La mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones

Contenido

Introducción

Este documento contiene la mayoría de las soluciones comunes a los problemas de VPN IPSec. Estas soluciones derivan directamente de solicitudes de servicio que el Soporte Técnico de Cisco ha solucionado. Muchas de estas soluciones se pueden implementar antes del troubleshooting detallado de una conexión de VPN IPSec. Como consecuencia, este documento proporciona una lista de verificación de los procedimientos comunes que se pueden probar antes de que usted comience a resolver problemas con una conexión y llame al Soporte Técnico de Cisco.

Si necesita documentos de ejemplo relacionados con la configuración de VPN de sitio a sitio y de VPN de acceso remoto, consulte las secciones *VPN de Acceso Remoto, VPN de Sitio a Sitio (L2L) con PIX, VPN de Sitio a Sitio (L2L) con IOS* y *VPN de Sitio a Sitio (L2L) con VPN3000* de Notas Técnicas y Ejemplos de Configuración.

Nota: Aunque los ejemplos de configuración que figuran en este documento son para utilizar en routers y dispositivos de seguridad, casi todos estos conceptos también son aplicables al concentrador VPN 3000.

Nota: Refiera al Troubleshooting de IP Security - Entendiendo y con los comandos debug de proporcionar los comandos debug de una explicación de común que se utilizan para resolver problemas los problemas del IPSec en el Cisco IOS ® Software y el PIX.

Nota: ASA/PIX no pasará el tráfico multicast a través de los túneles de VPN IPSec.

Nota: Puede buscar cualquier comando en este documento con la herramienta Command Lookup Tool (clientes registrados solamente).

Advertencia: Muchas de las soluciones presentadas en este documento pueden conllevar una pérdida temporaria de toda la conectividad de VPN IPSec en un dispositivo. Se recomienda que estas soluciones se implementen con precaución y de acuerdo con su política del control de cambios.

prerrequisitos

Requisitos

Cisco le recomienda que usted conozca la configuración de VPN IPSec en estos dispositivos de Cisco:

- Cisco PIX 500 Series Security Appliance
- Cisco ASA 5500 Series Security Appliance
- Routers del Cisco IOS
- Cisco VPN 3000 Series Concentrators (*opcional*)

Componentes Utilizados

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

- Cisco ASA 5500 Series Security Appliance
- Cisco PIX 500 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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

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 están enumeradas en un orden en particular, estas soluciones se pueden utilizar como una lista de verificación de elementos para comprobar o probar antes de implementar un troubleshooting detallado y llamar a TAC. Todas estas soluciones derivan directamente de las solicitudes de servicio a TAC y han servido para resolver numerosos problemas de clientes.

- 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
- Verificar que los Comandos sysopt estén Presentes (PIX/ASA solamente)
- 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 en estas secciones se redujeron 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 de VPN pase a través de los dispositivos NAT o PAT, como un router Linksys SOHO. Si NAT-T no está habilitado, en apariencia, los usuarios de Clientes de VPN frecuentemente se conectan a PIX o ASA sin un problema, pero no pueden acceder a la red interna que está detrás del dispositivo de seguridad.

Si no hablita NAT-T en el Dispositivo NAT/PAT, puede recibir el mensaje de error regular translation creation failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4 en PIX/ASA.

De manera similar, si no puede realizar el login simultáneo desde la misma dirección IP, aparece el mensaje de error Secure VPN connection terminated locally by client. `Reason 412: The remote peer is no longer responding.` el mensaje de error aparece. Habilite NAT-T en el dispositivo de VPN headend para resolver este error.

Nota: Con Cisco IOS Software Release 12.2(13)T y las versiones posteriores, NAT-T está habilitado de forma predeterminada en el Cisco IOS.

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

PIX/ASA 7.1 y versiones anteriores

```
pix(config)#isakmp nat-traversal 20
```

PIX/ASA 7.2(1) y versiones posteriores

```
securityappliance(config)#crypto isakmp nat-traversal 20
```

Para que funcione, los clientes también deben ser modificados.

En Cisco VPN Client, seleccione **Connection Entries** y haga clic en **Modify**. Se abre una ventana nueva donde tiene que elegir la **pestaña Transport**. En esta pestaña, elija **Enable Transparent Tunneling** y el botón de opción **IPSec over UDP (NAT / PAT)**. Luego, haga clic en **Save** y pruebe la conexión.

Nota: Este comando es el mismo para PIX 6.x y PIX/ASA 7.x.

Nota: Es importante permitir al UDP 4500 que tenga puertos NAT-T, UDP 500 y ESP mediante la configuración de una ACL, dado que PIX/ASA actúa como dispositivo NAT. Consulte Configuración de un Túnel IPsec a través de un Firewall con NAT para obtener más información y aprender más sobre la configuración de ACL en PIX/ASA.

Concentrador VPN

Elija **Configuration > Tunneling and Security > IPSEC > NAT Transparency > Enable:** ***IPSec sobre NAT-T*** para habilitar NAT-T en el Concentrador de VPN.

Nota: NAT-T también permite que diversos clientes VPN se conecten al mismo tiempo mediante un dispositivo PAT a cualquier headend, ya sea un Concentrador, un Router o PIX.

Probar la Conectividad Correctamente

Idealmente, la conectividad VPN se prueba desde los dispositivos detrás de los dispositivos de extremo que hacen el cifrado; sin embargo, muchos usuarios prueban la conectividad VPN con el **comando ping** en los dispositivos que hacen el cifrado. Si bien el **ping** generalmente sirve para este propósito, es importante que obtenga su su ping de la interfaz correcta. Si el **ping** se obtiene incorrectamente, puede parecer que la conexión VPN ha fallado cuando en realidad funciona. Tome este escenario como 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, un **ping** debe obtenerse de la red "interior" detrás de cualquier router. Esto es así porque las ACL crypto solo están configuradas para cifrar el tráfico con esas direcciones de origen. Un **ping** que se obtiene de las interfaces con conexión a Internet de cualquier router no se cifra. Utilice las opciones extendidas del **comando ping** en el modo EXEC privilegiado para obtener un ping de la interfaz "interior" de un router:

```
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 en este diagrama han sido substituido por los dispositivos de seguridad PIX o ASA. El **ping** utilizado para probar la conectividad también se puede obtener de la interfaz interior con la palabra clave **inside**:

```
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
```

Nota: No se recomienda que apunte a la interfaz interior de un dispositivo de seguridad con su **ping**. Si debe apuntar a la interfaz interior con su **ping**, debe habilitar **management-access** en esa interfaz o la aplicación no responderá.

```
securityappliance(config)#management-access inside
```

Nota: Cuando existe un problema con la conectividad, incluso la fase 1 de VPN no aparece. En ASA, si la conectividad falla, la salida SA es similar a este ejemplo, lo que posiblemente indica una configuración de peer crypto incorrecta o una configuración de la propuesta ISAKMP incorrecta:

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG2
```

Nota: El estado podría ser de MM_WAIT_MSG2 a MM_WAIT_MSG5, lo que denota la falla del intercambio del estado en cuestión en el modo principal (MM).

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

```
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 indicación alguna de que aparecerá un túnel VPN IPSec, posiblemente se deba al hecho de que ISAKMP no se ha habilitado. Asegúrese de haber habilitado ISAKMP en sus dispositivos. Utilice uno de estos comandos para habilitar ISAKMP en sus dispositivos:

- IOS de Cisco`router(config)#crypto isakmp enable`
- Cisco PIX 7.1 y versiones anterior (reemplazar **outside** por su interfaz deseada)`pix(config)#isakmp enable outside`
- PIX/ASA de Cisco 7.2(1) y versiones posterior (reemplazar **outside** por su interfaz deseada)`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/PIS obtenga PAT'd en el 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.

Nota: Asegúrese siempre de que los números de puerto UDP 500 y 4500 estén reservados para la negociación de las conexiones ISAKMP con el peer.

Nota: 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
```

Nota: 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. Habilite o inhabilite PFS en ambos peers de túnel; de lo contrario, el túnel IPsec de LAN a LAN (L2L) no se establece en el router PIX/ASA/IOS.

PIX/ASA:

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

```
hostname(config-group-policy)#pfs {enable | disable}
```

Para quitar el atributo PFS de la configuración en ejecución, 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 heredar un valor.

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

Router IOS:

Para especificar que IPsec debe solicitar a PFS cuando se solicitan nuevas Asociaciones de Seguridad para este tipo de entrada de mapa crypto, o que IPsec requiera a PFS cuando reciba solicitudes de nuevas Asociaciones de Seguridad, use el **comando set pfs** en el modo de configuración de mapa crypto. 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:

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

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

Despejar las Asociaciones de Seguridad Antiguas o Existentes (Túneles)

Si este mensaje de error ocurre en el router IOS, el problema es que la SA ha expirado o ha sido despejada. 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.

```
%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.

Nota: 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 desea despejar, los comandos aquí detallados pueden despejar todas las asociaciones de seguridad en el dispositivo. Proceda con cautela si otros túneles de VPN IPSec están en uso.

1. Vea las asociaciones de seguridad antes de despejarlas.IOS de Cisco`router#show crypto isakmp sa router#show crypto ipsec sa` **Dispositivos de Seguridad Cisco PIX/ASA**`securityappliance#show crypto isakmp sa securityappliance#show crypto ipsec sa` **Nota:** Estos comandos son los mismos para Cisco PIX 6.x y PIX/ASA 7.x.
2. Despeje las asociaciones de seguridad. Cada comando se puede ingresar como se muestra en negrita o con las opciones que aparecen con ellos.IOS de Cisco**ISAKMP (Fase I)**`router#clear crypto isakmp ? <0 - 32766> connection id of SA <cr>` **IPSec (Fase II)**`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>` **Dispositivos de Seguridad Cisco PIX/ASAISAKMP (Fase I)**`securityappliance#clear crypto isakmp sa` **IPSec (Fase II)**`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 de error **%PIX|ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision** en PIX/ASA. Para FWSM, puede recibir el mensaje de error %FWSM-5-713092: `Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision.` Configure el mismo valor en ambos peers para corregir el error.

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).

PIX/ASA

```
hostname(config)#isakmp policy 2 lifetime 14400
```

Router IOS

```
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. Reason 426:` Maximum Configured Lifetime Exceeded.

Para resolver este mensaje de error, configure el valor ***lifetime*** en *0* para configurar la duración de una asociación de seguridad IKE en infinito. La VPN estará siempre conectada y no terminará.

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

Para resolver el problema, también puede **habilitar re-xauth en la política de grupo**.

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 los keepalives de ISAKMP en el Cisco IOS con este comando:`router(config)#`**`crypto isakmp keepalive 15`**
- Utilice estos comandos para configurar los keepalives de ISAKMP en los Dispositivos de Seguridad de PIX/ASA:Cisco PIX 6.x`pix(config)#`**`isakmp keepalive 15`** Cisco PIX/ASA 7.x y versiones posteriores, para el grupo de túnel denominado **10.165.205.222**`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 PIX/ASA 7.x y versiones posteriores, para el grupo de túnel denominado **10.165.205.222**Inhabilita el procesamiento de keepalive de IKE, que está habilitado de forma predeterminada.`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.**Elija **%System Root% > Program Files > Cisco Systems >VPN Client > Profiles** en la PC Cliente que experimente el problema para inhabilitar el keepalive de IKE y, cuando corresponda, edite el **archivo PCF** para la conexión.Cambie **'ForceKeepAlives=0'** (valor predeterminado) a **'ForceKeepAlives=1'**.

Nota: 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, el hecho de que un túnel VPN IPSec no aparezca puede deberse a un simple error tipográfico. 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 ingresar una clave de nuevo para estar seguro de que es correcta; esta es una solución simple que puede ayudar a evitar el troubleshooting detallado.

In Remote Access VPN, verifique se que hayan ingresado la clave previamente compartida y el nombre de grupo válidos en Cisco VPN Client. Usted puede hacer frente a este error si la clave previamente compartida o el nombre de grupo no coinciden entre el cliente VPN y el dispositivo headend.

```
 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... may 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)
```

Usted también puede recuperar una clave previamente compartida sin realizar cambios de configuración en el dispositivo de seguridad PIX/ASA. Consulte PIX/ASA 7.x: Recuperación de la Clave Previamente Compartida.

Advertencia: Si usted quita los comandos relacionados con crypto, es probable que desactive uno o todos sus túneles VPN. Utilice estos comandos con cautela y consulte la política del control de cambios de su organización antes de seguir estos pasos.

- Utilice estos comandos para quitar y volver a ingresar la clave previamente compartida **secretkey** para el peer **10.0.0.1** o el grupo **vpngroup** en IOS:VPN de LAN a LAN de Cisco`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`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 **secretkey** para el peer **10.0.0.1** en los Dispositivos de Seguridad de PIX/ASA:Cisco PIX 6.x`pix(config)#`**`no isakmp key secretkey address 10.0.0.1`** `pix(config)#`**`isakmp key secretkey address 10.0.0.1`** Cisco PIX/ASA 7.x y versiones posteriores`securityappliance(config)#`**`tunnel-group 10.0.0.1 ipsec-attributes`** `securityappliance(config-tunnel-ipsec)#`**`no pre-shared-key`** `securityappliance(config-tunnel-ipsec)#`**`pre-shared-key secretkey`**

Clave Previamente Compartida No Coincidente

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

El mensaje **MM_WAIT_MSG_6** en el **comando show crypto isakmp sa** indica una clave previamente compartida no coincidente como se muestra en este ejemplo:

```
ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA
during rekey) Total IKE SA: 1 1 IKE Peer: 10.7.13.20 Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG_6
```

Para resolver este problema, vuelva a ingresar la clave previamente compartida en ambos dispositivos; la clave previamente compartida debe ser única y coincidente. Consulte Volver a Ingrese o Recuperar Clave Previamente Compartidas para obtener más información.

Quitar y Volver a Aplicar Mapas Crypto

Cuando usted despeja las asociaciones de seguridad y esto no resuelve un problema de VPN IPSec, quite y vuelva a aplicar el mapa crypto relevante para resolver una amplia variedad de problemas que incluye la caída intermitente del túnel VPN y la falla de algunos sitios de VPN para aparecer.

Advertencia: Si quita un mapa crypto de una interfaz, eso **definitivamente** desactiva cualquier túnel IPsec asociado con dicho mapa crypto. Siga estos pasos con cautela y considere la política del control de cambios de su organización antes proceder.

- Utilice estos comandos para quitar y reemplazar un mapa crypto en el Cisco IOS:Comience por quitar el mapa crypto de la interfaz. Utilice la forma no del **comando crypto map**.`router(config-if)#no crypto map mymap` Continúe usando la forma **no** para quitar un mapa de entire completo.`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:`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 PIX o ASA:Comience por quitar el mapa crypto de la interfaz. Utilice la forma no del **comando crypto map**.`securityappliance(config)#no crypto map mymap interface outside` Continúe usando la forma **no** para quitar los otros comandos crypto map.`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:`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`

Nota: 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.

Verificar que los Comandos sysopt estén Presentes (PIX/ASA solamente)

Los comandos sysopt connection permit-ipsec y **sysopt connection permit-vpn** permiten que los paquetes de un túnel IPsec y sus contenidos omitan 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 las versiones anteriores, el comando sysopt relevante para esta situación es **sysopt connection permit-ipsec**.

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

En PIX 6.x, esta funcionalidad **está inhabilitada** de forma predeterminada. Con PIX/ASA 7.0(1) y las versiones posteriores, estas funcionalidad **está habilitada** de forma predeterminada. Utilice estos comandos show para determinar si el **comando sysopt** relevante está habilitado en su dispositivo:

- Cisco PIX 6.x`pix# **show 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 no sysopt uauth allow-http-cache **no sysopt connection permit-ipsec** *!--- sysopt connection permit-ipsec is disabled* no sysopt connection permit-pptp no sysopt connection permit-l2tp no sysopt ipsec pl-compatible`
- Cisco PIX/ASA 7.x`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 sysopt** correcto para su dispositivo:

- Cisco PIX 6.x y PIX/ASA 7.0`pix(config)#**sysopt connection permit-ipsec**`
- Cisco PIX/ASA 7.1(1) y versiones posteriores`securityappliance(config)#**sysopt connection permit-vpn**`

Nota: Si no desea utilizar el **comando sysopt connection**, debe permitir explícitamente el tráfico requerido, que es tráfico interesante de origen a destino, por ejemplo, de LAN del dispositivo remoto a LAN del dispositivo local y "UDP port 500" para la interfaz exterior 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 radicar en PIX o en la incapacidad de su peer de 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 PIX está configurada como 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 que el ID de Fase 2 se envíe al peer, utilice el comando **isakmp identity** en el modo global configuration

```
crypto isakmp identity address
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as
authentication type
```

O

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by
connection type; IP address for !--- preshared key or cert DN for certificate authentication.
```

O

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchanging ISAKMP identity
information (default). !--- This name comprises the hostname and the domain name.
```

El túnel VPN no puede aparecer después de movea la configuración de PIX a ASA usando la herramienta de migración de configuración de PIX/ASA; en el log, aparecen estos mensajes:

```
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry found, removing! [IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match! [IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): No SPI to identify Phase 2 SA! [IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Este problema sucede debido a que, de forma predeterminada, PIX está configurado para

identificar la conexión como **hostname** donde ASA se identifica como **IP**. Para resolver este problema, utilice el **comando crypto isakmp identity** en el modo global configuration como se muestra a continuación:

```
crypto isakmp identity hostname !--- Use the fully-qualified domain name of !--- the host exchanging ISAKMP identity information (default). !--- This name comprises the hostname and the domain name.
```

Cuando recibe el mensaje de error Received an un-encrypted INVALID_COOKIE, emita el **comando crypto isakmp identity address** para resolver el problema.

Nota: El comando **isakmp identity** no se aprobó en la versión de software 7.2(1). Consulte Referencia de Comandos de Dispositivos de Seguridad de Cisco, versión 7.2 para obtener más información.

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 sin importar la configuración del tiempo de espera de inactividad y encuentra el error PEER_DELETE-IKE_DELETE_UNSPECIFIED.

Tiempo de inactividad y **tiempo de espera de la sesión de la** configuración como **ningunos** para hacer el túnel siempre **para arriba**, y para nunca caer el túnel incluso cuando use los dispositivos de tercero.

PIX/ASA 7.x y versiones posteriores

Ingrese el comando **vpn-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:

```
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:

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

Nota: Cuando tiene configurado **tunnel-all**, no necesita configurar **idle-timeout**, porque, incluso si configura VPN-idle timeout, no funcionará debido a que todo el tráfico está pasando por el túnel (dado que está configurado tunnel-all). Por lo tanto, el tráfico interesante (o incluso el tráfico generado por la PC) será interesante y no permitirá que Idle-timeout entre en acción.

Router del Cisco IOS

Utilice el **comando crypto ipsec security-association idle-time** en el modo global configuration o en el modo de configuración de mapa crypto para configurar el temporizador de inactividad de SA IPsec. De forma predeterminada, los temporizadores de inactividad de SA IPSec están inhabilitados.

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

El tiempo está en *segundos*, por lo que el temporizador de inactividad permite que un peer 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 el tráfico para cifrar; esto incluye una ACL crypto en una configuración de LAN a LAN o una ACL de tunelización dividida en una configuración de Acceso Remoto. Cuando estas ACL están configuradas incorrectamente o perdidas, el tráfico posiblemente fluya en una sola dirección a través del túnel VPN o puede ser que no sea enviado a través del túnel en absoluto.

Nota: Asegúrese de enlazar la ACL crypto con el mapa de map crypto mediante el comando crypto map match address en el modo global configuration.

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.**Nota:** En el concentrador VPN, puede ser que vea un log como este:`Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy`Para evitar este mensaje y para activar el túnel, asegúrese de que las ACL crypto no se superpongan y el mismo tráfico interesante no sea utilizado por ningún otro túnel VPN configurado.
- No utilice las ACL dos veces. Incluso si su ACL crypto y su ACL de exención de NAT especifican el mismo tráfico, utilice dos listas de acceso diferentes.
- Para la configuración de acceso remoto, no utilice access-list para el tráfico interesante con el mapa crypto dinámico. Esto puede hacer que el cliente VPN no se pueda conectar con el dispositivo headend. Si usted configuró equivocadamente la ACL crypto para VPN de acceso Remoto, puede recibir el mensaje de error %ASA-3-713042: `IKE Initiator unable to find policy:` Intf 2.**Nota:** Si se trata de un túnel de sitio a sitio VPN, asegúrese de hacer coincidir la lista de acceso con el peer. En el par, deben estar en orden inverso.Consulte Ejemplo de Configuración de Autenticación de PIX/ASA 7.x y Cisco VPN Client 4.x con Windows 2003 IAS RADIUS (en comparación con Active Directory) para ver una configuración de muestra que indique cómo configurar la conexión VPN de acceso remoto entre Cisco VPN Client y PIX/ASA.
- Asegúrese de que su dispositivo esté configurado para utilizar la ACL de exención de NAT. En un router, esto significa que debe utilizar el **comando route-map**. En PIX o ASA, esto significa que debe utilizar el comando **nat (0).** Se requiere una ACL de exención de NAT para las configuraciones tanto de LAN a LAN como de acceso remoto.Aquí, un router IOS está configurado para eximir el tráfico que se envía entre **192.168.100.0 /24** y **192.168.200.0 /24** o **192.168.1.0 /24** desde 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
```
Aquí, un PIX está configurado para eximir el tráfico que se envía entre **192.168.100.0 /24** y **192.168.200.0 /24** o **192.168.1.0 /24** desde NAT. Por ejemplo, el resto del tráfico está sujeto a la sobrecarga NAT:`access-list **noNAT** extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0 access-list **noNAT** extended permit ip 192.168.100.0 255.255.255.0 192.168.1.0 255.255.255.0 nat (inside) 0 access-list **noNAT** nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface` **Nota:** 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, etc.).**Nota:** En un entorno VoIP, donde las llamadas de voz entre las redes se están comunicando a través de VPN, las llamadas de voz no funcionan si las ACL de NAT 0 no se configuran correctamente. Antes de profundizar con el troubleshooting de VOIP, se sugiere verificar el estado de la conectividad VPN porque el problema podría ser la incorrecta configuración de las ACL de exención de NAT.**Nota:** Usted puede recibir el mensaje de error que se muestra si hay una configuración incorrecta de las ACL de exención de NAT (nat 0).`%PIX-3-305005: **No translation group** found for icmp src outside:192.168.100.41 dst inside:192.168.200.253 (type 8, code 0) %ASA-3-305005: No translation group found for udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p`**Nota: Ejemplo Incorrecto:**`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 0** para 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, un túnel de LAN a LAN se configura entre **192.168.100.0 /24** y **192.168.200.0 /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`**Nota:** Aunque no se ilustre aquí, este mismo concepto también se aplica a los Dispositivos de Seguridad PIX y ASA.En PIX/ASA, las ACL de túnel dividido para configuraciones de Acceso Remoto deben ser listas de **acceso estándar** que permitan el tráfico a la red a la cual los clientes VPN necesitan el acceso. Los routers IOS pueden utilizar ACL extendidas para el túnel dividido.**Nota:** En la lista de acceso extendida, utilice **"any"** en el origen de la ACL de tunelización dividida es similar a inhabilitar la tunelización dividida. Utilice solamente las redes de origen en la ACL extendida para la tunelización dividida.**Nota: Ejemplo Correcto:**`access-list 140 permit ip **10.1.0.0 0.0.255.255** 10.18.0.0 0.0.255.255` **Nota: Ejemplo Incorrecto:**`access-list 140 permit ip **any** 10.18.0.0 0.0.255.255` IOS de Cisco`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 PIX 6.**X**`pix(config)#**access-list 10 permit** 192.168.100.0 255.255.255.0 pix(config)#**vpngroup MYGROUP split-tunnel 10**` Cisco PIX/ASA 7.**X**`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**`

Este error ocurre en ASA 8.3 si NO NAT ACL está mal configurado o no se configura en ASA:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for udp
src outside: x.x.x.x/xxxxx dst inside: x.x.x.x/xx denied due to NAT reverse path failure
```

Para resolver este problema, verifique que la configuración sea correcta o reconfigure si las configuraciones son incorrectas.

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

Una VPN de sitio a sitio tiene que estar establecida entre HOASA y BOASA con la versión 8.3 en ambos ASA. 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 Client o la VPN de Sitio a Sitio no pueden establecer el túnel con el dispositivo de extremo remoto, verifique **que los dos peers contengan los mismos valores de parámetro de cifrado, hash, autenticación y Diffie-Hellman** y que la política de peer remoto especifique una duración menor o igual que la duración de 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, dropping
```

Generalmente, este mensaje aparece debido a las políticas ISAKMP no coincidentes o a una declaración faltante de NAT 0.

Además, aparece este mensaje:

```
Error Message    %PIX|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 se están enviando a la cola después de que se completa la Fase 1. Este mensaje de error puede aparecer por una de estas razones:

- Discordancia en la fase de cualquiera de los peers
- La ACL está evitando que los pares completen la fase 1

Este mensaje generalmente viene después del mensaje de error Removing peer from peer table failed, 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 headend debe coincidir con una de las Propuestas IKE de Cisco VPN Client.

Nota: Para Transform-set de IPsec y la política ISAKMP que se utilizan en PIX/ASA, el Cisco VPN Client 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

El ruteo es una parte fundamental de casi toda implementación de VPN IPSec. Asegúrese de que sus dispositivos de cifrado, como los Routers y los Dispositivos de Seguridad PIX o ASA, tengan la información de ruteo adecuada para enviar el tráfico a través de su túnel VPN. Por otra parte, si existen otros routers detrás de su dispositivo de gateway, asegúrese de que esos routers sepan cómo alcanzar el túnel y cuáles son las redes 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 PIX o un ASA, la configuración es similar a lo siguiente:`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:`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 PIX o un ASA, la configuración es similar a lo siguiente:
```
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 se asigna a dichos clientes VPN direcciones en el rango de **10.0.0.0 /24** cuando 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 del Cisco IOS:
```
crypto dynamic-map dynMAP 10
 set transform-set mySET
 reverse-route crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```
Dispositivo de Seguridad Cisco PIX o ASA:
```
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
```

Nota: 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 Superposicón de Redes Privadas.

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 Dispositivos de Seguridad de Cisco para obtener más información.

Nota: Para Transform-set de IPsec y la política ISAKMP que se utilizan en PIX/ASA, el Cisco VPN Client 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 crypto dinámica **debe ser** mayor que todas las otras entradas de mapa crypto estáticas. 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!
```

Nota: 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:

```
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 cisco
```

Nota: Los nombres de mapa crypto distinguen entre mayúsculas y minúsculas.

Nota: Este mensaje de error puede también ser considerado cuando la secuencia crypto dinámica del hombre no está correcta que hace al par golpear la correspondencia de criptografía incorrecta, y también por una lista de acceso crypto unida mal que defina el tráfico interesante: `%ASA-3-713042: IKE Initiator unable to find policy:`

En los escenarios donde diversos túneles VPN deben terminar en la misma interfaz, debemos crear un mapa crypto con el mismo nombre (solo se permite un mapa crypto por interfaz), pero con un número de secuencia diferente. Esto es válido para el router, PIX y ASA.

Consulte Configuración de IPsec entre PIX hub y PIX remotos con Cliente VPN y Autenticación Extendida para obtener más información y saber más sobre la configuración de PIX hub para el mismo mapa crypto con números de secuencia diferentes en la misma interfaz. En forma similar, consulte PIX/ASA 7.X: Agregar un Túnel Nuevo o un Acceso Remoto Nuevo a una VPN L2L Existentepara obtener más información y saber más sobre la configuración de mapa crypto para escenarios de VPN L2L y Acceso Remoto.

Verificar que la Dirección IP sea Correcta

Para determinar una configuración de VPN IPSec de LAN a LAN (L2L) de PIX/ASA Security Appliance 7.x, debe especificar el **<name>** del grupo de túnel como la **dirección IP de peer** remota (extremo del túnel remoto) en el comando **tunnel-group <name> type ipsec-l2l** para la creación y la administración de la base de datos de los registros de conexión específica para IPSec. La dirección IP de peer debe coincidir en los **comandos tunnel group name** y **Crypto 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 de peer no se configura correctamente, los logs pueden contener este mensaje, que puede resolverse mediante la configuración adecuada de la **Dirección IP de Peer**.

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

En la configuración de VPN IPSec de LAN a LAN (L2L) de PIX 6.x, la dirección IP de Peer (extremo del túnel remoto) debe coincidir con la **dirección de clave isakmp** y el **comando set peer** en el mapa crypto para obtener una conexión de VPN IPSec satisfactoria.

Cuando la dirección IP de peer no se ha configurado correctamente en la configuración de crypto de ASA, ASA no puede establecer el túnel VPN y se cuelga en la etapa *MM_WAIT_MSG4* solamente. Para resolver este problema, corrija la dirección IP de peer en la configuración.

Este es el resultado del **comando show crypto isakmp sa** cuando el túnel VPN se cuelga en la etapa MM_WAIT_MSG4.

```
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

```
%PIX|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.

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

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines should 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 un túnel de LAN a LAN y un túnel de VPN de Acceso Remoto se configuran en el mismo mapa de crypto, se indica el peer de LAN a LAN para obtener información XAUTH, y el túnel de LAN a LAN falla con "***CONF_XAUTH***" en la resultado del **comando show crypto isakmp sa**.

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

```
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
```

Nota: Este problema se aplica solamente al Cisco IOS y a PIX 6.x mientras que PIX/ASA 7.x no es afectado por este problema puesto que utiliza grupos de túnel.

Utilice la palabra clave **no-xauth** cuando ingrese la clave isakmp, de modo que el dispositivo no le indique al peer que requiere 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:

```
router(config)#crypto isakmp key cisco123 address 172.22.1.164 no-xauth
```

En el escenario donde PIX/ASA 7.x actúa como el servidor Easy VPN, el cliente VPN fácil no puede conectarse con headend debido al problema de Xauth. Inhabilite la autenticación de usuario en PIX/ASA para resolver el problema como se muestra:

```
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
```

Consulte 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:`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:`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.

Nota: 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 hay problemas del tiempo de espera sobre una conexión VPN, verifique el siguiente para resolver esto:

1. Verifique si el MSS del paquete se puede reducir más lejos.
2. Si el IPSec/tcp se utiliza en vez del IPSec/UDP, después coto-VPN-flujo de la configuración.
3. Recargue Cisco ASA.

Los Clientes VPN no Pueden Conectarse con ASA/PIX

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:

```
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, el problema debe estar 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.

Usted podría utilizar el **comando debug radius** para resolver problemas relacionados con el radius. Para conocer el resultado de muestra de **debug radius**, consulte este Resultado de Muestra.

Nota: Antes de que utilice el **comando debug** en ASA, consulte esta documentación: mensaje de advertencia.

La conexión de los descensos del cliente VPN con frecuencia en la primera conexión VPN de la tentativa o “de la Seguridad terminó por el par. Reason 433." o "Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)"

Problema

Es posible que los usuarios de Cisco VPN Client reciban este error cuando intentan la conexión con el dispositivo VPN headend.

“La *conexión de los descensos del cliente VPN con frecuencia en la primera tentativa*” o la “*conexión VPN de la Seguridad terminó por el par. Reason 433."* o "*Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)*" o "*Attempted to assign network or broadcast IP address, removing (x.x.x.x) from pool*"

Solución 1

El problema pudo estar con la asignación de la agrupación IP a través ASA/PIX, el servidor de RADIUS, servidor DHCP o a través del servidor de RADIUS que actuaba como servidor DHCP. Utilice el comando del **debug crypto** para verificar que el netmask y las direcciones IPestán correctos. 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. Marcar la contraseña de la autenticación de servidor en el servidor y el cliente y recargar el servidor de AAA pudieron resolver este problema.

Solución 3

Otra solución alternativa para este problema es inhabilitar la característica de la detección de la amenaza. A veces cuando hay retransmisiones múltiples para diversas asociaciones de seguridad incompletas (SA), el ASA con la característica de la amenaza-detección habilitada piensa que está ocurriendo un ataque de la exploración y los puertos VPN son marcados como el delincuente principal. 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
```

Para obtener más información sobre esta característica, consulte la detección de la amenaza.

Nota: Esto se puede utilizar como solución alternativa para verificar si este repara el verdadero problema. Asegúrese de que inhabilitar la detección de la amenaza en Cisco ASA compromete realmente varias funciones de seguridad tales como atenuación de las tentativas de la exploración, DOS con el SPID inválido, los paquetes que fallan la Inspección de la aplicación y las 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

Una vez que establecen al cliente VPN el túnel IPsec con el dispositivo de centro de distribuidor VPN (router PIX/ASA/IOS), los usuarios del cliente VPN pueden acceder los 10.10.10.0/24) recursos de la red interna (, pero no pueden acceder 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:

ASA/PIX

```
ciscoasa#show running-config !--- Split tunnel for the inside network access access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any !--- Split tunnel for the DMZ network access access-list vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0 any !--- Create a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients. ip local pool vpnclient 192.168.1.1-192.168.1.5 !--- This access list is used for a nat zero command that prevents !--- traffic which matches the access list from undergoing NAT. !--- No Nat for the DMZ network. access-list nonat-dmz permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 !--- No Nat for the Inside network. access-list nonat-in permit ip 10.10.10.0 255.255.255.0 192.168.1.0 255.255.255.0 !--- NAT 0 prevents NAT for networks specified in the ACL nonat . nat (DMZ) 0 access-list nonat-dmz nat (inside) 0 access-list nonat-in
```

Configuración de la Versión de ASA 8.3:

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
```

Verifique:

Si se ha establecido el túnel, ir al **Cisco VPN Client** y elegir los **detalles del estado > de la ruta** a marcar que las rutas aseguradas están mostradas para el DMZ y las redes internas.

Consulte PIX/ASA 7.x: Accesso del mail server en el ejemplo de la configuración de DMZ para obtener más información sobre cómo configurar el firewall PIX para el accesso a un mail server situado en la red de las zonas desmilitarizadas (DMZ).

Consulte PIX/ASA 7.x: Agregar un nuevo túnel o acceso remoto a un L2L existente VPN para proporcionar los pasos requeridos agregar un nuevo túnel VPN o un VPN de acceso remoto a una configuración VPN L2L que exista ya.

Consulte PIX/ASA 7.x: Permitir que la tunelización dividida para los clientes de VPN en el ejemplo de configuración ASA para proporcionar las Instrucciones paso a paso sobre cómo no prohibir a los clientes de VPN el accesso a Internet mientras que son tunneled en un dispositivo de seguridad adaptante de las 5500 Series del dispositivo de seguridad de Cisco (ASA).

Consulte PIX/ASA 7.x y al Cisco VPN Client 4.x con el ejemplo de la configuración de autenticación del RADIO de Windows 2003 IAS (contra el Active Directory) para obtener más información sobre cómo configurar la conexión VPN de acceso remoto entre un Cisco VPN Client (4.x para Windows) y el dispositivo de seguridad 7.x de la serie PIX 500.

Clientes de VPN incapaces de resolver los DN

Después de que se haya establecido el túnel, si los clientes de VPN no pueden resolver los DN, el problema puede ser la configuración del servidor DNS en el dispositivo de centro de distribuidor (ASA/PIX). También marcar la conectividad entre los clientes de VPN y el servidor DNS. La configuración del servidor DNS se debe configurar bajo política del grupo y aplicar bajo política del grupo en los atributos del general del túnel-grupo; por ejemplo:

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP
address(172.16.1.1) !--- and the domain name(cisco.com) in the group policy. 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 !--- using 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

La tunelización dividida deja los paquetes condicional directos de los clientes IPSec del acceso remoto sobre el túnel IPsec en la forma encriptada o los paquetes directos a una interfaz de la red en el texto claro forman, desencriptado, donde entonces se rutean a un destino final. La tunelización dividida se inhabilitade forma predeterminada, que es tráfico del tunnelall.

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

Nota: 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 por los ejemplos de la configuración detallada de la tunelización dividida:

- PIX/ASA 7.x: **Ejemplo de Configuración Cómo habilitar la Tunelización Dividida para los Clientes VPN en ASA**
- **Ejemplo de Configuración Router Permite que los Clientes VPN se Conecten a IPsec e Internet con Tunelización Dividida**
- Tunelización dividida para los clientes de VPN en el ejemplo de configuración del Concentrador VPN 3000

Hairpinning

Esta característica es útil para el tráfico VPN que ingrese una interfaz pero después se rutea fuera de esa misma interfaz. Por ejemplo, si usted tiene una red VPN del hub and spoke, donde está el eje el dispositivo de seguridad y las redes VPN alejadas son spokes, para que uno habló para comunicar con otro hablaron sobre, trafica debe salir en el dispositivo de seguridad y entonces otra vez al otro hablaron sobre.

Utilice la configuración del **trafico de seguridad igual** para permitir que el tráfico ingrese y que salga la misma interfaz.

```
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.

Por un más ejemplo de la configuración detallada, consulte PIX/ASA 7.x: Permitir el accesso del LAN local para los clientes VPN.

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

Aseegurarse siempre que las direcciones IPen el conjunto que se asignará para los clientes VPN, la red interna del dispositivo de centro de distribuidor y la red interna del cliente de VPN deben estar en diversas redes. Usted puede asignar la misma red principal con diversas subredes, pero los problemas de ruteo ocurren a veces.

Por otros ejemplos, ver el *diagrama* y el *ejemplo del* incapaz de acceder los servidores en la sección DMZ.

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

Problema

Solamente tres clientes VPN pueden conectar con ASA/PIX; la conexión para el 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
- Configurar ASA/PIX con la CLI
- Configurar el concentrador de la configuración del concentrador

Para obtener más información, consulte la sección de las políticas del grupo que configura de los procedimientos seleccionados de la configuración VPN del ASDM para las 5500 Series de Cisco ASA, versión 5.2.

Configurar los Logins Simultáneos

Si se selecciona la casilla de selección **Inherit** en ASDM, solo se permite el número predeterminado de logins simultáneos para el usuario. El valor predeterminado para los logins simultáneos es tres.

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

1. Iniciar el ASDM y después navegar a la **configuración > al VPN > a la política del grupo**.
2. Elija al **grupo** apropiado y haga clic en el **botón Edit**.
3. Una vez en la **ficha general**, deshacer la casilla de verificación de la **herencia** para los **Logins simultáneos** bajo **configuraciones de la conexión**. Elija un valor apropiado en el campo.**Nota:** El valor mínimo para este campo es 0, que inhabilita el login y previene el acceso del usuario.**Nota:** Cuando usted inicia sesión usando la misma cuenta de usuario de un diverso PC, terminan se establece a la sesión en curso (la conexión establecida de otro PC usando la misma cuenta de usuario), y la nueva sesión. Este es el comportamiento predeterminado y es independiente a los logins simultáneos VPN.

Configurar ASA/PIX con la CLI

Complete estos pasos para configurar el número deseado de logins simultáneos. En este ejemplo, 20 fueron elegidos como el valor deseado.

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

Para aprender más sobre este comando, consulte la Referencia de Comandos de Dispositivos de Seguridad de Cisco, versión 7.2.

Utilice el comando del MAX-sesión-**límite del VPN-sessiondb** en el modo global configuration para limitar a las sesiones de VPN a un valor inferior que el dispositivo de seguridad permite. No utilizar la ninguna versión de este comando para quitar 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:

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

Concentrador de la configuración

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 el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos) > Modify 10.19.187.229 > general > los Logins simultáneos**, y cambiar el número de logins a **5.**

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** de marcar la red o de encontrar si el servidor de aplicaciones es accesible de su red. Puede ser un problema con el Maximum Segment Size (MSS) para los paquetes transitorios que atraviesan un router o un dispositivo de PIX/ASA, específicamente los segmentos TCP con el conjunto de bits SYN.

Router del Cisco IOS - Cambiar el valor MSS en la interfaz exterior (interfaz del 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:

```
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:

```
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 PIX/ASA 7.x y IOS: Fragmentación VPN.

PIX/ASA 7.X - Consulte la documentación de PIX/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 estos documentos para resolver el problema:

- PIX/ASA 7.x y IOS: Fragmentación VPN
- Problema de PIX/ASA 7.0: MSS excedido - Los clientes HTTP no pueden navegar a algunos Web site

Incapaz de iniciar el túnel VPN de ASA/PIX

Problema

Usted no puede iniciar el túnel VPN ASA/PIX de la interfaz, y después del establecimiento del túnel, el cliente alejado end/VPN no puede pingear la interfaz interior ASA/PIX encendido del túnel VPN. Por ejemplo, el cliente pn puede no poder iniciar un SSH o una conexión HTTP a la interfaz interior ASA sobre el túnel VPN.

Solución

La interfaz interior de PIX no se puede pingear del otro extremo del túnel a menos que el comando del gestión-**accesso** se configure en el modo global configuration.

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

Nota: Este comando también ayuda en la iniciación de un ssh o de la conexión HTTP a la interfaz interior del ASA a través de un túnel VPN.

Nota: Esta información es verdad para la interfaz DMZ también. Por ejemplo, si usted quiere pingear la interfaz DMZ de PIX/ASA o querer iniciar un túnel de la interfaz DMZ, después se requiere el comando del gestión-**accesso DMZ**.

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

Nota: Si el cliente VPN no puede conectar, después aseegurar los puertos ESP y UDP están abierto, sin embargo si esos puertos no están abiertos entonces intentan conectar en TCP 10000 con la selección de este puerto bajo entrada de la conexión de cliente VPN. El click derecho **se modifica > ficha del transportador > IPSec sobre el TCP**. Consulte PIX/ASA 7.x para soportar el

IPSec sobre el TCP en cualquier ejemplo de la configuración del puerto para obtener más información sobre el IPSec sobre el 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 ocurre debido al problema descrito en el ID de bug de Cisco CSCtb53186 (clientes registrados solamente). Para resolver este problema, recargar el ASA. Consulte bug para obtener más información.

Este problema pudo también ocurrir cuando se bloquean los paquetes ESP. Para resolver este problema, configurando de nuevo el túnel VPN.

Este problema pudo ocurrir cuando los datos no se cifran, pero desencriptado solamente sobre el túnel VPN tal y como se muestra en de esta salida:

```
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, marcar el siguiente:

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 rutear está correcto y el tráfico golpea la interfaz exterior que pasa a través dentro. La salida de muestra muestra que el desciframiento está hecho, pero el cifrado no ocurre.
3. Si el comando de conexión-VPN del permiso del sysopt se ha configurado en el ASA. Si no configurado, configure este comando porque permite que el ASA exima el tráfico encrypted/VPN de marcar de la interfaz ACL.

Configurando al backup peer para el vpn hacer un túnel en la misma correspondencia de criptografía

Problema

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

Solución

Configurar a los peeres múltiples es equivalente a proporcionar a una lista del retraso. 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 debe tener una correspondencia de criptografía configurada ya 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:

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

Para obtener más información, consulte la sección determinada del par de la correspondencia de criptografía en la *Referencia de Comandos de Dispositivos de Seguridad de Cisco, versión 8.0*.

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 interface de la correspondencia de criptografía** en el modo global configuration de quitar un conjunto previamente definido de la correspondencia de criptografía a una interfaz. No utilizar la **ninguna** forma de este comando para quitar el conjunto de la correspondencia de criptografía de la interfaz.

```
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.

```
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. Esto es un problema conocido y el ID de bug CSCtb53186 (clientes registrados solamente) se ha clasifiado para abordar este problema. Para resolver este problema, recargar el ASA o actualizar el software a una versión en la que se repare este bug.

Error: -- %ASA-5-713904: El grupo = DefaultRAGroup, IP= x.x.x.x, cliente está utilizando una versión sin apoyo del v2 del modo de transacción. Túnel terminado.

Problema

El %ASA-5-713904: `El grupo = DefaultRAGroup, IP= 99.246.144.186, cliente está utilizando una versión sin apoyo del v2 del modo de transacción.` El mensaje de error terminado túnel aparece.

Solución

La razón del mensaje de error del v2 del modo de transacción es que el ASA soporta solamente la configuración de modo V6 IKE y no la vieja versión del modo V2. Utilice la versión de la configuración de modo V6 IKE para resolver este error.

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

Problema

El %ASA-6-722036: El IP del < xxxx > del usuario del < cliente-grupo > del grupo < x.x.x.x> que transmite el mensaje de error grande del paquete 1220 (umbral 1206) aparece en los registros del 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 apagar la compresión SVC con el comando none de la compresión svc, que resuelve el problema.

Error: Han desaprobado el comando none del autenticación-servidor-grupo

Problema

Si usted transferencia la configuración VPN de PIX/ASA que ejecuta la versión 7.0.x al otro dispositivo de seguridad que ejecuta 7.2.x, usted recibe este mensaje de error:

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
instead.
```

Solución

El autenticación-servidor-grupo del comando se soporta no más en 7.2(1) y versiones posteriores. Este comando fue desaprobado y se movió al modo de configuración del general-atributo del túnel-grupo.

Consulte la sección del isakmp ikev1-user-authentication de la referencia de comandos para obtener más información sobre este comando.

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

Problema

Si usted QoS habilitado en un extremo del túnel VPN, usted puede ser que reciba 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 checking
```

Solución

Este mensaje se causa normalmente cuando un extremo del túnel está haciendo QoS. Esto sucede cuando un paquete se detecta como estando fuera de servicio. Usted puede inhabilitar QoS para parar esto pero puede ser ignorada mientras el tráfico pueda atravesar el túnel.

ADVERTENCIA: la entrada de correspondencia de criptografía será incompleta

Problema

Cuando usted ejecuta el comando del IPSec-**ISAKMP del mymap 20 de la correspondencia de criptografía**, usted puede ser que reciba este error:

```
ADVERTENCIA: la entrada de correspondencia de criptografía será incompleta
```

Por ejemplo:

```
ciscoasa(config)#crypto map mymap 20 ipsec-isakmp WARNING: crypto map entry will be incomplete
```

Solución

Esto es una advertencia usual cuando usted define una nueva correspondencia de criptografía, un recordatorio que los parámetros tales como lista de acceso (direccionamiento del emparejamiento), transformen el conjunto y la dirección de peer debe ser configurada antes de que pueda trabajar. 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: Paquetes icmp grandes IDS:2151 en a la interfaz afuera

Problema

Incapaz de pasar el paquete ping grande a través del túnel del vpn. Cuando intentamos pasar los paquetes ping grandes conseguimos el error %ASA-4-400024: `Paquetes icmp grandes IDS:2151 en a la interfaz afuera`

Solución

Inhabilitar las firmas 2150 y 2151 para resolver este problema. Una vez que son las firmas el ping de los minusválidos trabaja muy 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: - %PIX|ASA-4-402119: IPSEC: Recibió un paquete del protocolo (SPI=spi, seq_num del number= de la secuencia) del remote_IP (nombre de usuario) al local_IP que falló marcar de la anti-respuesta.

Problema

Recibí este error en los mensajes del registro del ASA:

```
Error: - %PIX|ASA-4-402119: IPSEC: Recibió un paquete del protocolo (SPI=spi, seq_num del
number= de la secuencia) del remote_IP (nombre de usuario) al local_IP que falló marcar de la
anti-respuesta.
```

Solución

Para resolver este error, utilice el comando crypto de los ventana-tamaños de la respuesta de la seguridad-asociación del IPSec para variar los tamaños de la ventana.

`hostname(config)#`**`crypto ipsec security-association replay window-size 1024`**

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

Mensaje de Error - %PIX|ASA-4-407001: Negar el tráfico para el interface_name del host local: inside_address, límite de la licencia de número excedido

Problema

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

```
Mensaje de Error - %PIX|ASA-4-407001: Negar el tráfico para el interface_name del host local:
inside_address, límite de la licencia de número excedido
```

Solución

Se recibe este mensaje de error cuando el número de usuarios excede el límite del usuario de la licencia usada. Este error puede ser resuelto actualizando la licencia a un número más elevado de los 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: el mensaje de error indica que el paquete ESP con el HMAC recibido por el router está unido mal. Este error se pudo causar por estos 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: conexión crypto del borrar entre el VLAN y el, primero.

Problema

Este mensaje de error aparece cuando usted intenta agregar un VLAN permitido en el puerto troncal en un switch: `Comando rechazado:` conexión crypto del borrar entre el VLAN y el VLAN, primero.

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

Se rechaza este comando porque permitirlo dará lugar a una interfaz conectada crypto VLAN que pertenezca a la lista de VLAN permitida de la interfaz, que plantea una infracción del potencial seguridad IPSec. Observar que este comportamiento se aplica a todos los puertos troncales.

Solución

En vez del ningún comando vlan permitido switchport trunk (del vlanlist), utilice el switchport trunk no prohibido el comando none vlan o “el vlan permitida switchport trunk quitan (vlanlist)” el comando.

Mensaje de error - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Paquete de caída - Opción inválida de la escala de la ventana para la sesión x.x.x.x:27331 a x.x.x.x:23 respondedor [del iniciador (indicador 0,factor 0) (indicador 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 de caída - Opción inválida de la escala de la ventana para la sesión x.x.x.x:27331 a x.x.x.x:23 respondedor [del iniciador (indicador 0,factor 0) (indicador 1, factor 2)]
```

Solución

La licencia de usuario puede incluir 50, 100, o a los usuarios ilimitados como sea necesario. El escalamiento de la ventana fue agregado para permitir la transición transmisión de datos rápida en las redes gordas largas (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 el escalamiento de la ventana para soportar LFNs, los tamaños de la ventana TCP deben ser más de 65,535. Este mensaje de error puede ser resuelto aumentando los tamaños de la ventana TCP para ser más de 65,535.

%ASA-5-305013: Reglas asimétricas NAT correspondidas con para delantero y reverso. 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 asimétricas NAT correspondidas con para delantero y reverso. Poner al día por favor los flujos de este problema
```

Solución

Para resolver este problema cuando no en la misma interfaz que el host que usa NAT, utilice el direccionamiento asociado en vez de la dirección real para conectar con el host. Además, habilitar

el **comando inspect** si la aplicación embute la dirección IP.

%PIX|ASA-5-713068: No rutinarios recibida notifican el mensaje: notify_type

Problema

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

```
%PIX|ASA-5-713068: No rutinarios recibida notifican el mensaje: 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-Secundario) no podido poner al día los datos del tiempo de ejecución de failover del IPSec sobre la unidad standby (o) %ASA-6-720012: ((VPN-unidad) no podido poner al día los datos del tiempo de ejecución de failover del IPSec sobre la unidad standby

Problema

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

```
%ASA-5-720012: (VPN-Secundario) no podido poner al día los datos del tiempo de ejecución de
failover del IPSec sobre la unidad standby.

%ASA-6-720012: (VPN-unidad) no podido poner al día los datos del tiempo de ejecución de failover
del IPSec sobre la unidad standby.
```

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 failover VPN no puede poner al día los datos IPSec-relacionados del tiempo de ejecución porque el túnel IPsec correspondiente se ha borrado en la unidad standby. Para resolver éstos, ejecute el **comando standby del wr** en la unidad activa.

Dos bug se han clasifiado para dirigir este comportamiento y actualización a una versión de software del ASA donde se reparan estos bug. Consulte los ID de bug de Cisco CSCtj58420 (clientes registrados solamente) y CSCtn56517 (clientes registrados solamente) para obtener más información.

Error: -- %ASA-3-713063: Dirección de peer IKE no configurada para el destino 0.0.0.0

Problema

El %ASA-3-713063: La dirección de peer IKE no configurada para el mensaje de error de 0.0.0.0 del destino aparece y el túnel no puede subir.

Solución

Este mensaje aparece cuando no configuran a la dirección de peer IKE para un túnel L2L. Este error puede ser resuelto cambiando la numerada de secuencia de la correspondencia de criptografía, después quitando y reaplicando la correspondencia de criptografía.

Error: %ASA-3-752006: El administrador del túnel no pudo enviar un mensaje KEY_ACQUIRE.

Problema

`El %ASA-3-752006: Haga un túnel al administrador no podido para enviar un mensaje KEY_ACQUIRE. Mis configuration probable de la correspondencia de criptografía o del grupo de túnel.”` el mensaje de error se abre una sesión Cisco ASA.

Solución

Este mensaje de error se puede causar por un misconfiguration de la correspondencia de criptografía o del grupo de túnel. Asegúrese de que ambos estén configurados correctamente. Para más información sobre este mensaje de error, refiera al error 752006.

Aquí están algunas de las acciones correctivas:

- Quite el ACL crypto (por ejemplo, asociado al mapa dinámico).
- Quite la configuración relacionada inusitada IKEv2, si la hay.
- Verifique que el ACL crypto correspondiera con correctamente.
- Quite las entradas de lista de acceso duplicados, si las hay.

Error: %ASA-4-402116: IPSEC: Recibió un paquete ESP (SPI= 0x99554D4E, el number= 0x9E de la secuencia) de XX.XX.XX.XX (user= XX.XX.XX.XX) a YY.YY.YY.YY

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

```
El paquete interno decapsulated no corresponde con la directiva negociada en el SA.

El paquete especifica su destino como 10.32.77.67, su fuente como 10.105.30.1, 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

Usted necesita verificar las listas de acceso del tráfico interesante definidas en los ambos extremos del túnel VPN. Ambos deben hacer juego como imágenes espejo exactas.

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

Problema

No podido para iniciar el instalador 64-bit VA para habilitar el adaptador virtual debido al mensaje del registro del error 0xffffffff se recibe cuando AnyConnect no puede conectar.

Solución

Complete estos pasos para resolver este problema:

1. Ir a las **configuraciones de la comunicación de la gestión > de Internet de comunicación del sistema > de Internet** y asegúrese de que **apagar los certificados raíz automáticos que** se inhabilita la **actualización**.
2. Si se inhabilita, después inhabilitar la parte de **administrativa** entera del **modelo el** GPO asignado a la máquina y a la prueba afectadas otra vez.

Referirse apagan la actualización automática de los certificados raíz para obtener más información.

Error 5: Ningún nombre de la computadora principal existe para esto Entrada de conexión. Incapaz de hacer la conexión VPN.

Problema

El error 5: `Ningún nombre de la computadora principal existe para esto Entrada de conexión.` Incapaz de hacer el mensaje de error de la conexión VPN se recibe durante una nueva instalación PC.

Solución

Este problema se debe al ID de bug de Cisco CSCso94244 (clientes registrados solamente). Consulte este bug 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.

Mensaje de advertencia: "La “funcionalidad VPN puede no trabajar en absoluto”

Problema

Al intentar habilitar el isakmp en la interfaz exterior del ASA, se recibe este mensaje de advertencia:

```
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. Aseegurarle no tienen el **comando 0 de registración de la cola**. Hace que los tamaños de la cola configuran a 8192 y a los inicios de la asignación de memoria.

En las plataformas tales como ASA5505 y ASA5510, esta asignación de memoria tiende al memoria-morir de hambre otros módulos (IKE y etc.). El ID de bug de Cisco CSCtb58989 (clientes registrados solamente) se ha registrado para dirigirse a un tipo de conducta similar. Para resolver esto, configurar la cola de registración a un valor más bajo, como 512.

IPSec que completa el error

Problema

Se recibe este mensaje de error:

```
%PIX|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 el IPSec VPN negocia sin un algoritmo de troceo. El picado del paquete asegura la verificación de la integridad para el canal ESP. Por lo tanto, sin desmenuzar,

los paquetes malos formados son validados desapercibidos por Cisco ASA e intenta desencriptar estos paquetes. Sin embargo, porque estos paquetes son malformados, el ASA encuentra los defectos mientras que desencripta el paquete. Esto causa los mensajes de error del relleno se consideran que.

La recomendación es incluir un algoritmo de troceo en el conjunto de la transformación para el VPN y asegurarse de que el link entre los pares tiene malformación mínima del paquete.

Tiempo de retraso de la interrupción en la comunicación en los teléfonos del sitio remoto

Problema

El tiempo de retraso de la interrupción en la comunicación se experimenta en los teléfonos del sitio remoto. ¿Cómo se resuelve esto?

Solución

Inhabilite examen flaco y del sorbo para resolver este problema:

```
asa(config)# no inspect sip asa(config)# no inspect skinny
```

El túnel VPN consigue disconnected después de cada 18 horas

Problema

El túnel VPN consigue disconnected después de cada 18 horas aunque el curso de la vida se fija por 24 horas.

Solución

El curso de la vida es el tiempo máximo que el SA se puede utilizar para reintroducir. El valor que usted ingresa en la configuración pues el curso de la vida es diferente a partir de la época de la reintroducción del SA. Por lo tanto, es necesario negociar un nuevo par SA (o SA en el caso del IPSec) antes de que expire el actual. El tiempo de la reintroducción debe siempre ser más pequeño que el curso de la vida para tener en cuenta las tentativas múltiples en caso de que las primeras reintroduzcan la tentativa falla. Los RFC no especifican cómo calcular el tiempo de la reintroducción. Esto se deja a la discreción de los ejecutores. Por lo tanto, el tiempo variará dependiendo de la plataforma usada, que versión de software, etc.

Algunas implementaciones pueden utilizar un factor al azar para calcular el temporizador de la reintroducción. Por ejemplo, si el ASA inicia el túnel, después es normal que reintroducirá en 64800 segundos el = 75% de 86400. Si los iniciados del router, entonces el ASA pueden esperar más de largo para dar al par más hora de iniciar la reintroducción. Así, es normal que la sesión de VPN consigue desconectó cada 18 horas para utilizar otra clave para la negociación VPN. Esto no debe causar ningún descenso o el problema VPN.

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

Problema

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

Solución

El ASA monitorea cada conexión que los pasos con él y mantengan una entrada en su tabla de estado según la característica de la Inspección de la aplicación. Los detalles del tráfico encriptado que pasan con el VPN se mantienen bajo la forma de base de datos de la asociación de seguridad (SA). Para el LAN a las conexiones VPN LAN, mantiene dos diversos flujos de tráfico. Uno es el tráfico encriptado entre los gatewayes de 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 se termina el VPN, los detalles del flujo para este SA determinado se borran. Sin embargo, la entrada de tabla del estado mantenida por el ASA para esta conexión TCP llega a ser añeja debido a ninguna actividad, que obstaculiza la descarga. Esto significa que el ASA todavía conservará la conexión TCP para ese flujo determinado mientras que la aplicación de usuario termina. Sin embargo, las conexiones TCP se convertirán en parásito y eventual descanso después de que expire el temporizador ocioso TCP.

Este problema ha sido resuelto introduciendo una característica llamada los flujos tunneled Persistent IPSec. Han integrado a un comando new, los coto-VPN-flujos de la conexión del sysopt, en Cisco ASA para conservar la información de la tabla de estado en la renegociación del túnel VPN. Por abandono, se inhabilita este comando. Habilitando esto, Cisco ASA mantendrá la información de la tabla de estado TCP cuando el L2L VPN se recupera de la interrupción y restablece el túnel.

Estados del mensaje de error que el ancho de banda alcanzó para las funciones Crypto

Problema

Este mensaje de error se recibe en el 2900 Series Router:

```
Error: 20 de marzo 10:51:29: %CERM-4-TX_BW_LIMIT: Límite máximo del ancho de banda del tx de
85000 kbps alcanzados para las funciones Crypto con la licencia del paquete de la 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. Según esto, la licencia securityk9 puede permitir solamente una encripción de carga útil hasta las tarifas cerca de 90Mbps y limitar el número de sesiones cifradas tunnels/TLS al dispositivo. Para más información sobre las limitaciones de exportación crypto, refiera a Cisco ISR G2 SEC y a autorización HSEC.

En caso de los dispositivos de Cisco, se deriva para ser menos que el tráfico unidireccional 85Mbps adentro o el router de los ISR G2, con un total bidireccional de 170 Mbps. Este requisito solicita las 3900 Plataformas ISR G2 de Cisco 1900, 2900, y. Este comando le ayuda en ver estas limitaciones:

```
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----
```

Hay un bug clasifiado para dirigir este comportamiento. Refiera al Id. de bug Cisco CSCtu24534 (clientes registrados solamente) para más información.

Para evitar este problema, usted necesita comprar una licencia HSECK9. Una licencia de función del "hseck9" proporciona las funciones aumentadas de la encripción de carga útil con las cuentas crecientes del túnel VPN y asegura las sesiones de la Voz. Para más información sobre el router de Cisco ISR que autoriza, refiera a la activación de software.

Problema: El tráfico saliente del cifrado en un túnel IPsec puede fallar, incluso si el tráfico entrante del desciframiento está trabajando.

Solución

Este problema se ha observado en conexión IPSec después de que el múltiplo reintroduzca, pero la condición del activador no está clara. La presencia de este problema puede ser establecida marcando la salida del comando del **descenso de la demostración ASP** y verificandola que el contador expirado del contexto VPN aumenta para cada paquete saliente enviado. Refiera al Id. de bug Cisco CSCtd36473 (clientes registrados solamente) para más información.

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 consigue iniciado, AG_INIT_EXCH el mensaje aparece en la salida del **comando show crypto isakmp sa** y en la **salida de los debugs** también. La razón puede ser debido a las políticas isakmp que unen mal o si el UDP 500 del puerto consigue bloqueado en la manera.

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

- Problema de PIX/ASA 7.0: MSS excedido - Los clientes HTTP no pueden navegar a algunos Web site
- PIX/ASA 7.x y IOS: Fragmentación VPN
- Cisco ASA 5500 Series Security Appliances
- Dispositivos de seguridad Cisco PIX de la serie 500
- Negociación IPSec/Protocolos IKE
- Cisco VPN 3000 Series Concentrators

- Soporte Técnico y Documentación - Cisco Systems