Configuración de un túnel IPSec – Concentrador VPN 3000 de Cisco al firewall de punto de control 4.1

Contenido

Introducción

Este documento muestra cómo formar un túnel IPsec con claves previamente compartidas para unir dos redes privadas:

- Una red privada dentro del Cisco VPN 3000 Concentrator (192.168.1.x).
- Una red privada dentro del Firewall del punto de verificación 4.1 (10.32.50.x).

Se asume que fluye el tráfico por dentro del concentrador VPN y del interior el punto de verificación a Internet (representado en este documento por las redes 172.18.124.x) antes de que esta configuración comience.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- VPN 3000 Concentrator
- Software Release 2.5.2.F concentrador VPN 3000
- Escudo de protección de punto de control 4.1

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Convenciones

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

Configurar el concentrador VPN 3000

Complete estos pasos para configurar el concentrador VPN 3000.

1. Seleccione Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec (Seguridad IP) > IKE Proposals (Propuestas IKE) > Modify (Modificar) para crear una propuesta de Intercambio de claves de Internet (IKE) llamada "des-sha" con un Algoritmo de tronco seguro (SHA), Estándar de datos encripciónes (DES) y Diffie-Hellman grupo 1. Mantenga el valor de la vida útil en los 86400 segundos predeterminados.**Note**: El intervalo válido para el tiempo de vida de IKE del concentrador VPN es 60-2147483647 segundos.
2. Seleccione Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE). Seleccione "des-sha" y haga clic en Activate (Activar) para activar la propuesta IKE.
3. Seleccione Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec (LAN a LAN> Add (Agregar).Configure un túnel IPsec llamado “to_checkpoint” con el direccionamiento del punto de verificación como el par. Para la clave precompartida, ingrese la clave actual. Bajo la autenticación, el ESP/SHA/HMAC-160 selecto, y el DES-56 selecto para el cifrado. Ingrese la propuesta IKE ("des-sha" en este ejemplo) y las redes locales y remotas.
4. Seleccione Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > Security Associations (Asociaciones de seguridad) > Modify (Modificar). Verifique que la perfecta reserva hacia adelante **esté inhabilitada** y deje a Time Lifetime del IPSec en el valor por defecto **28800** segundos.**Note**: El intervalo válido para la vida útil de IPSec del concentrador VPN es 60-2147483647 segundos.
5. Guarde la configuración.

Configure el Firewall del punto de verificación 4.1

Complete estos pasos para configurar el Firewall del punto de verificación 4.1.

1. Puesto que el IKE y las vidas útiles predeterminadas de IPSec diferencian entre los vendedores, las **propiedades > el cifrado** selectos para fijar las vidas útiles del punto de control para estar de acuerdo con el concentrador VPN omite.El tiempo de vida de IKE del valor por defecto del concentrador VPN es 86400 segundos (minutos =1440).La vida útil predeterminada de IPSec del concentrador VPN es 28800 segundos.
2. Seleccione Manage (Administración) > Network Objects (Objetos de red) > New (o Edit) Nuevo (o Editar) > Network (Red) para configurar el objeto para la red interna ("cpinside") detrás del punto de control. Esto debe estar de acuerdo con la “red remota” en el concentrador VPN.
3. Seleccione **Manage > Network Objects > Edit** para editar el objeto para el punto final del gateway (punto de verificación “RTPCPVPN”) que el concentrador VPN tiene en su parámetro del par.En Location (Ubicación), seleccione Internal (Interna). En Type (Tipo), seleccione Gateway. Bajo los módulos instalados, marque el **VPN-1 y FireWall-1** y marque la **estación de administración**.
4. Seleccione **Manage > Network Objects > nuevo (o edite) > red** para configurar el objeto para (“inside_cisco”) la red externa detrás del concentrador VPN. Esto debe estar de acuerdo con la red “local” en el concentrador VPN.
5. Seleccione **Manage > Network Objects > New > Workstation** para agregar un objeto para (“cisco_endpoint”) el gateway externo del concentrador VPN. Ésta es la interfaz “pública” del concentrador VPN.En Location (Ubicación), seleccione External (Externa). En Type (Tipo), seleccione Gateway.**Note**: No seleccione la casilla de verificación VPN-1/FireWall-1
6. Seleccione Manage (Administración) > Network objects (Objetos de red) > Edit (Editar) para editar la ficha VPN del punto final del punto de control Gateway (denominado"RTPCPVPN"). En Domain (Dominio), seleccione Other (Otro) y luego, seleccione el interior de la red de Punto de control (denominado "cpinside") en la lista desplegable. Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit (Editar).
7. Cambie las propiedades IKE para la encripción de DES para estar de acuerdo con el **DES-56** y el **algoritmo de encripción** con el concentrador VPN.
8. Cambie las propiedades IKE al picado SHA1 para estar de acuerdo con el algoritmo **SHA/HMAC-160** en el concentrador VPN.Cancelar la selección del modo agresivoEl control **soporta las subredes**.**Secreto previamente compartido del** control bajo método de autentificación. Esto está de acuerdo con el modo de autenticación del concentrador VPN, las claves del preshared.
9. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con la **clave** real del **preshared del** concentrador VPN.**isakmp key key address address netmask netmask**
10. Seleccione Manage (Administración) > Network Objects (Objetos de red) > Edit (Editar) para editar la ficha VPN de "cisco_endpoint". En Domain, seleccione Other y luego, seleccione el interior de la red de Cisco (denominado "inside_cisco"). Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit (Editar).
11. Cambie la encripción de DES de las propiedades IKE para estar de acuerdo con el **DES-56, algoritmo de encripción** con el concentrador VPN.
12. Cambie las propiedades IKE al picado SHA1 para estar de acuerdo con el algoritmo

SHA/HMAC-160 en el concentrador VPN.Cambie estas configuraciones:Anule la selección del modo agresivo.El control **soporta las subredes**.**Secreto previamente compartido del** control bajo método de autentificación. Esto está de acuerdo con el modo de autenticación del concentrador VPN de claves del preshared.

13. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con la clave real del preshared del concentrador VPN.
14. En la ventana del editor de políticas, ingrese una ventana tanto con el origen como con el destino, como en "inside_cisco" y "cpinside" (bidireccional). Set Service=Any, Action=Encrypt, y Track=Long.
15. Bajo título de la acción, haga clic el verde **cifran el** icono y lo seleccionan **Edit Properties** para configurar las políticas de encripción.
16. Seleccione IKE y luego haga clic en Edit (Editar).
17. En la ventana de las propiedades IKE, cambie estas propiedades para estar de acuerdo con el IPSec del concentrador VPN transforma.En Transform (Transformar), seleccione Encryption (Encriptación) + Data Integrity (ESP) (Integridad de datos (ESP)). El Algoritmo de encripción debería ser DES, la Integridad de los datos debería ser SHA1 y la Gateway de par permitida debería ser la gateway externa Cisco (que se llama "cisco_endpoint"). Click OK.
18. Después de que usted configure el punto de verificación, la **directiva** selecta **> instala** en el menú de punto de control para hacer que los cambios tomen el efecto.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Resumen de la red

Cuando las redes internas adyacentes del múltiplo se configuran en el dominio del cifrado en el punto de verificación, el dispositivo pudo resumirlas automáticamente con respecto al tráfico interesante. Si el concentrador VPN no se configura para hacer juego, el túnel es probable fallar. Por ejemplo, si las redes internas de 10.0.0.0 /24 y de 10.0.1.0 /24 se configuran para ser incluidas en el túnel, puede ser que sean resumidas a 10.0.0.0 /23.

Depuración del concentrador de la VPN 3000

Los debugs posibles del concentrador VPN incluyen el IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. Esto está establecido en Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases).

Puede ver las depuraciones en Monitoring (Monitoreo) > Event log (Registro de evento) > Get log (Obtener registro).

Seleccione el **Monitoring (Monitoreo) > Sessions (Sesiones)** para monitorear el tráfico de túnel de

LAN a LAN.

Seleccione el **> Actions - Logout (Acciones – Cierre de sesión) de las Sesiones de LAN a LAN del Administration (Administración) > Administer sessions (Administrar sesiones)** para borrar el túnel.

Depuración del Checkpoint 4.1 Firewall

Note: Esto era una instalación del Microsoft Windows NT. Dado que el seguimiento se configuró en Long (Prolongado) en la ventana del editor de políticas, el tráfico rechazado deberá aparecer en rojo en el visor de registros. Un debug más prolijo se puede obtener con:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

y en otra ventana.

```
C:\WINNT\FW1\4.1\fwstart
```

Publique estos comandos de borrar los SA en el punto de verificación:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

¿La respuesta en `es` **sí** `usted seguro?` mensaje

Ejemplo de resultado del comando debug

Concentrador Cisco VPN 3000

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems