivos de seguridad Cisco ASA

        a. ISAKMP (Fase I)

<#root>

```
securityappliance#

clear crypto isakmp sa
```

        b. IPSec (Fase II)

<#root>

```
security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

Verificar la duración de ISAKMP

Si frecuentemente los usuarios se desconectan a través del túnel L2L, el problema puede ser la menor duración configurada en SA ISAKMP.

Si ocurre alguna discrepancia en la duración de ISAKMP, puede recibir el mensaje%ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekey intent due to collisionerror message in /ASA.

El valor predeterminado es 86.400 segundos o 24 horas. Como regla general, una duración más corta proporciona negociaciones de ISAKMP más seguras (hasta un punto); sin embargo, con duraciones más cortas, el dispositivo de seguridad configura las SA IPsec futuras más rápido.

Se logra una coincidencia cuando ambas políticas de los dos peers contienen los mismos valores de parámetro de cifrado, hash, autenticación y Diffie-Hellman, y cuando la política del peer remoto especifica una duración inferior o igual a la duración de la política comparada.

Si las duraciones no son idénticas, se utiliza la duración más corta (de la política del peer remoto). Si no se encuentra una coincidencia aceptable, IKE rechaza la negociación y la SA IKE no se establece.

Especifique la duración de SA. En este ejemplo, se establece una duración de 4 horas (14.400 segundos). El valor predeterminado es 86.400 segundos (24 horas).

ASA

<#root>

```
hostname(config)#

isakmp policy 2 lifetime  14400
```

Router Cisco IOS®

<#root>

```
R2(config)#
crypto isakmp policy 10
R2(config-isakmp)#
lifetime 86400
```

Si se supera la duración máxima configurada, usted recibe el siguiente mensaje de error cuando la conexión VPN se termina:

Secure VPN Connection terminated locally by the Client. Motivo 426: Se Ha Superado La Duración Máxima Configurada.

Para resolver este mensaje de error, establezca elvalor de duración en cero (0) para establecer la duración de una asociación de seguridad IKE en infinito. La VPN siempre está conectada y no termina.

```
hostname(config)#isakmp policy 2 lifetime 0
```

También puede inhabilitar re-xauth en la política de grupo para resolver el problema.

Habilitar o Inhabilitar los Keepalives de ISAKMP

Si configura los keepalives de ISAKMP, esto ayuda a prevenir las caídas esporádicas de las VPN de Acceso Remoto o de LAN a LAN, que incluyen los clientes VPN, los túneles y los túneles que se caen después de un período de inactividad.

Esta función permite que el extremo del túnel monitoree la presencia continua de un peer remoto e informa su propia presencia a ese par.

Si el peer deja de responder, el extremo quita la conexión.

Para que los keepalives de ISAKMP funcionen, ambos extremos de VPN deben soportarlos.

Configure señales de mantenimiento ISAKMP en Cisco IOS® con este comando:

<#root>

```
router(config)#
crypto isakmp keepalive 15
```

Utilice estos comandos para configurar señales de mantenimiento ISAKMP en los dispositivos de seguridad ASA:

Cisco ASA para el grupo de túnel denominado10.165.205.222

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive
   threshold 15 retry 10
```

En algunas situaciones, es necesario inhabilitar esta función para solucionar el problema, por ejemplo, si el cliente VPN está detrás de un Firewall que evita los paquetes DPD.

Cisco ASA, para el grupo de túnel denominado10.165.205.222

Desactive el procesamiento de keepalive IKE, que está activado de forma predeterminada.

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

Inhabilite Keepalive para Cisco VPN Client 4.x.

Navegue hasta%System Root% > Program Files > Cisco Systems >VPN Client > Profiles en la PC cliente que experimenta el problema para inhabilitar el keepalive IKE, y edite el archivo PCF, donde corresponda, para la conexión.

Cambie theForceKeepAlives=0(predeterminado) a ForceKeepAlives=1.

Los keepalives son propiedad de Cisco y no son soportados por dispositivos de terceros.

Volver a Ingrese o Recuperar Claves Previamente Compartidas

En muchos casos, un simple error tipográfico puede ser el culpable cuando un túnel VPN IPsec no funciona. Por ejemplo, en el dispositivo de seguridad, las claves previamente compartidas se ocultan una vez que se ingresan.

Esta ofuscación hace imposible ver si una clave es incorrecta. Asegúrese de que ha ingresado las claves previamente compartidas correctamente en cada extremo de VPN.

Vuelva a introducir una clave para asegurarse de que es correcta; se trata de una solución sencilla que puede ayudarle a evitar una resolución de problemas detallada.

In Remote Access VPN, verifique se que hayan ingresado la clave previamente compartida y el nombre de grupo válidos en Cisco VPN Client.

Puede enfrentarse a este error si el nombre de grupo o la clave previamente compartida no coinciden entre el cliente VPN y el dispositivo de cabecera.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

Advertencia: Si elimina comandos relacionados con criptografía, es probable que desactive uno o todos sus túneles VPN. Utilice estos comandos con precaución y consulte la directiva de control de cambios de su organización antes de quitar los comandos relacionados con criptografía.

Utilice estos comandos para remover y volver a ingresar la clave previamente compartida keysecretkeypara el peer10.0.0.1o el groupvpngroupin Cisco IOS®:

VPN de LAN a LAN de Cisco

<#root>

```
router(config)#
```

no crypto isakmp key secretkey

```
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

VPN de Acceso Remoto de Cisco

<#root>

```
router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

Utilice estos comandos para quitar y volver a ingresar la clave previamente compartida keysecretkeypara el peer10.0.0.1en los dispositivos de seguridad /ASA:

Cisco 6.x

<#root>

```
(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco/ASA 7.x y versiones posteriores

<#root>

```
securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#
```

```
ikev1


pre-shared-key
   secretkey
```

Clave Previamente Compartida No Coincidente

La iniciación del Túnel VPN se desconecta. Este problema ocurre debido a una clave previamente compartida no coincidente durante las negociaciones de la fase I.

El mensaje MM_WAIT_MSG_6en el comando show crypto isakmp indica una clave previamente compartida no coincidente como se muestra en este ejemplo:

```
<#root>

ASA#

show crypto isakmp sa


Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :

MM_WAIT_MSG_6
```

Para resolver este problema, vuelva a introducir la clave previamente compartida en ambos dispositivos; la clave previamente compartida debe ser única y coincidir. Para obtener más información, consulte Volver a introducir o Recuperar claves previamente compartidas.

Quitar y Volver a Aplicar Mapas Crypto

Cuando borra las asociaciones de seguridad, y no resuelve un problema de VPN IPsec, quite y vuelva a aplicar el mapa crypto relevante para resolver una amplia variedad de problemas que incluyen caídas intermitentes del túnel VPN y fallas de algunos sitios VPN para aparecer.

Advertencia: Si quita un mapa criptográfico de una interfaz, definitivamente desactiva cualquier túnel IPsec asociado con ese mapa criptográfico. Proceda con precaución con estos pasos y considere la política de control de cambios de su organización antes de continuar.

Utilice estos comandos para quitar y reemplazar un mapa criptográfico en Cisco IOS®:

Comience por quitar el mapa crypto de la interfaz. Utilice la forma no del comando crypto map.

<#root>

```
router(config-if)#
no crypto map mymap
```

Continúe utilizando la enoforma para quitar un mapa criptográfico completo.

<#root>

```
router(config)#
no crypto map mymap 10
```

Reemplace el mapa crypto en la interfaz Ethernet0/0 para el peer 10.0.0.1. Este ejemplo muestra la configuración requerida mínima de la mapa crypto:

<#root>

```
router(config)#
crypto map mymap 10 ipsec-isakmp
router(config-crypto-map)#
match address 101
router(config-crypto-map)#
set transform-set mySET
router(config-crypto-map)#
set peer 10.0.0.1
router(config-crypto-map)#
exit
router(config)#
interface ethernet0/0
router(config-if)#
crypto map mymap
```

Utilice estos comandos para quitar y reemplazar un mapa crypto en el ASA:

Comience por quitar el mapa crypto de la interfaz. Utilice la forma no del comando crypto map.

<#root>

```
securityappliance(config)#
```

```
no crypto map mymap interface outside
```

Continúe utilizando la enoforma para quitar los otros comandos de mapa criptográfico.

```
<#root>

securityappliance(config)#

no crypto map mymap 10 match
   address 101

securityappliance(config)#

no crypto map mymap set
   transform-set mySET

securityappliance(config)#

no crypto map mymap set
   peer 10.0.0.1
```

Reemplace el mapa crypto para el peer 10.0.0.1. Este ejemplo muestra la configuración requerida mínima de la mapa crypto:

```
<#root>

securityappliance(config)#

crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

Si usted quita y vuelva a aplicar un mapa crypto, esto también resuelve el problema de conectividad si la dirección IP de headend se ha cambiado.

Verifique que los comandos sysopt estén presentes (solo ASA)

Los comandos sysopt connection permit-ipsecandsysopt connection permit-vpnallow paquetes de un túnel IPsec y sus cargas útiles para omitir las ACL de interfaz en el dispositivo de seguridad.

Es probable que los túneles IPsec que se terminan en el dispositivo de seguridad fallen si uno de estos comandos no se habilita.

En Security Appliance Software Version 7.0 y versiones anteriores, el comando sysopt relevante para esta situación es sysopt connection permit-ipsec.

En Security Appliance Software Version 7.1(1) y versiones posteriores, el comando sysopt relevante para esta situación es sysopt connection permit-vpn.

En la versión 6.x, esta funcionalidad estádeshabilitada de forma predeterminada. Con /ASA 7.0(1) y versiones posteriores, esta funcionalidad estáhabilitada de forma predeterminada. Utilice estos comandos show para determinar si el comando relevantsysopt está habilitado en su dispositivo:

Cisco ASA

```
<#root>

securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn


!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

Utilice estos comandos para habilitar el comando correctsysopt para su dispositivo:

Cisco ASA

```
<#root>

securityappliance(config)#

sysopt connection permit-vpn
```

Si no desea utilizar el comando sysopt connection, permita explícitamente el tráfico interesante requerido desde el origen al destino.

Por ejemplo, de LAN remota a LAN local del dispositivo remoto y "puerto UDP 500" para la interfaz externa del dispositivo remoto a la interfaz externa del dispositivo local, en ACL externa.

Verificar la identidad ISAKMP

Si el túnel VPN IPsec ha fallado dentro de la negociación IKE, la falla puede deberse a la falla o a la incapacidad de su peer para reconocer la identidad de su peer.

Cuando dos peers utilizan IKE para establecer asociaciones de seguridad IPSec, cada peer envía su identidad ISAKMP al peer remoto.

Envía su dirección IP o su nombre de host según cómo cada uno tenga configurada su identidad ISAKMP.

De forma predeterminada, la identidad ISAKMP de la unidad de firewall se establece en la dirección IP.

Como regla general, configure el dispositivo de seguridad y las identidades de sus peers de la misma manera para evitar una falla de negociación IKE.

Para configurar el ID de fase 2 que se enviará al peer, utilice el comando isakmp identitycommand en el modo de configuración global.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

O

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

O

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

El túnel VPN no puede activarse después de un cambio de configuración de a ASA con la herramienta de migración de la configuración de ASA; estos mensajes aparecen en el registro:

[IKEv1]: Grupo = x.x.x.x, IP = x.x.x.x, se ha encontrado una entrada de tabla de pares obsoleta, quitando.

[IKEv1]: Grupo = x.x.x.x, IP = x.x.x.x, Error al eliminar el par de la tabla del correlacionador, no hay coincidencia.

[IKEv1]: Grupo = x.x.x.x, IP = x.x.x.x, build_ipsec_delete(): No hay SPI para identificar la SA de fase 2.

[IKEv1]: Grupo = x.x.x.x, IP = x.x.x.x, Error al eliminar el par de la tabla del correlacionador, no hay coincidencia.

Verificar el Tiempo de Espera de la Sesión/Inactividad

Si el tiempo de espera de inactividad se establece en 30 minutos (valor predeterminado), significa que el túnel se desactiva después de 30 minutos sin tráfico a través de él.

El cliente VPN se desconecta después de 30 minutos independientemente del parámetro de tiempo de espera inactivo y encuentra `el` error **`PEER_DELETE-IKE_DELETE`**_UNSPECIFIEDerror.

Configure el tiempo de espera inactivo y el tiempo de espera de la sesión para que el túnel siempre esté activo, y para que el túnel nunca se caiga incluso cuando se utilicen dispositivos de terceros.

ASA

Ingrese el comando evpn-idle-timeout en el modo de configuración de política de grupo o en el modo de configuración de nombre de usuario para configurar el período de tiempo de espera del usuario:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-idle-timeout none
```

Configure una cantidad máxima de tiempo para las conexiones VPN con el comando vpn-session-timeout en el modo de configuración de política de grupo o en el modo de configuración de nombre de usuario:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-session-timeout none
```

Cuando tiene unnel-all configurado, no necesita configurar idle-timeout porque, incluso si configura VPN-idle timeout, no funciona porque todo el tráfico pasa a través del túnel (ya que tunnel-all está configurado).

Por lo tanto, el tráfico interesante (o incluso el tráfico generado por la PC) es interesante y no permite que Idle-timeout entre en acción.

Router Cisco IOS®

Utilice el comando crypto ipsec security-association idle-time en el modo de configuración global o en el modo de configuración de mapa criptográfico para configurar el temporizador de inactividad de SA IPsec.

De forma predeterminada, los temporizadores de inactividad de SA IPSec están inhabilitados.

<#root>

```
crypto ipsec security-association idle-time
seconds
```

El tiempo se mide en segundos, que el temporizador de inactividad permite que un par inactivo mantenga una SA. Los valores válidos para el argumento de segundos varía de 60 a 86.400.

Verifcar que las ACL sean Correctas y estén Enlazadas al Mapa Crypto

Hay dos listas de acceso que se utilizan en una configuración típica de VPN IPSec. Una lista de acceso se utiliza para eximir el tráfico destinado al túnel VPN del proceso NAT.

La otra lista de acceso define qué tráfico cifrar; esto incluye una ACL crypto en una configuración de LAN a LAN o una ACL de túnel dividido en una configuración de acceso remoto.

Cuando estas ACL se configuran incorrectamente o se pierden, el tráfico quizás fluye en una dirección a través del túnel VPN o no se envía a través del túnel en absoluto.

Asegúrese de enlazar la ACL crypto con el mapa crypto con el comando crypto map match address en el modo de configuración global.

Asegúrese de haber configurado todas las listas de acceso necesarias para completar su configuración de VPN IPSec y de que esas listas de acceso definan el tráfico correcto.

Esta lista contiene las cosas simples para verificar cuando usted sospecha que una ACL es la causa de los problemas con su VPN IPSec.

Asegúrese de que sus ACL crypto y de exención de NAT especifiquen el tráfico correcto.

Si usted tiene varios túneles VPN y varias ACL crypto, asegúrese de que esas ACL no se superpongan.

Asegúrese de que su dispositivo esté configurado para utilizar la ACL de exención de NAT. En un router, esto significa que usted utiliza el comando route-map.

En el ASA, esto significa que usted utiliza el comando thenat (0). Se requiere una ACL de exención de NAT para las configuraciones tanto de LAN a LAN como de acceso remoto.

Aquí, un router Cisco IOS® está configurado para eximir el tráfico que se envía entre 192.168.100.0 /24y 192.168.200.0 /24o192.168.1.0 /24 de NAT. El tráfico destinado a cualquier otra parte está sujeto a la sobrecarga NAT:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

Las ACL de exención de NAT solo funcionan con la dirección IP o las redes IP, como esos ejemplos mencionados (access-list noNAT), y deben ser idénticas a las ACL de mapa crypto.

Las ACL de exención de NAT no funcionan con los números de puerto (por ejemplo, 23, 25,...).

En un entorno VOIP, donde las llamadas de voz entre redes se comunican a través de la VPN, las llamadas de voz no funcionan si las ACL NAT 0 no están configuradas correctamente.

Antes de la resolución de problemas, se recomienda verificar el estado de la conectividad VPN porque el problema podría ser la configuración incorrecta de ACL exentas de NAT.

Usted puede recibir el mensaje de error que se muestra si hay una configuración incorrecta de las ACL de exención de NAT (nat 0).

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

Ejemplo Incorrecto:

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

Si la exención de NAT (NAT 0) no funciona, intente quitarla y ejecute el comando NAT 0para que funcione.

Asegúrese de que sus ACL no están al revés y de que sean del tipo adecuado.

Las ACL de exención de NAT y crypto para las configuraciones de LAN a LAN deben escribirse desde la perspectiva del dispositivo en el cual se configura la ACL.

Esto significa que las ACL deben reflejarse entre sí. En este ejemplo, se configura un túnel de LAN a LAN entre192.168.100.0 /24y192.168.200.0 /24.

Crypto ACL de Router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

Crypto ACL de Router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

Aunque no se muestra aquí, este mismo concepto se aplica a los dispositivos de seguridad ASA.

En ASA, las ACL de túnel dividido para las configuraciones de acceso remoto deben ser listas de acceso estándar que permitan el tráfico a la red a la que los clientes VPN necesitan acceso.

Los routers Cisco IOS® pueden utilizar ACL extendida para túnel dividido. En la lista de acceso ampliada, usar 'any'en el origen en la ACL de túnel dividido es similar a inhabilitar el túnel dividido.

Utilice solamente las redes de origen en la ACL extendida para el túnel dividido.

Ejemplo Correcto:

<#root>

```
access-list 140 permit ip
10.1.0.0 0.0.255.255
 10.18.0.0 0.0.255.255
```

Ejemplo Incorrecto:

```
<#root>
access-list 140 permit ip
any
 10.18.0.0 0.0.255.255
```

IOS® de Cisco

```
<#root>
router(config)#
access-list 10 permit ip 192.168.100.0
router(config)#
crypto isakmp client configuration group MYGROUP
router(config-isakmp-group)#
acl 10
```

Cisco ASA

```
<#root>
securityappliance(config)#
access-list 10 standard
   permit 192.168.100.0 255.255.255.0
securityappliance(config)#
group-policy MYPOLICY internal
securityappliance(config)#
group-policy MYPOLICY attributes
securityappliance(config-group-policy)#
split-tunnel-policy
   tunnelspecified
securityappliance(config-group-policy)#
```

```
split-tunnel-network-list
   value 10
```

Configuración de la exención de NAT en la versión 8.3 de ASA para un túnel de VPN de sitio a sitio:

Debe establecerse una VPN de sitio a sitio entre HOASA y BOASA con ambos ASA con la versión 8.3. La configuración de la exención de NAT en HOASA parece similar a esto:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

Verificar las Políticas ISAKMP

Si el túnel IPsec no está ACTIVADO, verifique que las políticas ISAKMP se correspondan con con los peers remotos. Esta política ISAKMP es aplicable a las VPN IPsec de Sitio a Sitio (L2L) y de Acceso Remoto.

Si los Cisco VPN Clients o la VPN de sitio a sitio no pueden establecer el túnel con el dispositivo de extremo remoto, compruebe que los dos pares contienen los mismos valores de parámetro de cifrado, hash, autenticación y Diffie-Hellman.

Verifique cuando la política de peer remoto especifica una duración menor o igual a la duración en la política que envió el iniciador.

Si las duraciones no son idénticas, el dispositivo de seguridad utiliza la duración más corta. Si no existe una coincidencia aceptable, ISAKMP rechaza la negociación y la SA no se establece.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

A continuación, se proporciona el mensaje del log detallado:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

Este mensaje suele aparecer debido a políticas ISAKMP no coincidentes o a una sentencia NAT 0 perdida.

Además, aparece este mensaje:

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Este mensaje indica que los mensajes de la Fase 2 están en la cola después de que se complete la Fase 1. Este mensaje de error se debe a una de estas razones:

- Discordancia en la fase de cualquiera de los peers
- ACL impide que los peers completen la fase 1

Este mensaje suele aparecer después **del** mensaje **de** error **Remoción del peer de la tabla de peer, no match!**.

Si el Cisco VPN Client no puede conectar el dispositivo headend, el problema puede ser la discordancia de la política ISAKMP. El dispositivo de cabecera debe coincidir con una de las propuestas IKE de Cisco VPN Client.

Para la política ISAKMP y el conjunto de transformación IPsec que se utiliza en ASA, el cliente Cisco VPN no puede utilizar una política con una combinación de DES y SHA.

Si utiliza DES, debe utilizar MD5 para el algoritmo de hash o puede utilizar las otras combinaciones, 3DES con SHA y 3DES con MD5.

Verificar que el Ruteo sea Correcto

Asegúrese de que los dispositivos de cifrado, como los routers y los dispositivos de seguridad ASA, tengan la información de routing adecuada para enviar tráfico a través del túnel VPN.

Si existen otros routers detrás del dispositivo de gateway, asegúrese de que dichos routers saben cómo alcanzar el túnel y qué redes están en el otro lado.

Un componente crucial de ruteo en una implementación de VPN es Reverse Route Injection (RRI).

RRI coloca entradas dinámicas para las redes remotas o los clientes VPN en la tabla de ruteo de un gateway de VPN.

Estas rutas son útiles para el dispositivo en el cual están instaladas, así como para los otros dispositivos de la red, porque las rutas instaladas mediante RRI se pueden redistribuir a través de un protocolo de ruteo como EIGRP o OSPF.

En una configuración de LAN a LAN, es importante que cada extremo tenga una o más ruta a las redes para las que se supone se cifra el tráfico.

En este ejemplo, el Router A debe tener rutas a las redes detrás del Router B a través de 10.89.129.2. El Router B debe tener una ruta similar a 192.168.100.0 /24:

La primera manera de asegurarse de que cada router conozca la ruta apropiada es configurar las rutas estáticas para cada red de destino. Por ejemplo, el Router A puede tener estas declaraciones de ruta configuradas:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

Si el Router A fue reemplazado por un ASA, la configuración puede verse de la siguiente manera:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

Si existe un gran número de redes detrás de cada extremo, la configuración de las rutas estáticas se torna difícil de mantener.

En cambio, se recomienda que utilice Reverse Route Injection, según lo descrito. RRI se coloca en las rutas de la tabla de ruteo para todas las redes remotas enumeradas en la ACL crypto.

Por ejemplo, la ACL crypto y el mapa crypto del Router A son similares a lo siguiente:

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

Si el Router A fue reemplazado por un ASA, la configuración puede verse de la siguiente manera:

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

crypto map mymap 10 set reverse-route

En una configuración de Acceso Remoto, los cambios de ruteo no siempre son necesarios.

Sin embargo, si existen otros routers detrás del Dispositivo de Seguridad o del router de gateway VPN, esos routers necesitan conocer la trayectoria a los clientes VPN de alguna manera.

En este ejemplo, suponga que a los clientes VPN se les dan direcciones en el rango de 10.0.0.0 /24cuando se conectan.

Si no hay un protocol de ruteo funcionando entre el gateway y el otro router, las rutas estáticas se pueden utilizar en los routers como Router 2:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Si entre el gateway y otros routers se utiliza un protocolo de ruteo como EIGRP o OSPF, se recomienda que se utilice Reverse Route Injection según lo descrito.

RRI agrega automáticamente rutas para el cliente VPN a la tabla de ruteo del gateway. Estas rutas se pueden distribuir a los otros routers en la red.

Router Cisco IOS®:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

```
reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Dispositivo de seguridad Cisco ASA:

```
<#root>
crypto dynamic-map dynMAP 10 set transform-set mySET
crypto dynamic-map dynMAP 10 set reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

El problema de ruteo ocurre si el conjunto de direcciones IP asignadas para los clientes VPN son superposiciones con las redes internas del dispositivo headend. Para obtener más información, consulte la sección Redes Privadas Superpuestas .

Verificar que Transform-Set sea Correcto

Asegúrese de que los algoritmos de hash y cifrado de IPSec que usará transform set en ambos extremos sean los mismos.

Consulte la sección Referencia de comandos de la guía de configuración de Cisco Security Appliance para obtener más información.

Para la política ISAKMP y el conjunto de transformación IPsec que se utiliza en ASA, el cliente Cisco VPN no puede utilizar una política con una combinación de DES y SHA.

Si utiliza DES, debe utilizar MD5 para el algoritmo de hash o puede utilizar las otras combinaciones, 3DES con SHA y 3DES con MD5.

Verifique el Nombre y los Números de Secuencia de Mapa Crypto, y que el mapa Crypto esté aplicado en la interfaz correcta en la que comienza/termina el túnel IPsec

Si los peers estáticos y dinámicos están configurados en el mismo mapa crypto, el orden de las entradas de mapa crypto es muy importante.

El número de secuencia de la entrada de mapa criptográfico dinámico debe ser mayor que todas las demás entradas de mapa criptográfico estático.

Si las entradas estáticas tienen una numeración mayor que la entrada dinámica, las conexiones con dichos peers fallan y aparecen los debugs como se muestran.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

En el Dispositivo de Seguridad, solo se permite un mapa Crypto Dinámico para cada interfaz.

A continuación, se proporciona un ejemplo de un mapa crypto numerado correctamente que contiene una entrada estática y una entrada dinámica. Observe que la entrada dinámica tiene el número de secuencia más alto y que se ha dejado espacio para agregar entradas estáticas adicionales:

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe
```

Los nombres de mapa crypto distinguen entre mayúsculas y minúsculas.

Este mensaje de error también se puede ver cuando la secuencia de comando man crypto dinámica no es correcta, lo que hace que el peer llegue al mapa crypto incorrecto.

Esto también se debe a una lista de acceso criptográfico no coincidente que define el tráfico interesante:**%ASA-3-713042: El iniciador IKE no pudo encontrar la política:**

En un escenario en el que varios túneles VPN se terminen en la misma interfaz, cree un mapa criptográfico con el mismo nombre (solo se permite un mapa criptográfico por interfaz) pero con un número de secuencia diferente.

Esto es así para el router y ASA.

De manera similar, consulte ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco para obtener más información sobre la configuración del mapa criptográfico para el escenario L2L y Remote Access VPN.

Verificar que la Dirección IP sea Correcta

Cree y administre la base de datos de registros específicos de conexión para IPSec.

Para una configuración de VPN IPsec de LAN a LAN (L2L) del dispositivo de seguridad ASA, especifique el<name>del grupo de túnel como Dirección IP de peer remoto (extremo de túnel remoto) en el comando tunnel-group <name> type ipsec-l2.

La dirección IP del peer debe coincidir con los comandos inunnel group name y theCrypto map

set address.

Si bien usted configura la VPN con ASDM, se generó el nombre de grupo de túnel automáticamente con la dirección IP de peer correcta.

Si la dirección IP del par no está configurada correctamente, los registros pueden contener este mensaje, que se puede resolver mediante la configuración adecuada de la dirección IP del par.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

Cuando la dirección IP de peer no se ha configurado correctamente en la configuración crypto ASA, ASA no puede establecer el túnel VPN y cuelga en la etapa MM_WAIT_MSG4solamente.

Para resolver este problema, corrija la dirección IP de peer en la configuración.

Este es el resultado del comando show crypto isakmp cuando el túnel VPN se cuelga en el estado MM_WAIT_MSG4.

```
<#root>

hostname#

show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

Verificar el Grupo de Túnel y los Nombres de Grupo

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

El mensaje aparece cuando se cae un túnel porque el túnel permitido especificado en la política de grupo difiere del túnel permitido en la configuración del grupo de túnel.

```
<#root>

group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
```

```
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

Habilite la política de IPSec en Grupo Predeterminado en la política de Protocolos Existentes de Grupo Predeterminado.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Inhabilitar XAUTH para los Peers L2L

Si se configuran un túnel de LAN a LAN y un túnel VPN de acceso remoto en el mismo mapa criptográfico, se le solicita al par de LAN a LAN información XAUTH, y el túnel de LAN a LAN falla con "CONF_XAUTH" en la salida del comando show crypto isakmp.

A continuación, se proporciona un ejemplo del resultado de SA:

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

Este problema sólo se aplica a Cisco IOS®, mientras que ASA no se ve afectado por este problema, ya que utiliza grupos de túnel.

Utilice la palabra clave eno-xauthkeyword cuando ingrese la clave isakmp, de manera que el dispositivo no solicite al par información XAUTH (nombre de usuario y contraseña).

Esta palabra clave inhabilita XAUTH para los peers IPSec estáticos. Ingrese un comando similar a este en el dispositivo que tiene la configuración VPN L2L y RA en el mismo mapa de crypto:

<#root>

```
router(config)#
```

crypto isakmp key cisco123 address
**   172.22.1.164 no-xauth**

En la situación en la que ASA actúa como servidor Easy VPN, el cliente Easy VPN no puede conectarse al centro distribuidor debido al problema de Xauth.

Inhabilite la autenticación de usuario en el ASA para resolver el problema como se muestra:

```
<#root>

ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#

tunnel-group example-group ipsec-attributes

ASA(config-tunnel-ipsec)#

isakmp ikev1-user-authentication none
```

Vea la sección Miscelánea de este documento para saber más sobre el comando isakmp ikev1-user-authentication.

Agotamiento Progresivo del Conjunto VPN

Cuando el rango de las direcciones IP asignadas al conjunto VPN no es suficiente, usted puede extender la disponibilidad de las direcciones IP de dos maneras:

1. Quite el rango existente y defina el nuevo rango. Aquí tiene un ejemplo:

```
<#root>

CiscoASA(config)#

no ip local pool testvpnpool 10.76.41.1-10.76.41.254

CiscoASA(config)#

ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. Cuando las subredes discontinuas deben ser agregadas al conjunto VPN, usted puede definir dos conjuntos VPN separados y luego especificarlos en orden en “túnel-group attributes”. Aquí tiene un ejemplo:

```
<#root>

CiscoASA(config)#

ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254

CiscoASA(config)#
```

```
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

El orden en el cual usted especifica los conjuntos es muy importante porque ASA asigna direcciones de estos conjuntos en el orden en el cual los conjuntos aparecen en este comando.

La configurción address-pools en el comando group-policy address-pools command siempre invalida la configuración de grupo local en el comando tunnel-group address-pool.

Problemas con el Tiempo de Espera para el Tráfico del Cliente VPN

Cuando haya problemas de latencia en una conexión VPN, verifique estas condiciones para resolver esto:

1. Verifique si el MSS del paquete se puede reducir más.
2. Si se utiliza IPsec/tcp en lugar de IPsec/udp, configure preserve-vpn-flow .
3. Reconecte el Cisco ASA.

Los clientes VPN no pueden conectarse con ASA

Problema

Los Cisco VPN Clients no pueden autenticar cuando X-auth se utiliza con el servidor Radius.

Solución

El problema puede ser que xauth se ha desconectado. Aumente el valor del tiempo de espera para el servidor AAA a fin de resolver este problema.

Por ejemplo:

<#root>

```
Hostname(config)#
aaa-server test protocol radius
```

```
hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

Problema

Los Cisco VPN Clients no pueden autenticar cuando X-auth se utiliza con el servidor Radius.

Solución

Inicialmente, asegúrese de que la autenticación funcione correctamente. Para restringir el problema, primero verifique la autenticación con la base de datos local de ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

Si esto funciona correctamente, el problema está relacionado con la configuración del servidor Radius.

Verifique la conectividad del servidor Radius desde ASA. Si el ping funciona sin ningún problema, verifique la configuración relacionada con Radius en ASA y la configuración de la base de datos en el servidor Radius.

Puede utilizar el comando debug radius para resolver problemas relacionados con radius. Para obtener información sobre sampledebug radiusoutput, consulte thisSample Output.

Antes de utilizar el comando debug en ASA, consulte esta documentación:Mensaje de advertencia.

La conexión del cliente VPN se corta con frecuencia en el primer intento o "Security Connection terminated by peer. Reason 433." o "Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)"

Problema

Los usuarios del cliente Cisco VPN reciben este error cuando intentan la conexión con el

dispositivo VPN de cabecera.

El cliente VPN interrumpe la conexión con frecuencia en el primer intento

Conexión VPN de seguridad finalizada por el par. Reason 433.

Conexión VPN segura finalizada por el Peer Reason 433: (Motivo no especificado por el Peer)

Se intentó asignar una dirección IP de red o difusión, quitando (x.x.x.x) del grupo

Solución 1

El problema puede estar relacionado con la asignación del grupo de IP, ya sea a través de ASA, el servidor Radius, el servidor DHCP o a través del servidor Radius que actúa como servidor DHCP.

Utilice el comando debug crypto para verificar que la máscara de red y las direcciones IP sean correctas. Además, verificar que el conjunto no incluya la dirección de red y a la dirección de broadcast.

Los servidores de RADIUS deben poder asignar las direcciones IPapropiados a los clientes.

Solución 2

Este problema también ocurre debido al incidente de la autenticación ampliada. Usted debe marcar el servidor de AAA para resolver problemas este error.

Compruebe la contraseña de autenticación del servidor en Servidor y cliente. Volver a cargar el servidor AAA puede resolver este problema.

Solución 3

Otra solución alternativa para este problema es inhabilitar la característica de la detección de la amenaza.

En los momentos en que hay varias retransmisiones para diferentes asociaciones de seguridad (SA) incompletas, el ASA con la función de detección de amenazas habilitada piensa que se produjo un ataque de escaneo y los puertos VPN están marcados como el principal infractor.

Intentar inhabilitar la característica de la amenaza-detección como esto puede causar mucho incremento en el proceso del ASA. Utilice estos comandos para inhabilitar la detección de la amenaza:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Esto se puede utilizar como solución alternativa para verificar si este repara el verdadero problema.

Asegúrese de que deshabilitar la detección de amenazas en Cisco ASA realmente comprometa varias funciones de seguridad como la mitigación de los Intentos de escaneo, DoS con SPI no válido, paquetes que fallan en la Inspección de la aplicación y Sesiones incompletas.

Solución 4

Este problema también ocurre cuando un conjunto de la transformación no se configura correctamente. Una configuración adecuada del conjunto de la transformación resuelve el problema.

El acceso remoto y los usuarios del EZVPN conectan con el VPN pero no pueden acceder a los recursos externos

Problema

Los usuarios de acceso remotos no tienen ninguna conectividad a Internet una vez que conectan con el VPN.

Los usuarios de acceso remotos no pueden acceder los recursos situados detrás de otros VPN en el mismo dispositivo.

Los usuarios de acceso remotos pueden acceder solamente la red local.

Soluciones

Intentar estas soluciones para resolver este problema:

- Incapaz de acceder los servidores en el DMZ
- Clientes de VPN incapaces de resolver los DN
- Fractura-Túnel - Incapaz de acceder Internet o las redes excluidas
- Accesso del LAN local
- Redes privadas superpuestas

Incapaz de acceder los servidores en el DMZ

Una vez que el cliente VPN se ha establecido en el túnel IPsec con el dispositivo de cabecera VPN (ASA/router Cisco IOS®), los usuarios del cliente VPN pueden acceder a los recursos de la red INTERNA (10.10.10.0/24), pero no pueden acceder a la red DMZ (10.1.1.0/24).

Diagrama

Marcar que el túnel dividido, NINGUNA configuración de NAT está agregado en el dispositivo de centro de distribuidor para acceder los recursos en la red DMZ.

Ejemplo:

Configuración de ASA:

Esta configuración muestra cómo configurar la exención de NAT para la red DMZ para habilitar a los usuarios de VPN para acceder la red DMZ:

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

Después de que usted agregue una nueva entrada para la configuración de NAT, borrar la traducción NAT.

```
Clear xlate
Clear local
```

Controle lo siguiente:

Si se ha establecido el túnel, vaya a Cisco VPN Clienty elija Status > Route Detailspara verificar que las rutas seguras se muestran para las redes DMZ e INSIDE.

Consulte ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco para conocer los pasos necesarios para agregar un nuevo túnel VPN o una VPN de acceso remoto a una configuración VPN L2L que ya existe.

Consulte ASA: Allow Split Tunneling for VPN Clients en el Ejemplo de Configuración de ASA para obtener instrucciones paso a paso sobre cómo permitir el acceso de clientes VPN a Internet mientras se tunelizan en un Cisco 5500 Series Adaptive Security Appliance (ASA).

Clientes de VPN incapaces de resolver los DN

Una vez establecido el túnel, si los clientes VPN no pueden resolver el DNS, el problema puede ser la configuración del servidor DNS en el dispositivo de cabecera (ASA).

También marcar la conectividad entre los clientes de VPN y el servidor DNS. La configuración del servidor DNS debe configurarse en la directiva de grupo y aplicarse en la directiva de grupo en los atributos generales del grupo de túnel; por ejemplo:

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a


group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com


!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.


tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

Clientes VPN incapaces de conectar los servidores internos por nombre

El cliente VPN no puede pingear los hosts o los servidores del telecontrol o de la red interna del centro distribuidor por nombre. Usted necesita habilitar la configuración del fractura-DN en el ASA para resolver este problema.

Fractura-Túnel - Incapaz de acceder Internet o las redes excluidas

El túnel dividido permite a los clientes IPSec de acceso remoto dirigir condicionalmente los paquetes sobre el túnel IPSec en forma cifrada o a una interfaz de red en forma de texto sin cifrar, descifrada, donde se enrutan a un destino final.

El túnel dividido está inhabilitado de forma predeterminada, lo que estunnelalltraffic.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

La opción excludespecified se soporta solamente para los clientes del Cisco VPN, no los clientes EzVPN.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

Consulte estos documentos para obtener ejemplos de configuración detallados de split-tunnel:

- ASA: Ejemplo de Configuración de Permitir la Tunelización Dividida para Clientes VPN en ASA
- Ejemplo de Configuración Router Permite que los Clientes VPN se Conecten a IPsec e Internet con Tunelización Dividida

Solución de horquilla

Esta característica es útil para el tráfico VPN que ingrese una interfaz pero después se rutea fuera de esa misma interfaz.

Por ejemplo, en una red VPN radial, donde el dispositivo de seguridad es el hub y las redes VPN remotas son radios, el tráfico de comunicación radio-radio debe entrar en el dispositivo de seguridad y luego salir de nuevo al otro spoke.

Utilice la configuración del mismo tráfico de seguridad para permitir que el tráfico entre y salga de la misma interfaz.

<#root>

securityappliance(config)#

same-security-traffic permit intra-interface

Accesso del LAN local

Los usuarios de acceso remotos conectan con el VPN y pueden conectar con la red local solamente.

Para ver un ejemplo de configuración más detallado, consulte ASA: Allow local LAN access for VPN clients.

Redes privadas superpuestas

Problema

Si usted no puede acceder la red interna después del establecimiento del túnel, marcar la dirección IP asignado al cliente VPN que solapa con la red interna detrás del dispositivo de centro de distribuidor.

Solución

Verifique que las direcciones IP en el conjunto que se asignarán para los clientes VPN, la red interna del dispositivo de cabecera y la red interna del cliente VPN estén en redes diferentes.

Usted puede asignar la misma red principal con diversas subredes, pero los problemas de ruteo ocurren a veces.

Para obtener más ejemplos, consulte la secciónDiagrama yEjemplodeNo se puede acceder a los servidores en DMZ.

Incapaz de conectar a más de tres usuarios del cliente de VPN

Problema

Solo tres clientes VPN pueden conectarse a ASA/; la conexión del cuarto cliente falla. Sobre el incidente, se visualiza este mensaje de error:

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

Soluciones

En la mayoría de los casos, este problema se relaciona con una configuración simultánea del login dentro de la política del grupo y del sesión-límite máximo.

Intentar estas soluciones para resolver este problema:

- Configurar los Logins Simultáneos
- Configuración del ASA con CLI
- Configurar Configurar

Configurar los Logins Simultáneos

Si la casilla de verificación Inherit en ASDM está marcada, sólo se permite el número predeterminado de inicios de sesión simultáneos para el usuario. El valor predeterminado para los inicios de sesión simultáneos es tres (3).

Para resolver este problema, aumentar el valor para los logins simultáneos.

1. Inicie ASDM y luego navegue hastaConfiguration > VPN > Group Policy.
2. Elija el grupoadecuado y haga clic en elbotónEditar.
3. Una vez en la ficha General, deshaga la casilla de verificación Heredapara Inicios de sesiónsimultáneos en Configuración de la conexión. Elija un valor apropiado en el campo.

   El valor mínimo de este campo es cero (0), lo que deshabilita el inicio de sesión y evita el acceso de los usuarios.

   Cuando inicia sesión con la misma cuenta de usuario desde un equipo diferente, la sesión actual (la conexión establecida desde otro equipo con la misma cuenta de usuario) finaliza y se establece la nueva sesión.

Este es el comportamiento predeterminado y es independiente a los logins simultáneos VPN.

Configuración del ASA con CLI

Complete estos pasos para configurar el número deseado de inicios de sesión simultáneos. En este ejemplo, se ha elegido veinte (20) como valor deseado.

<#root>

```
ciscoasa(config)#
group-policy Bryan attributes
ciscoasa(config-group-policy)#
vpn-simultaneous-logins 20
```

Para obtener más información sobre este comando, consulte Referencia de Comandos de Dispositivos de Seguridad de Cisco.

Utilice el comando vpn-sessiondb max-session-limit en el modo de configuración global para limitar las sesiones VPN a un valor inferior al permitido por el dispositivo de seguridad.

Utilice la versión de este comando para eliminar el límite de sesión. Utilice el comando para sobrescribir otra vez la configuración actual.

```
vpn-sessiondb max-session-limit {session-limit}
```

Este ejemplo muestra cómo establecer un límite máximo de la sesión de VPN de 450:

<#root>

```
hostname#
vpn-sessiondb max-session-limit 450
```

Configurar

Mensaje de error

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solución

Complete estos pasos para configurar el número deseado de logins simultáneos. Usted puede también intentar establcer los Logins simultáneos a 5 para este SA:

Elija Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultánea Logins, y cambie el número de logins a5.

Incapaz de iniciar la sesión o una aplicación y de reducir la transferencia después del establecimiento del túnel

Problema

Después del establecimiento del túnel IPsec, la aplicación o la sesión no inicia a través del túnel.

Soluciones

Utilice el comando ping para comprobar la red o buscar si se puede acceder al servidor de aplicaciones desde la red.

Puede ser un problema con el tamaño de segmento máximo (MSS) para paquetes transitorios que atraviesan un router o dispositivo /ASA, específicamente segmentos TCP con el bit SYN configurado.

Router de Cisco IOS®: cambie el valor de MSS en la interfaz externa (interfaz de extremo del túnel) del router

Funcionar con estos comandos para cambiar el valor MSS en la interfaz exterior (interfaz del extremo del túnel) del router:

<#root>

```
Router>
enable

Router#
configure terminal
Router(config)#
interface ethernet0/1

Router(config-if)#ip tcp adjust-mss 1300
Router(config-if)#
end
```

Estos mensajes muestran la salida de los debugs para TCP MSS:

<#root>

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

El MSS consigue ajustado a 1300 en el router según lo configurado.

Para obtener más información, consulte ASA y Cisco IOS®: VPN Fragmentation.

ASA: consulte la documentación de /ASA

Hay una incapacidad para acceder Internet correctamente o para reducir la transferencia a través del túnel porque da el mensaje de error de la talla del MTU y los problemas MSS.

Consulte este documento para resolver el problema:

- ASA y Cisco IOS®: fragmentación de VPN

No se puede iniciar el túnel VPN desde ASA

Problema

No puede iniciar el túnel VPN desde la interfaz ASA y, después del establecimiento del túnel, el cliente VPN/extremo remoto no puede hacer ping a la interfaz interior de ASA en el túnel VPN.

Por ejemplo, el cliente pn puede ser incapaz de iniciar una conexión SSH o HTTP a la interfaz interior de ASA sobre el túnel VPN.

Solución

La interfaz interna del túnel no se puede hacer ping desde el otro extremo del túnel a menos que el comando management-accessse configure en el modo de configuración global.

<#root>

```
ASA-02(config)#

management-access inside
```

```
ASA-02(config)#
show management-access
management-access inside
```

Este comando también ayuda con la iniciación de ssh o la conexión http a la interfaz interior de ASA a través de un túnel VPN.

Esta información es verdad para la interfaz DMZ también. Por ejemplo, si desea hacer ping a la interfaz DMZ de /ASA o iniciar un túnel desde la interfaz DMZ, se requiere el comando management-access DMZ.

<#root>

```
ASA-02(config)#
management-access DMZ
```

Si el cliente VPN no puede conectarse, asegúrese de que los puertos ESP y UDP estén abiertos.

Sin embargo, si esos puertos no están abiertos, intente conectarse en TCP 10000 con la selección de este puerto en la entrada de conexión del cliente VPN.

Haga clic con el botón derecho en Modify > transport tab > IPsec over TCP.

Incapaz de pasar el tráfico a través del túnel VPN

Problema

Usted no puede pasar el tráfico a través de un túnel VPN.

Solución

Este problema también puede ocurrir cuando se bloquean los paquetes ESP. Para resolver este problema, vuelva a configurar el túnel VPN.

Este problema puede ocurrir cuando los datos no se cifran, sino que solo se descifran a través del túnel VPN, como se muestra en este resultado:

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
```

```
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y


 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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
      #send errors: 0, #recv errors: 0
```

Para resolver este problema, verifique estas condiciones:

1. Si las listas de acceso crypto corresponden con con el sitio remoto, y ese las listas de acceso NAT 0 están correctas.
2. Si el ruteo es correcto y el tráfico llega a la interfaz exterior que pasa a través del interior. La salida de muestra muestra que el desciframiento está hecho, pero el cifrado no ocurre.
3. Si el comando sysopt permit connection-vpn se ha configurado en el ASA. Si no está configurado, configure este comando porque permite que el ASA exima el tráfico cifrado/VPN de la verificación ACL de la interfaz.

Configure el par de respaldo para el túnel VPN en el mismo mapa criptográfico

Problema

Usted quiere utilizar a los pares del backup múltiple para un solo túnel del vpn.

Solución

La configuración de múltiples peers es equivalente a la provisión de una lista de reserva. Para cada túnel, el dispositivo de seguridad intenta negociar con el primer par en la lista.

Si no responde ese par, el dispositivo de seguridad funciona su manera abajo de la lista hasta que o responda un par o no hay pares en la lista.

El ASA tiene un mapa crypto ya configurado como el peer primario. El par secundario podría ser agregado después el primario.

Este ejemplo de configuración muestra el peer primario como X.X.X.X y al backup peer como Y.Y.Y.Y:

<#root>

```
ASA(config)#
crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

Inhabilitar/túnel del reinicio VPN

Problema

Para inhabilitar temporalmente el VPN hacer un túnel y reiniciar el servicio, completan el procedimiento descrito en esta sección.

Solución

Utilice el comando crypto map interface en el modo de configuración global para eliminar un conjunto de mapas criptográficos previamente definido en una interfaz.

Utilice la enoforma de este comando para quitar el conjunto de mapas criptográficos de la interfaz.

<#root>

```
hostname(config)#
no crypto map
 map-name
interface
 interface-name
```

Este comando quita un mapa crypto configurado en cualquier interfaz de dispositivo de seguridad activo y cambia el túnel VPN IPSec a inactivo en esa interfaz.

Para reiniciar el túnel IPsec en una interfaz, usted debe asignar un conjunto de la correspondencia de criptografía a una interfaz antes que la interfaz pueda proporcionar los servicios IPSec.

<#root>

```
hostname(config)#
crypto map
 map-name
interface
 interface-name
```

Algunos túneles no cifrados

Problema

Cuando una gran cantidad de túneles se configura en el gateway de VPN, algunos túneles no pasan el tráfico. El ASA no recibe los paquetes encriptados para esos túneles.

Solución

Este problema ocurre porque el ASA no puede pasar los paquetes encriptados a través de los túneles. Las reglas de cifrado duplicados se crean en la tabla ASP.

Error:- %ASA-5-713904: Grupo = DefaultRAGroup, IP = x.x.x.x, ... versión v2 del modo de transacción no compatible.Túnel finalizado.

Problema

El mensaje**`%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... versión v2 de Transaction Mode no admitida.Tunnel`** terminatederror aparece.

Solución

El motivo del mensaje de error `Transaction Mode v2`es que ASA sólo admite IKE Mode Config V6 y no la versión antigua del modo V2.

Utilice la versión de la configuración de modo V6 IKE para resolver este error.

Error:- %ASA-6-722036: grupo de clientes del grupo de usuarios xxxx IP x.x.x.x que transmite el paquete grande 1220 (umbral 1206)

Problema

El mensaje de error**`%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)`** aparece en los registros de ASA.

¿Qué hace este registro significa y cómo esto pueden ser resueltos?

Solución

Estados de este mensaje del registro que un paquete grande fue enviado al cliente. La fuente del paquete no es consciente del MTU del cliente.

Esto puede también ser debido a la compresión de los datos incompresibles. La solución alternativa es desactivar la compresión SVC con el comando nonecommand de compresión vc, que resuelve el problema.

Mensaje de error cuando QoS se habilita en un extremo del túnel VPN

Problema

Si habilitó QoS en un extremo del túnel VPN, puede recibir este mensaje de error:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

Solución

Este mensaje se produce normalmente cuando un extremo del túnel realiza QoS. Esto sucede cuando se detecta que un paquete está fuera de servicio.

Usted puede inhabilitar QoS para parar esto pero puede ser ignorada mientras el tráfico pueda atravesar el túnel.

ADVERTENCIA: entrada de mapa criptográfico incompleta

Problema

Cuando ejecuta el comando crypto map mymap 20 ipsec-isakmpcommand, puede recibir este error:

```
ADVERTENCIA: entrada de mapa criptográfico incompleta
```

Por ejemplo:

<#root>

```
ciscoasa(config)#
```

```
crypto map mymap 20 ipsec-isakmp
```

```
WARNING: crypto map entry incomplete
```

Solución

Esta es una alerta habitual cuando define un nuevo mapa criptográfico; un recordatorio de que parámetros como la lista de acceso (dirección de coincidencia), el conjunto de transformación y la dirección de peer deben configurarse antes de que pueda funcionar.

Es también normal que la primera línea que usted teclea para definir la correspondencia de criptografía no muestra en la configuración.

Error:- %ASA-4-400024: IDS:2151 Paquete ICMP grande de a en interfaz externa

Problema

Incapaz de pasar el paquete ping grande a través del túnel del vpn. Cuando intentamos pasar paquetes ping grandes, obtenemos el error**%ASA-4-400024: IDS:2151 Paquete ICMP grande de a en la interfaz externa.**

Solución

Inhabilite las firmas 2150 y 2151 para resolver este problema.Una vez que se inhabilitan las firmas, el ping funciona bien.

Utilice estos comandos para inhabilitar las firmas:

Neutralización de la firma 2151 de la auditoría de ASA(config)#ip

Neutralización de la firma 2150 de la auditoría de ASA(config)#ip

Error:- %ASA-4-402119: IPSEC: se ha recibido un paquete de protocolo (SPI=spi, número de secuencia= número_seq) de remote_IP (nombre de usuario) a local_IP que no ha superado la comprobación de bloqueo de reproducción.

Problema

Recibí este error en los mensajes del registro del ASA:

Error:- %|ASA-4-402119: IPSEC: se ha recibido un paquete de protocolo (SPI=spi, número de secuencia= núm_seq) de remote_IP (nombre de usuario) a local_IP que no ha superado la comprobación de la reproducción.

Solución

Para resolver este error, utilice el comando crypto ipsec security-association replay window-size para variar el tamaño de la ventana.

<#root>

```
hostname(config)#
```

crypto ipsec security-association replay window-size 1024

Cisco recomienda que usted utiliza los tamaños de la ventana completos 1024 para eliminar cualquier problema de la anti-respuesta.

Mensaje de error - %ASA-4-407001: Denegar tráfico para nombre_interfaz_host:dirección_interna, límite de número de licencia excedido

Problema

Pocos hosts no pueden conectar con Internet, y este mensaje de error aparece en el syslog:

Mensaje de error - %ASA-4-407001: Denegar tráfico para nombre_interfaz_host:dirección_interna, límite de número de licencia excedido

Solución

Se recibe este mensaje de error cuando el número de usuarios excede el límite del usuario de la licencia usada. Este error se puede resolver actualizando la licencia a un número mayor de usuarios.

La licencia de usuario puede incluir 50, 100, o a los usuarios ilimitados como sea necesario.

Mensaje de error - %VPN_HW-4-PACKET_ERROR:

Problema

El mensaje de error %VPN_HW-4-PACKET_ERROR:error indica que el paquete ESP con HMAC recibido por el router no coincide. Este error puede deberse a los siguientes problemas:

- Módulo defectuoso VPN H/W
- Paquete ESP corrupto

Solución

Para resolver este mensaje de error:

- Ignorar los mensajes de error a menos que haya interrupción del tráfico.
- Si hay interrupción del tráfico, Reemplazar el módulo.

Mensaje de error: Comando rechazado: elimine primero la conexión crypto entre VLAN XXXX y XXXX.

Problema

Este mensaje de error aparece cuando intenta agregar una VLAN permitida en el puerto trunk en un switch:`Comando rechazado: eliminar conexión crypto entre VLAN XXXX y VLAN XXXX, primero..`

El troncal PÁLIDO del borde no se puede modificar para permitir los VLAN adicionales. Es decir, no puede agregar VLAN en el troncal SPA VPN IPSEC.

Este comando se rechaza porque da como resultado una interfaz VLAN conectada crypto que pertenece a la lista de VLAN permitida, que plantea una brecha de seguridad IPSec potencial.

Observar que este comportamiento se aplica a todos los puertos troncales.

Solución

En lugar del comando `no switchport trunk allowed vlan (vlanlist)`, utilice el comando `switchport trunk allowed vlan` nonecommand o el comando"`switchport trunk allowed vlan remove (vlanlist)`".

Mensaje de error - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Paquete descartado - Opción de ampliación de ventana no válida para la sesión x.x.x.x:27331 a x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

Problema

Este error ocurre cuando usted intenta al telnet de un dispositivo en el otro extremo de un túnel VPN o cuando usted intenta a telnet del router sí mismo:

`Mensaje de error - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Paquete descartado - Opción de ampliación de ventana no válida para la sesión x.x.x.x:27331 a x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]`

Solución

La licencia de usuario puede incluir 50, 100, o a los usuarios ilimitados como sea necesario. Se añadió una función de escala de ventana para permitir una rápida transmisión de datos en redes de gran tamaño (LFN).

Estos son típicamente conexiones con mismo el ancho de banda alto, pero también Latencia alta.

Las redes con las conexiones satelitales son un ejemplo de un LFN, puesto que los links satelitales tienen siempre altos retrasos de propagación pero tienen típicamente ancho de banda alto.

Para habilitar la función de ampliación de ventana para admitir LFN, el tamaño de la ventana TCP debe ser superior a 65.535. Este mensaje de error se puede resolver si aumenta el tamaño de la ventana TCP a más de 65.535.

%ASA-5-305013: reglas NAT asimétricas coincidentes para reenvío e inversión . Poner al día por favor los flujos de este problema

Problema

Este mensaje de error aparece una vez que sube el túnel VPN:

%ASA-5-305013: reglas NAT asimétricas coincidentes para reenvío e inversión . Poner al día por favor los flujos de este problema

Solución

Para resolver este problema cuando no está en la misma interfaz que el host con NAT, utilice la dirección asignada en lugar de la dirección real para conectarse al host.

Además, habilite el comando inspectsi la aplicación incrusta la dirección IP.

%ASA-5-713068: mensaje de notificación no rutinario recibido: notify_type

Problema

Este mensaje de error aparece si el túnel VPN no puede subir:

%ASA-5-713068: mensaje de notificación no rutinario recibido: notify_type

Solución

Este mensaje ocurre debido al misconfiguration (es decir, cuando las políticas o los ACL no se configuran para ser lo mismo en los pares).

Una vez que se corresponden con las políticas y los ACL el túnel sube sin ningún problema.

%ASA-5-720012: (VPN-Secondary) Error al actualizar los datos de tiempo de ejecución de conmutación por error de IPSec en la

unidad en espera (o) %ASA-6-720012: (VPN-unit) Error al actualizar los datos de tiempo de ejecución de conmutación por error de IPsec en la unidad en espera

Problema

Uno de estos mensajes de error aparece cuando usted intenta actualizar el dispositivo de seguridad adaptante de Cisco (ASA):

%ASA-5-720012: (VPN-Secondary) Error al actualizar los datos de tiempo de ejecución de conmutación por error de IPSec en la unidad en espera.

%ASA-6-720012: (unidad VPN) Error al actualizar los datos de tiempo de ejecución de conmutación por error de IPsec en la unidad en espera.

Solución

Estos mensajes de error son errores informativos. Los mensajes no afectan las funciones del ASA o del VPN.

Estos mensajes aparecen cuando el subsistema de conmutación por error de VPN no puede actualizar los datos de tiempo de ejecución relacionados con IPsec porque el túnel IPsec relacionado se ha eliminado en la unidad en espera.

Para resolver estos problemas, ejecute el comando wr standby en la unidad activa.

Error:- %ASA-3-713063: dirección de par IKE no configurada para destino 0.0.0.0

Problema

Aparece el mensaje de error **%ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0** y el túnel no puede activarse.

Solución

Este mensaje aparece cuando no configuran a la dirección de peer IKE para un túnel L2L.

Este error se puede resolver si cambia el número de secuencia del mapa criptográfico y, a continuación, elimina y vuelve a aplicar el mapa criptográfico.

Error: %ASA-3-752006: el Administrador de túneles no pudo enviar un mensaje KEY_ACQUIRE.

Problema

El`%ASA-3-752006: Administrador de túnel no pudo enviar un mensaje KEY_ACQUIRE.Configuración incorrecta probable del mapa criptográfico o grupo de túnel. El` mensaje de error se registra en Cisco ASA.

Solución

Este mensaje de error puede ser causado poruna configuración errónea del mapa Crypto o del grupo de túnel. Asegúrese de que ambos estén configurados correctamente. Para obtener más información sobre este mensaje de error, consulte Error 752006 .

A continuación se detallan algunas de las acciones correctivas posibles:

- Elimine el ACL Crypto (por ejemplo, asociado al mapa dinámico).
- Elimine la configuración IKEv2 no utilizada, si la hay.
- Verifique que el Crypto coincida.
- Elimine las entradas de lista de acceso duplicadas, si las hay.

Error: %ASA-4-402116: IPSEC: se recibió un paquete ESP (SPI= 0x99554D4E, número de secuencia= 0x9E) de XX.XX.XX.XX (usuario= XX.XX.XX.XX) a YY.YY.YY.YY

En una configuración de túnel VPN LAN-LAN, este error se recibe en un extremo ASA:

```
El paquete interno desencapsulado no coincide con la política negociada en la SA.

El paquete especifica su destino como 10.32.77.67, su fuente como 10.30.1, y su protocolo como icmp.

El SA especifica su proxy local como 10.32.77.67/255.255.255.255/ip/0 y su remote_proxy como 10.105.42.192/255.255.255.224/ip/0.
```

Solución

Compruebe las listas de acceso de tráfico interesante definidas en ambos extremos del túnel VPN. Ambos deben coincidir como imágenes reflejadas exactas.

No podido iniciar el instalador 64-bit VA para habilitar el adaptador virtual debido al error 0xffffffff

Problema

`Error al iniciar el instalador de VA de 64 bits para habilitar el adaptador virtual debido al error 0xffffffff`log mensaje se recibe cuando AnyConnect no puede conectarse.

Solución

Complete estos pasos para resolver este problema:

1. Vaya a System > Internet Communication Management > Internet Communication settings y asegúrese de queTurn Off Automatic Root Certificates Update esté inhabilitado.
2. Si está deshabilitada, deshabilite la parte enteraPlantilla administrativa del GPO asignado al equipo afectado y vuelva a realizar la prueba.

Consulte Desactivar la actualización automática de certificados raíz para obtener más información.

El Cisco VPN Client no trabaja con el indicador luminoso LED amarillo de la placa muestra gravedad menor de datos en Windows 7

Problema

El Cisco VPN Client no trabaja con el indicador luminoso LED amarillo de la placa muestra gravedad menor de datos en Windows 7.

Solución

El Cisco VPN Client instalado en Windows 7 no trabaja con las conexiones 3G puesto que los indicadores luminosos LED amarillo de la placa muestra gravedad menor de datos no se soportan en los clientes VPN instalados en una máquina de Windows 7.

Alerta: "Es posible que la funcionalidad VPN no funcione en absoluto"

Problema

Durante los intentos de habilitar isakmp en la interfaz exterior de ASA, se recibe este mensaje de alerta:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

En este momento, accesso al ASA a través del ssh. Se para el HTTPS y otros clientes SSL son también afectados.

Solución

Este problema es debido a los requisitos de memoria por diversos módulos tales como maderero y crypto.

Asegúrese de que no tiene el comando logging queue 0. Establece el tamaño de la cola en 8192 y la asignación de memoria aumenta.

En plataformas como ASA5505 y ASA5510, esta asignación de memoria tiende a agotar la memoria de otros módulos.

Error de Padding de IPSec

Problema

Se recibe este mensaje de error:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

Solución

El problema ocurre porque la VPN IPSec negocia sin un algoritmo hash. El hash de paquete garantiza la comprobación de integridad del canal ESP.

Por lo tanto, sin hash, los paquetes mal formados son aceptados sin ser detectados por Cisco ASA e intenta descifrar estos paquetes.

Sin embargo, debido a que estos paquetes están mal formados, el ASA encuentra fallas durante el descifrado de paquetes. Esto causa los mensajes de error de padding.

Se recomienda incluir un algoritmo de troceo en el conjunto de transformación para la VPN y asegurarse de que el enlace entre los pares tenga una malformación mínima.

El Túnel VPN se Desconecta Después de 18 Horas de Actividad

Problema

El túnel VPN se desconecta después de 18 horas de actividad, aunque el tiempo de actividad esté configurado en 24 horas.

Solución

La duración es el tiempo máximo que la SA puede utilizarse para la regeneración de claves. El valor que usted ingresa en la configuración para definir el tiempo de actividad es diferente al tiempo de reinicio de señal del SA.

Por lo tanto, es necesario negociar un nuevo SA (o par de SA en el caso de la IPSec) antes de que expire el actual.

El tiempo de reinicio debe ser siempre más pequeño que el tiempo de actividad para poder realizar nuevos intentos en caso de que el primer intento de falle.

Los no especifican cómo calcular el tiempo de reinicio. Esto se deja a la discreción de los ejecutores.

Por lo tanto, el tiempo varía según la plataforma. Algunas implementaciones pueden utilizar un factor al azar para calcular el temporizador de reinicio.

Por ejemplo, si ASA inicia el túnel, es normal que se vuelva a configurar en 64800 segundos = 75% de 86400.

Si se inicia el enrutador, el ASA puede esperar más para dar al par más tiempo de iniciar la reintroducción.

Entonces, es normal que la sesión de VPN caduque cada 18 horas para utilizar otra clave para la negociación VPN. Esto no debe causar una desconexión o problema en la VPN.

El Flujo de Tráfico no se Mantiene Después de que el Túnel LAN-LAN se Renegocie

Problema

El flujo de tráfico no se mantiene después de que el túnel LAN-LAN se renegocie.

Solución

El ASA monitorea cada conexión que pasa a través de él y mantiene una entrada en su tabla de estado de acuerdo con la función de inspección de la aplicación.

Los detalles del tráfico encriptado que pasan por la VPN se mantienen bajo la forma de base de datos de asociación de seguridad (SA). Las conexiones VPN LAN-LAN mantienen dos flujos de tráfico distintos.

Uno es el tráfico encriptado entre los gateways VPN. El otro es el flujo de tráfico entre el recurso de red detrás del gateway de VPN y el usuario final detrás del otro extremo.

Cuando la VPN se desactiva, los detalles del flujo para este SA determinado se borran.

Sin embargo, la entrada de la tabla de estado guardada por el ASA para esta conexión TCP queda desactualizada debido a la falta de actividad, que obstaculiza la descarga.

Esto significa que ASA aún conserva la conexión TCP para ese flujo particular mientras la aplicación de usuario termina.

Sin embargo, las conexiones TCP se pierden y, finalmente, se agota el tiempo de espera después de que caduque el temporizador de inactividad TCP.

Este problema se ha resuelto con la introducción de una función llamada Flujos de túnel IPSec persistentes.

Se ha integrado un comando nuevo de preservación de flujos VPN en el sistema operativo (sysopt connection preserve-vpn-flows) al Cisco ASA para retener la información de la tabla de estado durante la renegociación del túnel VPN.

Por defecto, este comando está desactivado. Para habilitar esto, Cisco ASA mantiene la información de la tabla de estado TCP cuando la VPN L2L se recupera de la interrupción y restablece el túnel.

Mensaje de Error que Indica que se ha Alcanzado el Ancho de Bando de la Funcionalidad Crypto

Problema

Este mensaje de error se recibe en el enrutador Serie 2900:

`Error: 20 de marzo 10:51:29: %CERM-4-TX_BW_LIMIT: Se alcanzó el límite máximo de ancho de banda Tx de 85000 Kbps para la funcionalidad de cifrado con la licencia del paquete de tecnología securityk9.`

Solución

Éste es un problema conocido que ocurre debido a las guías de consulta estrictas publicadas por el gobierno de los Estados Unidos.

De acuerdo con esto, la licencia securityk9 solo puede permitir un cifrado de carga útil de hasta velocidades cercanas a 90 Mbps y limitar el número de túneles cifrados/sesiones TLS al dispositivo.

Para obtener más información sobre las restricciones de exportación de criptografía, consulte Cisco ISR G2 SEC and HSEC Licensing.

En los dispositivos Cisco, la encripción de carga se deriva para que sea menor que 85 Mbps de carga unidireccional de salida o entrada del enrutador ISR G2, con un total de 170 Mbps de carga bidireccional.

Este requisito aplica para las platadormas Cisco ISR G2 1900, 2900 y 3900. Este comando ayuda

a ver estas limitaciones:

<#root>

```
Router#
```

show platform cerm-information

```
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)         85000                  85000
 Rx Bandwidth(in kbps)         85000                  85000
 Number of tunnels               225                    225
 Number of TLS sessions         1000                   1000
---Output truncated----
```

Para evitar este problema, compre una licencia HSECK9. La licencia de función HSECK9 incorpora las funciones aumentadas de encripción de carga útil con recuentos de túnel mayores y sesiones de voz seguras.

Para obtener más información sobre las licencias del router ISR de Cisco, consulte Activación de software.

Problema: el tráfico de cifrado saliente en un túnel IPsec falla, incluso si el tráfico de descifrado entrante funciona.

Solución

Este problema se ha observado en conexiones IPSec después de reinicios múltiples, pero la causa no está clara.

La presencia de este problema se puede establecer si verifica la salida del comando show asp dropcommand y verifica que el contador de contexto VPN caducado aumente para cada paquete saliente enviado.

Miscelánea

AG_INIT_EXCH el mensaje aparece en “isakmp crypto sa de la demostración” y la “salida de los comandos debug "

Si el túnel no se inicia, **el mensaje AG_INIT**_EXCHaparece en la salida del comando show crypto isakmp e indebugoutput también.

La razón puede ser debido a una discordancia de las políticas isakmp o si el puerto udp 500 se bloquea en el camino.

El mensaje del debug “recibió un mensaje IPC durante el estado inválido” aparece

Este mensaje es un mensaje de información y no tiene nada hacer con la desconexión del túnel VPN.

Información Relacionada

- ASA y Cisco IOS®: fragmentación de VPN
- Cisco ASA 5500 Series Security Appliances
- Negociación IPSec/Protocolos IKE
- 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).

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).