Configuración de IPSec entre tres routers mediante el uso de direcciones privadas

Contenido

Introducción

Este documento describe una configuración completamente enredada con tres Routers que utilice a las direcciones privadas. El ejemplo ilustra estas características:

- Encapsulating Security Payload (ESP) - Data Encryption Standard (DES) solamente
- Claves previamente compartidas
- Redes privadas detrás de cada router: 192.168.1.0, 192.168.2.0, y 192.168.3.0
- configuración de la política isakmp y de la correspondencia de criptografía
- Tráfico de túnel definido con los **comandos access-list y route-map**. Además del Port Address Translation (PAT), los mapa del ruta se pueden aplicar a una traducción de dirección de red estática una por (NAT) en el Software Release 12.2(4)T2 y Posterior de Cisco IOS®. Para más información refiera al NAT - Capacidad de utilizar el Route Maps con la descripción general de características de las traducciones estáticas.

Nota: La tecnología de encripción está sujeta a los controles de exportación. Es su responsabilidad conocer la ley con respecto a la exportación de tecnología de encripción. Si tiene alguna pregunta acerca del control de las exportaciones, envíe un correo electrónico a export@cisco.com.

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.

- Versión de Cisco IOS Software 12.3.(7)T.
- Routeres Cisco configurados con el IPSec.

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

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

Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

En este documento, se utilizan estas configuraciones:

- Router 1
- Router 2
- Router 3

Router 1

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
```

```
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !--
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4 authentication
pre-share !--- Pre-shared keys for different peers.
crypto isakmp key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130 ! !
!--- IPSec policies: crypto ipsec transform-set encrypt-
des esp-des ! ! crypto map combined local-address
Serial0 !--- Set the peer, transform-set and encryption
traffic for tunnel peers. crypto map combined 20 ipsec-
isakmp set peer 100.228.202.154 set transform-set
encrypt-des match address 106 crypto map combined 30
ipsec-isakmp set peer 200.154.17.130 set transform-set
encrypt-des match address 105 ! ! interface Serial0 ip
address 100.232.202.210 255.255.255.252 ip nat outside
serial restart-delay 0 !--- Apply the crypto map to the
interface. crypto map combined ! interface FastEthernet0
ip address 192.168.1.1 255.255.255.0 ip nat inside ! ip
classless ip route 0.0.0.0 0.0.0.0 100.232.202.209 no ip
http server no ip http secure-server ! !--- Define
traffic for NAT. ip nat inside source route-map nonat
interface Serial0 overload !--- Access control list
(ACL) that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255 access-list 106 permit ip
192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255 access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip 192.168.1.0 0.0.0.255 any !--- Do not
perform NAT on the IPSec traffic. route-map nonat permit
10 match ip address 150 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! ! end
```

Router 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
```

```
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.228.202.154 crypto isakmp key xxxxxx1234
address 100.232.202.210 ! ! !--- IPSec policies. crypto
ipsec transform-set encrypt-des esp-des ! ! crypto map
combined local-address Ethernet1 !--- Set the peer,
transform-set and encryption traffic for tunnel peers.
crypto map combined 7 ipsec-isakmp set peer
100.232.202.210 set transform-set encrypt-des match
address 105 crypto map combined 8 ipsec-isakmp set peer
100.228.202.154 set transform-set encrypt-des match
address 106 ! ! ! interface Ethernet0 ip address
192.168.3.1 255.255.255.0 ip nat inside ! interface
Ethernet1 ip address 200.154.17.130 255.255.255.224 ip
nat outside !--- Apply the crypto map to the interface.
crypto map combined ! ip classless ip route 0.0.0.0
0.0.0.0 200.154.17.129 no ip http server no ip http
secure-server ! !--- Define traffic for NAT. ip nat
inside source route-map nonat interface Ethernet1
overload !--- ACL shows traffic to encrypt over the
tunnel. access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 106 permit ip
192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip any any !--- Do not perform NAT on the
IPSec traffic. route-map nonat permit 10 match ip
address 150 ! ! ! control-plane ! ! line con 0 line aux
0 line vty 0 4 ! ! end
```

Configuración del router3

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
```

```
!--- Configure IKE policy and pre-shared keys for each peer. !--- IKE policy defined for peers. crypto isakmp policy 4 authentication pre-share !--- Pre-shared keys for different peers. crypto isakmp key xxxxxx1234 address 100.232.202.210 crypto isakmp key xxxxxx1234 address 200.154.17.130 ! ! !--- IPSec policies: crypto ipsec transform-set encrypt-des esp-des ! ! !--- Set the peer, transform-set and encryption traffic for tunnel peers. crypto map combined local-address Serial0 crypto map combined 7 ipsec-isakmp set peer 100.232.202.210 set transform-set encrypt-des match address 106 crypto map combined 8 ipsec-isakmp set peer 200.154.17.130 set transform-set encrypt-des match address 105 ! ! interface Serial0 ip address 100.228.202.154 255.255.255.252 ip nat outside serial restart-delay 0 !-- Apply the crypto map to the interface. crypto map combined ! interface FastEthernet0 ip address 192.168.2.1 255.255.255.0 ip nat inside ! ip classless ip route 0.0.0.0 0.0.0.0 100.228.202.153 no ip http server no ip http secure-server ! !--- Define traffic for NAT. ip nat inside source route-map nonat interface Serial0 overload !--- ACL that shows traffic to encrypt over the tunnel. access-list 105 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 access-list 106 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL to avoid the traffic through NAT over the tunnel. access-list 150 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 access-list 150 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL to perform NAT on the traffic that does not go over the tunnel. access-list 150 permit ip 192.168.2.0 0.0.0.255 any !--- Do not perform NAT on the IPSec traffic. route-map nonat permit 10 match ip address 150 ! ! ! control-plane ! ! line con 0 line aux 0 line vty 0 4 login ! ! end
```

Verificación

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

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

- show crypto engine connections active — Muestra los paquetes encripcións y desencripcións entre los pares IPSec.
- show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.
- **muestre IPSec crypto sa** — Muestra las configuraciones usadas por (IPSec) los SA actuales.

Troubleshooting

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

Comandos para resolución de problemas

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

Nota: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.

Nota: Las siguientes depuraciones se deben ejecutar en ambos routers IPSec (pares). Borrar los SA se debe hacer en ambos pares.

- debug crypto ipsec — Muestra errores durante la fase 1.
- debug crypto ipsec — Muestra errores durante la fase 2.
- debug crypto engine — Muestra información del motor de criptografía.
- **clear crypto connection connection-id [slot** | *rsm* | *vip]* — termina a una sesión encriptada actualmente en curso. Las sesiones encriptadas terminan normalmente cuando los tiempos de la sesión hacia fuera. Utilice el comando show crypto cisco connections para conocer el valor de la conexión id.
- **borre el isakmp crypto** — Borra la fase 1 SA.
- **borre el sa crypto** — Borra la fase 2 SA.

Información Relacionada

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