Configurando un túnel IPsec entre un router Cisco y una a NG de punto de control

Contenido

Introducción

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

- La red privada 172.16.15.x dentro del router.
- La red privada 192.168.10.x dentro de la última generación del punto de verificación™ (NG).

prerrequisitos

Requisitos

Los procedimientos delineados en este documento se basan en estas suposiciones.

- Se configura la política básica del punto de verificación™ NG.
- Se configuran todo el acceso, Network Address Translation (NAT), y configuraciones de la encaminamiento.
- Trafique por dentro del router y el interior el punto de verificación™ NG a Internet fluye.

Componentes Utilizados

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

- Router 1751 de Cisco
- Software de Cisco IOS® (C1700-K9O3SY7-M), versión 12.2(8)T4, SOFTWARE DE LA VERSIÓN (fc1)
- Estructura 50027 del punto de verificación™ NG

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

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Configure el VPN Router del Cisco 1751

1751 Router del Cisco VPN

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1 encr 3des hash md5 authentication pre-
share group 2 lifetime 1800 !--- IPSec configuration.
crypto isakmp key aptrules address 209.165.202.129 !
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
! crypto map aptmap 1 ipsec-isakmp set peer
209.165.202.129 set transform-set aptset match address
110 ! interface Ethernet0/0 ip address 209.165.202.226
255.255.255.224 ip nat outside half-duplex crypto map
aptmap ! interface FastEthernet0/0 ip address
172.16.15.1 255.255.255.0 ip nat inside speed auto !---
NAT configuration. ip nat inside source route-map nonat
interface Ethernet0/0 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.202.225 no ip http server ip pim
bidir-enable !--- Encryption match address access list.
access-list 110 permit ip 172.16.15.0 0.0.0.255
192.168.10.0 0.0.0.255 !--- NAT access list. access-list
```

```
120 deny ip 172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10 match ip address 120 line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 password
cisco login end
```

Configure NG de punto de control

El punto de verificación™ NG es una configuración orientada al objeto. Los objetos de red y las reglas se definen para componer la directiva que pertenece a la configuración VPN que se configurará. Esta directiva entonces está instalada usando el editor de políticas del punto de verificación™ NG para completar el lado del punto de verificación™ NG de la configuración VPN.

1. Cree la subred de la red de Cisco y la subred de la red ng del punto de verificación™ como objetos de red. Esto es se cifra qué. Para crear los objetos, seleccione **Manage > Network Objects**, después seleccione **New > Network**. Ingrese la información de red apropiada, después haga clic la **AUTORIZACIÓN**.Estos ejemplos muestran una configuración de los objetos llamados CP_Network y Cisco_Network.
2. Cree los objetos de Cisco_Router y de Checkpoint_NG como objetos de estación de trabajo. Éstos son los dispositivos VPN. Para crear los objetos, seleccione **Manage > Network Objects**, después seleccione **New > Workstation**.Observe que usted puede utilizar el objeto de estación de trabajo del punto de verificación™ NG creado durante la configuración del punto de control inicial™ NG. Seleccione las opciones para fijar el puesto de trabajo como el **gateway** y **dispositivo VPN interoperable**.Estos ejemplos muestran una configuración de los objetos llamados cocinero y Cisco_Router.
3. Configure el IKE en la lengueta VPN, después haga clic **editan**.
4. Configure la directiva de intercambio de claves, y el tecleo **edita los secretos**.
5. Fije las claves previamente compartidas que se utilizarán, después haga clic la **AUTORIZACIÓN** varias veces hasta que desaparezcan las ventanas de configuración.
6. Seleccione el **Rules (Reglas) > Add Rules (Agregar reglas) > Top (Superiores)** para configurar las reglas de encripción para la directiva.La regla en el top es la primera regla realizada antes de que cualquier otra regla que pueda desviar el cifrado. Configure la fuente y el destino para incluir el CP_Network y el Cisco_Network, como se muestra aquí. Una vez que usted ha agregado la sección de la acción del cifrar de la regla, haga clic con el botón derecho del ratón la **acción** y selecciónela **Edit Properties**.
7. Con el IKE seleccionado y resaltado, el tecleo **edita**.
8. Confirme la configuración IKE.
9. Una de las cuestiones principales con ejecutar el VPN entre los dispositivos de Cisco y otros dispositivos del IPSec es la renegociación del intercambio de claves. Asegúrese de que la configuración para el intercambio IKE en el router Cisco sea exactamente lo mismo que ésa configurada en el punto de verificación™ NG.**Nota:** El valor real de este parámetro es dependiente en su política de seguridad corporativa determinada.En este ejemplo, la configuración IKE en el router se ha fijado a 30 minutos con el **comando lifetime 1800**. El mismo valor tiene que ser fijado en el punto de verificación™ NG.Para fijar este valor en el punto de verificación™ NG, selecto **maneje el objeto de red**, después seleccione el objeto del punto de verificación™ NG y el tecleo **edita**. Entonces seleccione el **VPN**, y edite el IKE. Seleccione el **avance** y configure los parámetros de reinserción. Después de que usted configure el intercambio de claves para el objeto de red ng del punto de verificación™, realice la misma configuración de la renegociación del intercambio de claves para el objeto

de red de Cisco_Router.**Nota:** Asegúrese de que usted tenga el grupo Diffie-Hellman correcto seleccionado hacer juego eso configurada en el router.

10. La configuración de la política es completa. Salve la directiva y la **directiva** selecta **> instala** para habilitarla.La ventana de instalación visualiza las notas de progreso mientras que se compila la directiva.Cuando la ventana de instalación indica que la instalación de regulación es completa, haga clic **cerca del** final el procedimiento.

Verificación

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

Verifique al router Cisco

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto isakmp sa** : muestra todas las asociaciones de seguridad actuales IKE (SA) en un par.
- show crypto ipsec sa — Muestra la configuración actual utilizada por las SA actuales

Verifique NG de punto de control

Para ver los registros, seleccione el **Window (Ventana) > Log Viewer (Visor de registro)**.

Para ver el estado del sistema, seleccione el **Window (Ventana) > Sytem Status (Estado del sistema)**.

Troubleshooting

Router Cisco

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

Para la información adicional sobre Troubleshooting, refiera por favor al Troubleshooting de IP Security - Entendiendo y con los comandos debug.

Nota: Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

- **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.
- debug crypto ipsec — Muestra eventos de IPSec.
- **borre el isakmp crypto** — Borra todas las conexiones del IKE activo.
- **borre el sa crypto** — Borra todo el SA de IPSec.

Salida del registro acertada del debug

```
18:05:32: ISAKMP (0:0): received packet from
   209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
   but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
   against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
   with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
```

Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): processing HASH payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing SA payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): Checking IPSec proposal 1 18:05:33: ISAKMP: transform 1, ESP_3DES 18:05:33: ISAKMP: attributes in transform: 18:05:33: ISAKMP: SA life type in seconds 18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10 18:05:33: ISAKMP: authenticator is HMAC-MD5 18:05:33: ISAKMP: encaps is 1 18:05:33: ISAKMP (0:1): atts are acceptable. 18:05:33: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 18:05:33: ISAKMP (0:1): processing NONCE payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing ID payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing ID payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE 18:05:33: IPSEC(key_engine): got a queue event... 18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA from 209.165.202.226 to 209.165.202.129 for prot 3 18:05:33: ISAKMP: received ke message (2/1) 18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): Creating IPSec SAs 18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226 (proxy 192.168.10.0 to 172.16.15.0) 18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4 18:05:33: lifetime of 3600 seconds 18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129 (proxy 172.16.15.0 to 192.168.10.0) 18:05:33: has spi -2006413528 and conn_id 201 and flags C 18:05:33: lifetime of 3600 seconds 18:05:33: ISAKMP (0:1): deleting node -1335371103 error FALSE reason "quick mode done (await()" 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE** 18:05:33: IPSEC(key_engine): got a queue event... 18:05:33: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.165.202.226, remote=209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and 0kb, spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0, flags= 0x4 18:05:33: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 209.165.202.226, remote=209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and 0kb, spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0, flags= 0xC 18:05:33: IPSEC(create_sa): sa created, (sa) sa_dest= 209.165.202.226, sa_prot= 50, sa_spi= 0x800022D3(2147492563), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200 18:05:33: IPSEC(create_sa): sa created, (sa) sa_dest= 209.165.202.129, sa_prot= 50, sa_spi= 0x88688F28(2288553768), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201 18:05:34: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate of a previous packet. 18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2 18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2 node marked dead -1335371103 18:05:34: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate of a previous packet. 18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2 18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2 node marked dead -1335371103 sv1-6#**show crypto isakmp sa**

dst src state conn-id slot 209.165.202.226 209.165.202.129 QM_IDLE 1 0 sv1-6#**show crypto ipsec sa** interface: Ethernet0/0 Crypto map tag: aptmap, local addr. 209.165.202.226 local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0) current_peer: 209.165.202.129 PERMIT, flags={origin_is_acl,} **#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21 #pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24** #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 209.165.202.226, remote crypto endpt.: 209.165.202.129 path mtu 1500, media mtu 1500 current outbound spi: 88688F28 inbound esp sas: spi: 0x800022D3(2147492563) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap sa timing: remaining key lifetime (k/sec): (4607997/3559) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x88688F28(2288553768) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap sa timing: remaining key lifetime (k/sec): (4607997/3550) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: sv1-6#**show crypto engine conn act** ID Interface IP- Address State Algorithm Encrypt Decrypt 1 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 0 200 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 **24** 201 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C **21** 0

Información Relacionada

- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems