Configurando un túnel IPsec - Router Cisco al escudo de protección 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: la red privada 192.168.1.x dentro del router Cisco y la red privada 10.32.50.x dentro del Escudo de protección de punto de control.

prerrequisitos

Requisitos

Esta configuración de muestra asume que fluye el tráfico por dentro del router y del interior el punto de verificación a Internet (representado aquí por las redes 172.18.124.x) antes de que usted comience la configuración.

Componentes Utilizados

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

- Cisco 3600 Router

- Software de Cisco IOS® (C3640-JO3S56I-M), versión 12.1(5)T, SOFTWARE DE LA VERSIÓN (fc1)
- 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.

Convenciones

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

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

Este documento usa estas configuraciones.

- Configuración del router
- Configuración del escudo de protección de punto de control

Configuración del router

Configuración del Cisco 3600 Router

```
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
```

```
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1 authentication pre-share crypto isakmp
key ciscorules address 172.18.124.157 ! !--- IPsec
configuration crypto ipsec transform-set rtpset esp-des
esp-sha-hmac ! crypto map rtp 1 ipsec-isakmp set peer
172.18.124.157 set transform-set rtpset match address
115 ! call rsvp-sync cns event-service server !
controller T1 1/0 ! controller T1 1/1 ! interface
Ethernet0/0 ip address 172.18.124.35 255.255.255.240 ip
nat outside no ip mroute-cache half-duplex crypto map
rtp ! interface Ethernet0/1 ip address 192.168.1.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet1/0 no ip address shutdown duplex auto speed
auto ! ip kerberos source-interface any ip nat pool
INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240 ip nat inside source route-map nonat
pool INTERNET ip classless ip route 0.0.0.0 0.0.0.0
172.18.124.34 no ip http server ! access-list 101 deny
ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 access-
list 101 permit ip 192.168.1.0 0.0.0.255 any access-list
115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any route-
map nonat permit 10 match ip address 101 ! dial-peer cor
custom ! line con 0 transport input none line aux 0 line
vty 0 4 login ! end
```

Configuración del escudo de protección de punto de control

Complete estos pasos para configurar el escudo de protección de punto de control.

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 Cisco omite.Predeterminado de Cisco el tiempo de vida de IKE es 86400 segundos (= 1440 minutos), y puede ser modificado por estos comandos:**política isakmp crypto #curso de la vida #**El tiempo de vida de IKE configurable de Cisco es a partir de 60-86400 segundos. Predeterminado de Cisco la vida útil de IPSec es 3600 segundos, y puede ser modificada por el **comando crypto ipsec security-association lifetime seconds -**.Vida útil de Cisco IPSec configurable es a partir de 120-86400 segundos.
2. Seleccione **Manage > Network Objects > nuevo (o edite) > red** para configurar el objeto para la red interna (llamada “cpinside”) detrás del punto de verificación.Esto debe estar de acuerdo con el (segunda) red de destino en el comando de **192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 del IP del permiso de la lista de acceso 115 de** Cisco.Seleccione la ubicación inferior **interna**.
3. Seleccione **Manage > Network Objects > Edit** para editar el objeto para el punto final del punto de control RTPCPVPN (gateway) ese las puntas del router Cisco en al comando de **172.18.124.157 del par del conjunto**.Seleccione la ubicación inferior **interna**. En Type (Tipo), seleccione Gateway. Bajo los módulos instalados, seleccione la **casilla de verificación VPN-1 & Firewall-1**, y también seleccione la **casilla de verificación de estación de administración**:
4. Seleccione **Manage > Network Objects > New > Network** para configurar el objeto para la red externa (llamada “inside_cisco”) detrás del router Cisco.Esto debe estar de acuerdo con la primera) red de la fuente (en el comando de **192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 del IP del permiso de la lista de acceso 115 de** Cisco.Seleccione el **externo** bajo ubicación.

5. Seleccione **Manage > Network Objects > New > Workstation** para agregar un objeto para el gateway externo del router Cisco (llamado “cisco_endpoint”). Ésta es la interfaz de Cisco a la cual el **comando crypto map name** es aplicado.Seleccione el **externo** bajo ubicación. En Type (Tipo), seleccione Gateway.**Nota:** 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 estos comandos:**política isakmp crypto #encryption desNota:** La encripción de DES es el valor por defecto así que no es visible en la configuración de Cisco.
8. Cambie las propiedades IKE al picado SHA1 para estar de acuerdo con estos comandos:**política isakmp crypto #sha del hashNota:** El algoritmo de troceo SHA es el valor por defecto así que no es visible en la configuración de Cisco.Cambie estas configuraciones:Cancelar la selección del modo agresivoEl control **soporta las subredes**.**Secreto previamente compartido del** control bajo método de autentificación. Esto está de acuerdo con estos comandos:**política isakmp crypto #authentication pre-share**
9. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con el **comando crypto isakmp key key address address de** Cisco:
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 estos comandos:**política isakmp crypto #encryption desNota:** La encripción de DES es el valor por defecto así que no es visible en la configuración de Cisco.
12. Cambie las propiedades IKE al picado SHA1 para estar de acuerdo con estos comandos:**política isakmp crypto #sha del hashNota:** El algoritmo de troceo SHA es el valor por defecto así que no es visible en la configuración de Cisco.Cambie estas configuraciones:Cancelar la selección del modo agresivoEl control **soporta las subredes**.**Secreto previamente compartido del** control bajo método de autentificación. Esto está de acuerdo con estos comandos:**política isakmp crypto #authentication pre-share**
13. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con el comando cisco **crypto de los address address de la** *clave de la* **clave del isakmp**.
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. Haga clic el verde **cifran el** icono y lo seleccionan **Edit Properties** para configurar las políticas de encripción bajo título de la acción.
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 de Cisco transforma en el **comando crypto ipsec transform-set rtpset esp-des esp-sha-hmac**:En Transform (Transformar), seleccione Encryption (Encriptación) + Data Integrity (ESP) (Integridad de datos (ESP)). El algoritmo de encripción debe ser **DES**, integridad de los datos debe ser **SHA1**, y el gateway de peer permitido debe ser el gateway

del router externo (llamado “cisco_endpoint”). Haga clic en 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

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando 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.

- show crypto isakmp sa: Ver todas las asociaciones actuales de seguridad IKE (SAs) de un par.
- **muestre IPSec crypto sa** — Vea las configuraciones usadas por los SA actuales.

Troubleshooting

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

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **motor del debug crypto** — Mensajes del debug de las visualizaciones sobre los motores de criptografía, que realizan el cifrado y el desciframiento.
- debug crypto isakmp — Muestra mensajes acerca de eventos IKE.
- **IPSec del debug crypto** — Eventos del IPSec de las visualizaciones.
- **borre el isakmp crypto** — Borra todas las conexiones del IKE activo.
- **borre el sa crypto** — Borra todo el SA de IPSec.

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 no configuran al router 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.

Punto de control

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
```

Nota: Esto era una instalación del Microsoft Windows NT.

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

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp Crypto ISAKMP debugging is on cisco_endpoint#debug crypto
isakmp Crypto IPSEC debugging is on cisco_endpoint#debug crypto engine Crypto Engine debugging
is on cisco_endpoint# 20:54:06: IPSEC(sa_request): , (key eng. msg.) src= 172.18.124.35, dest=
172.18.124.157, src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
3600s and 4608000kb, spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1) 20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_NO_STATE 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_NO_STATE 20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0 20:54:06: ISAKMP
(0:1): found peer pre-shared key matching 172.18.124.157 20:54:06: ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy 20:54:06: ISAKMP: encryption DES-CBC 20:54:06: ISAKMP:
hash SHA 20:54:06: ISAKMP: default group 1 20:54:06: ISAKMP: auth pre-share 20:54:06: ISAKMP
(0:1): atts are acceptable. Next payload is 0 20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0 20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1):
received packet from 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1): processing KE
payload. message ID = 0 20:54:06: CryptoEngine0: generate alg parameter 20:54:06: ISAKMP (0:1):
processing NONCE payload. message ID = 0 20:54:06: ISAKMP (0:1): found peer pre-shared key
matching 172.18.124.157 20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1 20:54:06:
ISAKMP (0:1): SKEYID state generated 20:54:06: ISAKMP (1): ID payload next-payload : 8 type : 1
protocol : 17 port : 500 length : 8 20:54:06: ISAKMP (1): Total payload length: 12 20:54:06:
CryptoEngine0: generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_KEY_EXCH 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_KEY_EXCH 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0 20:54:06: ISAKMP
(0:1): processing HASH payload. message ID = 0 20:54:06: CryptoEngine0: generate hmac context
for conn id 1 20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157 20:54:06:
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267 20:54:06: CryptoEngine0:
generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I)
QM_IDLE 20:54:06: CryptoEngine0: clear dh number for conn id 1 20:54:06: ISAKMP (0:1): received
packet from 172.18.124.157 (I) QM_IDLE 20:54:06: CryptoEngine0: generate hmac context for conn
id 1 20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267 20:54:06: ISAKMP
(0:1): processing SA payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): Checking IPSec
proposal 1 20:54:06: ISAKMP: transform 1, ESP_DES 20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1 20:54:06: ISAKMP: SA life type in seconds 20:54:06: ISAKMP: SA
life duration (basic) of 3600 20:54:06: ISAKMP: SA life type in kilobytes 20:54:06: ISAKMP: SA
life duration (VPI) of 0x0 0x46 0x50 0x0 20:54:06: ISAKMP: authenticator is HMAC-SHA 20:54:06:
validate proposal 0 20:54:06: ISAKMP (0:1): atts are acceptable. 20:54:06:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src=
172.18.124.35, dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 20:54:06: validate proposal
```

request 0 20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267 20:54:06: CryptoEngine0: generate hmac context for conn id 1 20:54:06: ipsec allocate flow 0 20:54:06: ipsec allocate flow 0 20:54:06: ISAKMP (0:1): Creating IPSec SAs 20:54:06: inbound SA from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to 192.168.1.0) 20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4 20:54:06: lifetime of 3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06: outbound SA from 172.18.124.35 to 172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) 20:54:06: has spi 404516441 and conn_id 2001 and flags 4 20:54:06: lifetime of 3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE 20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason "" 20:54:06: IPSEC(key_engine): got a queue event... 20:54:06: IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157, dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4 20:54:06: IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4 20:54:06: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi= 0xA29984CA(2727969994), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000 20:54:06: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0x181C6E59(404516441), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001 cisco_endpoint#sho cry ips sa interface: Ethernet0/0 Crypto map tag: rtp, local addr. 172.18.124.35 local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0) current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14 #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 1, #recv errors 0 local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157 path mtu 1500, media mtu 1500 current outbound spi: 181C6E59 inbound esp sas: spi: 0xA29984CA(2727969994) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp --More-- sa timing: remaining key lifetime (k/sec): (4607998/3447) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x181C6E59(404516441) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp sa timing: remaining key lifetime (k/sec): (4607997/3447) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: cisco_endpoint#**show crypto isakmp sa** dst src state conn-id slot 172.18.124.157 172.18.124.35 QM_IDLE 1 0 cisco_endpoint#**exit**

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Configurar el IPSec Network Security
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico y Documentación - Cisco Systems