Profesional de la configuración: IPSec sitio a sitio VPN entre el ejemplo de configuración de dos routeres IOS

Contenido

Introducción

Este documento proporciona una configuración de muestra para el túnel IPsec del LAN a LAN (sitio a localizar) entre dos Routers del ® del Cisco IOS que usa al Cisco Configuration Professional (Cisco CP). Las rutas estáticas se utilizan para simplificar.

prerrequisitos

Requisitos

Aseegurese que usted cumple este requisito antes de que usted intente esta configuración:

- La conectividad del IP de punta a punta debe ser establecida antes de comenzar esta configuración.

Componentes Utilizados

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

- Cisco 1841 Router con el Cisco IOS Software Release 12.4(15T)
- Versión 2.5 de Cisco CP

Nota: Refiera a la configuración básica del router usando el Cisco Configuration Professional para permitir que al router configure Cisco CP.

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configuración

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

- Router una configuración de Cisco CP
- Configuración del router B Cisco CP
- Configuración CLI del router B

Router una configuración de Cisco CP

Realice estos pasos para configurar el túnel del VPN de sitio a sitio en el router del Cisco IOS:

1. Elija el > Security (Seguridad) de la **configuración** > el **VPN** > el **VPN de sitio a sitio**, y haga clic el botón de radio al lado de **crean un VPN de sitio a sitio**. Haga clic el **lanzamiento la tarea seleccionada**.
2. Elija al **Asisitente gradual** para proceder con la configuración, y haga clic **después**.
3. En la próxima ventana, proporcione la información de la conexión VPN en los espacios respectivos. Elija la interfaz del túnel VPN del menú desplegable. Aquí, se elige **FastEthernet0**. En la sección de la identidad del par, elija al **par con el IP Address estático** y proporcione la dirección IP del peer remoto. Entonces, proporcione las claves previamente compartidas (*cisco123* en este ejemplo) en la sección de la autenticación. Pasado, haga clic **después**.
4. El tecleo **agrega** para agregar las propuestas IKE que especifican el algoritmo de encripción, el algoritmo de autenticación, y el método del intercambio de claves.
5. Proporcione el método del algoritmo de encripción, del algoritmo de autenticación, y del intercambio de claves, y después haga clic la **AUTORIZACIÓN**. El algoritmo de encripción, el algoritmo de autenticación, y los valores del método del intercambio de claves deben

hacer juego con los datos que se proporcionarán en el router B.
6. Haga clic en Next (Siguiente).
7. En esta nueva ventana, se proporcionan los detalles determinados de la transformación. El conjunto de la transformación especifica el cifrado y los algoritmos de autenticación usados para proteger los datos en el VPN hacen un túnel. El tecleo **agrega** para proporcionar estos detalles. Usted puede agregar cualquier número de conjuntos Transform según las necesidades usando este método.
8. Proporcione la transformación los detalles determinados (integridad y los algoritmos de encripción), y haga clic la **AUTORIZACIÓN**.
9. Elija requerido **transforman el conjunto** que se utilizará del menú desplegable, y hacen clic **después**.
10. En la ventana siguiente, proporcione los detalles sobre el tráfico que se protegerá a través del túnel VPN. Proporcione la fuente y las redes de destino del tráfico que se protegerá para proteger el tráfico entre la fuente y las redes de destino especificadas. En este ejemplo, la red de origen es *10.10.10.0* y la red de destino es *10.20.10.0*. Haga clic en Next (Siguiente).
11. Clic en Finalizar en la próxima ventana para completar la configuración en el router A.

Configuración del router B Cisco CP

Realice estos pasos para configurar el túnel del VPN de sitio a sitio en el router del Cisco IOS (router B):

1. Elija el > Security (Seguridad) de la **configuración** > el **VPN** > el **VPN de sitio a sitio**, y haga clic el botón de radio al lado de **crean un VPN de sitio a sitio**. Haga clic el **lanzamiento la tarea seleccionada**.
2. Elija al **Asisitente gradual** para proceder con la configuración, y haga clic **después**.
3. En la próxima ventana, proporcione la información de la conexión VPN en los espacios respectivos. Elija la interfaz del túnel VPN del menú desplegable. Aquí, se elige **FastEthernet0**. En la sección de la identidad del par, elija al **par con el IP Address estático** y proporcione la dirección IP del peer remoto. Entonces, proporcione las claves previamente compartidas (*cisco123* en este ejemplo) en la sección de la autenticación. Pasado, haga clic **después**.
4. El tecleo **agrega** para agregar las propuestas IKE que especifican el algoritmo de encripción, el algoritmo de autenticación, y el método del intercambio de claves.
5. Proporcione el método del algoritmo de encripción, del algoritmo de autenticación, y del intercambio de claves, y después haga clic la **AUTORIZACIÓN**. El algoritmo de encripción, el algoritmo de autenticación, y los valores del método del intercambio de claves deben hacer juego con los datos proporcionados en el router A.
6. Haga clic en Next (Siguiente).
7. En esta nueva ventana, se proporcionan los detalles determinados de la transformación. El conjunto de la transformación especifica el cifrado y los algoritmos de autenticación usados para proteger los datos en el VPN hacen un túnel. El tecleo **agrega** para proporcionar estos detalles. Usted puede agregar cualquier número de conjuntos Transform según las necesidades usando este método.
8. Proporcione la transformación los detalles determinados (integridad y los algoritmos de encripción), y haga clic la **AUTORIZACIÓN**.
9. Elija requerido **transforman el conjunto** que se utilizará del menú desplegable, y hacen clic

después.

10. En la ventana siguiente, proporcione los detalles sobre el tráfico que se protegerá a través del túnel VPN. Proporcione la fuente y las redes de destino del tráfico que se protegerá para proteger el tráfico entre la fuente y las redes de destino especificadas. En este ejemplo, la red de origen es *10.20.10.0* y la red de destino es *10.10.10.0*. Haga clic en Next (Siguiente).
11. Esta ventana muestra el resumen de la configuración del VPN de sitio a sitio. Marque la **conectividad VPN de la prueba después de configurar el** checkbox si usted quiere probar la conectividad VPN. Aquí, se marca el cuadro mientras que la Conectividad necesita ser marcada. Haga clic en Finish (Finalizar).
12. **Comienzo del** tecleo para marcar la conectividad VPN.
13. En la próxima ventana, el resultado de la prueba de la conectividad VPN se proporciona. Aquí, usted puede ver si el túnel está hacia arriba o hacia abajo. En este ejemplo de configuración, el túnel está “encima de”, tal y como se muestra en de verde.Esto completa la configuración en el routerB del Cisco IOS y muestra que el túnel está para arriba.

Configuración CLI del router B

router B

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden !--- as the default values are
chosen. crypto isakmp policy 2 authentication pre-share
!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
```

```
cisco123 address 172.16.1.1 ! ! !--- Configuration for
IPsec policies. !--- Enables the crypto transform
configuration mode, !--- where you can specify the
transform sets that are used !--- during an IPsec
negotiation. crypto ipsec transform-set Router-IPSEC
esp-des esp-sha-hmac ! !--- Indicates that IKE is used
to establish !--- the IPsec Security Association for
protecting the !--- traffic specified by this crypto map
entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description
Tunnel to172.16.1.1 !--- Sets the IP address of the
remote end. set peer 172.16.1.1 !--- Configures IPsec to
use the transform-set !--- "Router-IPSEC" defined
earlier in this configuration. set transform-set Router-
IPSEC !--- Specifies the interesting traffic to be
encrypted. match address 100 ! ! ! !--- Configures the
interface to use the !--- crypto map "SDM_CMAP_1" for
IPsec. interface FastEthernet0 ip address 172.17.1.1
255.255.255.0 duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet1 ip address
10.20.10.2 255.255.255.0 duplex auto speed auto !
interface FastEthernet2 no ip address ! interface Vlan1
ip address 10.77.241.109 255.255.255.192 ! ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2 ip route
10.77.233.0 255.255.255.0 10.77.241.65 ip route
172.16.1.0 255.255.255.0 172.17.1.2 ! ! ip nat inside
source route-map nonat interface FastEthernet0 overload
! ip http server ip http authentication local ip http
secure-server ! !--- Configure the access-lists and map
them to the Crypto map configured. access-list 100
remark SDM_ACL Category=4 access-list 100 remark IPSec
Rule access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255 ! ! ! !--- This ACL 110 identifies
the traffic flows using route map access-list 110 deny
ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255 access-list
110 permit ip 10.20.10.0 0.0.0.255 any route-map nonat
permit 10 match ip address 110 ! control-plane ! ! line
con 0 login local line aux 0 line vty 0 4 privilege
level 15 login local transport input telnet ssh ! end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- Router IOS - comandos show

Router IOS - comandos show

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.`RouterB# show crypto isakmp sa dst src state conn-id slot status 172.17.1.1 172.16.1.1 QM_IDLE 3 0 ACTIVE`
- **muestre IPSec crypto sa** — Muestra todo el SA de IPSec actual en un par.`RouterB# show crypto ipsec sa interface: FastEthernet0 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) current_peer 172.16.1.1 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68 #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0,`

```
#pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.17.1.1,
remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500 current outbound spi:
0xB7C1948E(3082917006) inbound esp sas: spi: 0x434C4A7F(1129073279) transform: esp-des esp-
sha-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map:
SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3004) IV size: 8 bytes replay
detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xB7C1948E(3082917006) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn
id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime
(k/sec): (4578719/3002) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound
ah sas: outbound pcp sas:
```

- **active del show crypto engine connections** — Conexiones actuales e información de las demostraciones sobre los paquetes encriptados y desencriptados.`RouterB#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 3 FastEthernet0 172.17.1.1 set HMAC_SHA+DES_56_CB 0 0 2001 FastEthernet0 172.17.1.1 set DES+SHA 0 59 2002 FastEthernet0 172.17.1.1 set DES+SHA 59 0`

Troubleshooting

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

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Refiera a la información importante en los comandos Debug y el Troubleshooting de IP Security: Entendiendo y con los comandos debug antes de que usted utilice los **comandos debug**.

- **IPSec 7 del debug crypto** — Visualiza los IPSec Negotiations de la fase 2.**isakmp 7 del debug crypto** — Visualiza negociaciones ISAKMP de la fase 1.
- **IPSec del debug crypto** — Visualiza los IPSec Negotiations de la fase 2.**isakmp del debug crypto** — Visualiza negociaciones ISAKMP de la fase 1.

Información Relacionada

- Guía de inicio rápido del Cisco Configuration Professional
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems