Configurar IPSec entre un router y un PIX usando el comando nat 0 access-list

Contenido

Introducción

Este documento ilustra una configuración de Seguridad IP (IPSec) entre un router y un Firewall del Secure PIX de Cisco. Queremos utilizar los IP Addresses internos privados al pasar el tráfico entre el LAN de las jefaturas y los LAN remotos, y traducir los host LAN a los IP Addresses routable cuando los usuarios tienen acceso a Internet. Sin embargo, los usuarios pueden también tener acceso a las páginas públicas en Internet sin su tráfico que pasa a través del túnel usando el **comando route-map**.

Refiera a ASA/PIX: Dispositivo de seguridad a un ejemplo de la configuración del router IOS túnel ipsec de LAN a LAN para aprender más sobre el decorado donde un LAN-a-LAN hace un túnel entre un router y el PIX/ASA de los dispositivos del Cisco Security.

Antes de que usted comience

Convenciones

Para más información sobre los convenios del documento, vea los convenios de los consejos técnicos de Cisco.

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

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

- Router de Cisco con el Software Release 12.0(7)T de Cisco IOS®
- Versión del Firewall de Cisco PIX 5.1(1)

La Información presentada en este documento fue creada de los dispositivos en un entorno específico del laboratorio. 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 un comando antes de ejecutarlo.

Teoría previa

En el PIX, los comandos access-list y nat 0 funcionan de manera conjunta. Cuando un usuario en la red de 10.1.1.0 va a la red de 10.2.2.0, utilizamos la lista de acceso para permitir que el tráfico de la red de 10.1.1.0 sea cifrado sin el Network Address Translation (NAT). Sin embargo, cuando van esos mismos usuarios en cualquier parte, los traducen al direccionamiento de 172.17.63.210 con la traducción de la dirección de puerto (PALMADITA). En el router, utilizan a los **comandos route-map and access-list** de permitir que el tráfico de la red de 10.2.2.0 sea cifrado sin el NAT. Sin embargo, cuando van esos mismos usuarios en cualquier parte, los traducen al direccionamiento de 172.17.63.210 con la traducción de la dirección de puerto (PALMADITA).

Los siguientes son comandos configuration requeridos en el Firewall PIX para que el tráfico no ejecutarse a través de la PALMADITA sobre el túnel, y tráfico a Internet a ejecutarse a través del patente.

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

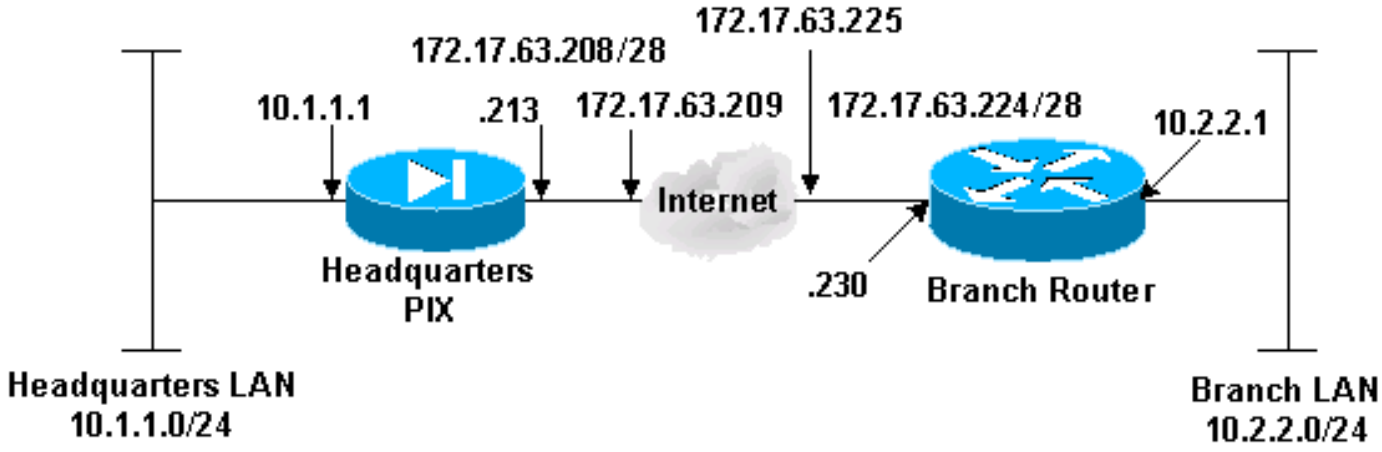
Configurar

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 herramienta Command Lookup del IOS.

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas a continuación.

Jefaturas PIX

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!--- Traffic to the router: access-list ipsec permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!--- Do not Network Address Translate (NAT) traffic to
the router: access-list nonat permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HQ_PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.17.63.213 255.255.255.240
ip address inside 10.1.1.1 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
```

```
global (outside) 1 172.17.63.210
!--- Do not NAT traffic to the router: nat (inside) 0
access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.17.63.209 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- IPSec policies: sysopt connection permit-ipsec
crypto ipsec transform-set avalanche esp-des esp-md5-
hmac
crypto ipsec security-association lifetime seconds 3600
crypto map forsberg 21 ipsec-isakmp
crypto map forsberg 21 match address ipsec
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
!--- IKE policies: isakmp enable outside
isakmp key westernfinal2000 address 172.17.63.230
netmask 255.255.255.255
isakmp identity address
isakmp policy 21 authentication pre-share
isakmp policy 21 encryption des
isakmp policy 21 hash md5
isakmp policy 21 group 1
telnet timeout 5
terminal width 80
Cryptochecksum:e36245da9428c4c07b489f787c8ccd3b
: end
```

Router de rama

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Branch_Router
!
!
!
!
!
!
ip subnet-zero
!
!
!--- IKE policies: crypto isakmp policy 11
 hash md5
 authentication pre-share
crypto isakmp key westernfinal2000 address 172.17.63.213
```

```
!
!
!--- IPSec policies: crypto ipsec transform-set sharks
esp-des esp-md5-hmac
!
!
crypto map nolan 11 ipsec-isakmp
 set peer 172.17.63.213
 set transform-set sharks
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
120
!
!
!
interface Ethernet0
 ip address 172.17.63.230 255.255.255.240
 no ip directed-broadcast
 ip nat outside
 no ip route-cache
 crypto map nolan
!
interface Ethernet1
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.240
!--- Except the private network from the NAT process: ip
nat inside source route-map nonat pool branch overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.63.225
no ip http server
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 120
permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 !---
Except the private network from the NAT process: access-
list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any !---
Except the private network from the NAT process: route-
map nonat permit 10
 match ip address 130
!
!
line con 0
 transport input none
line 1 16
line aux 0
line vty 0 4
!
end
```

Verificación

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

La herramienta intérprete de la salida apoyan a los ciertos comandos show, que permite que usted vea un análisis de la **salida del comando show**.

- show crypto isakmp sa: Ver todas las asociaciones actuales de seguridad IKE (SAs) de un par.
- **muestre ipsec crypto sa** - Muestra las configuraciones usadas por las asociaciones de seguridad actuales del [IPSec].
- show crypto engine connections active: (sólo el router) muestra las conexiones actuales y la información sobre los paquetes encripcións y desencripcións.

Troubleshooting

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

Comandos para resolución de problemas

La herramienta intérprete de la salida apoyan a los ciertos comandos show, que permite que usted vea un análisis de la **salida del comando show**.

Nota: Antes de publicar los **comandos debug**, vea por favor la información importante en los comandos Debug.

Las siguientes depuraciones deben estar ejecutándose en ambos pares IPSec.

- **isakmp crypto de la depuración** - (router y PIX) visualiza los errores durante la fase 1.
- **ipsec crypto de la depuración** - (router y PIX) visualiza los errores durante la fase 2.
- debug crypto engine – (sólo router) Muestra información del motor crypto.

La verificación de las asociaciones de seguridad se debe realizar en ambos pares Realizan a los comandos pix en el modo del permiso; los comandos del router se ejecutan en el modo non-enable (no habilitar).

- clear crypto isakmp sa - (PIX) Elimina las asociaciones de seguridad de la Fase 1.
- clear crypto isakmp – (PIX) Elimina las asociaciones de seguridad de la Fase 2.
- clear crypto isakmp – (Router) Elimina las asociaciones de seguridad de la Fase 1.
- clear crypto sa – (Router) Elimina las asociaciones de seguridad de la Fase 2.

Salida de depuración de muestra

- Depuraciones de las jefaturas PIX
- Depuraciones del router de rama

Depuraciones de las jefaturas PIX

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Branch_Router
!
!
!
!
!
!
ip subnet-zero
!
!
!--- IKE policies: crypto isakmp policy 11
 hash md5
 authentication pre-share
crypto isakmp key westernfinal2000 address 172.17.63.213
!
!
!--- IPSec policies: crypto ipsec transform-set sharks esp-des esp-md5-hmac
!
!
crypto map nolan 11 ipsec-isakmp
 set peer 172.17.63.213
 set transform-set sharks
 !--- Include the private-network-to-private-network traffic !--- in the encryption process.
match address 120
!
!
!
interface Ethernet0
 ip address 172.17.63.230 255.255.255.240
 no ip directed-broadcast
 ip nat outside
 no ip route-cache
 crypto map nolan
!
interface Ethernet1
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip nat pool branch 172.17.63.230 172.17.63.230 netmask 255.255.255.240
!--- Except the private network from the NAT process: ip nat inside source route-map nonat pool
branch overload
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 172.17.63.225
no ip http server
!--- Include the private-network-to-private-network traffic !--- in the encryption process:
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 !--- Except the private network
from the NAT process: access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list
130 permit ip 10.2.2.0 0.0.0.255 any !--- Except the private network from the NAT process:
route-map nonat permit 10
 match ip address 130
!
!
line con 0
 transport input none
line 1 16
line aux 0
line vty 0 4
!
end
```

Depuraciones del router de rama

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Branch_Router
!
!
!
!
!
!
ip subnet-zero
!
!
!--- IKE policies: crypto isakmp policy 11
 hash md5
 authentication pre-share
crypto isakmp key westernfinal2000 address 172.17.63.213
!
!
!--- IPSec policies: crypto ipsec transform-set sharks esp-des esp-md5-hmac
!
!
crypto map nolan 11 ipsec-isakmp
 set peer 172.17.63.213
 set transform-set sharks
 !--- Include the private-network-to-private-network traffic !--- in the encryption process.
match address 120
!
!
!
interface Ethernet0
 ip address 172.17.63.230 255.255.255.240
 no ip directed-broadcast
 ip nat outside
 no ip route-cache
 crypto map nolan
!
interface Ethernet1
 ip address 10.2.2.1 255.255.255.0
```

```
 no ip directed-broadcast
 ip nat inside
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip nat pool branch 172.17.63.230 172.17.63.230 netmask 255.255.255.240
!--- Except the private network from the NAT process: ip nat inside source route-map nonat pool
branch overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.63.225
no ip http server
!--- Include the private-network-to-private-network traffic !--- in the encryption process:
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 !--- Except the private network
from the NAT process: access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list
130 permit ip 10.2.2.0 0.0.0.255 any !--- Except the private network from the NAT process:
route-map nonat permit 10
 match ip address 130
!
!
line con 0
 transport input none
line 1 16
line aux 0
line vty 0 4
!
end
```

Información Relacionada

- Pedidos los comentarios (RFC)
- Soporte Técnico - Cisco Systems