IPSec/GRE con el NAT en el ejemplo de configuración del router IOS

Contenido

Introducción

La configuración de ejemplo muestra cómo configurar la encapsulación de ruteo genérica (GRE) sobre Seguridad IP (IPSec) donde GRE/IPSec atraviesa un firewall y realiza la Traducción de dirección de red (NAT).

Antes de comenzar

Convenciones

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

prerrequisitos

Este tipo de configuración podría ser utilizado para hacer un túnel y para cifrar el tráfico que no pasaría normalmente con un Firewall, tal como IPX (como en nuestro ejemplo aquí) o actualizaciones de ruteo. En este ejemplo, el túnel entre los 2621 y los 3660 solamente trabajos cuando el tráfico se genera de los dispositivos en los segmentos LAN (no un ping extendido IP/IPX de los routeres IPSec). La conectividad IP/IPX fue probada con el ping IP/IPX entre los dispositivos 2513A y 2513B.

Nota: Esto no trabaja con la traducción de dirección de puerto (PAT).

Componentes Utilizados

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

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Versión de Software Cisco PIX Firewall 7.x y posterior

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Configurar

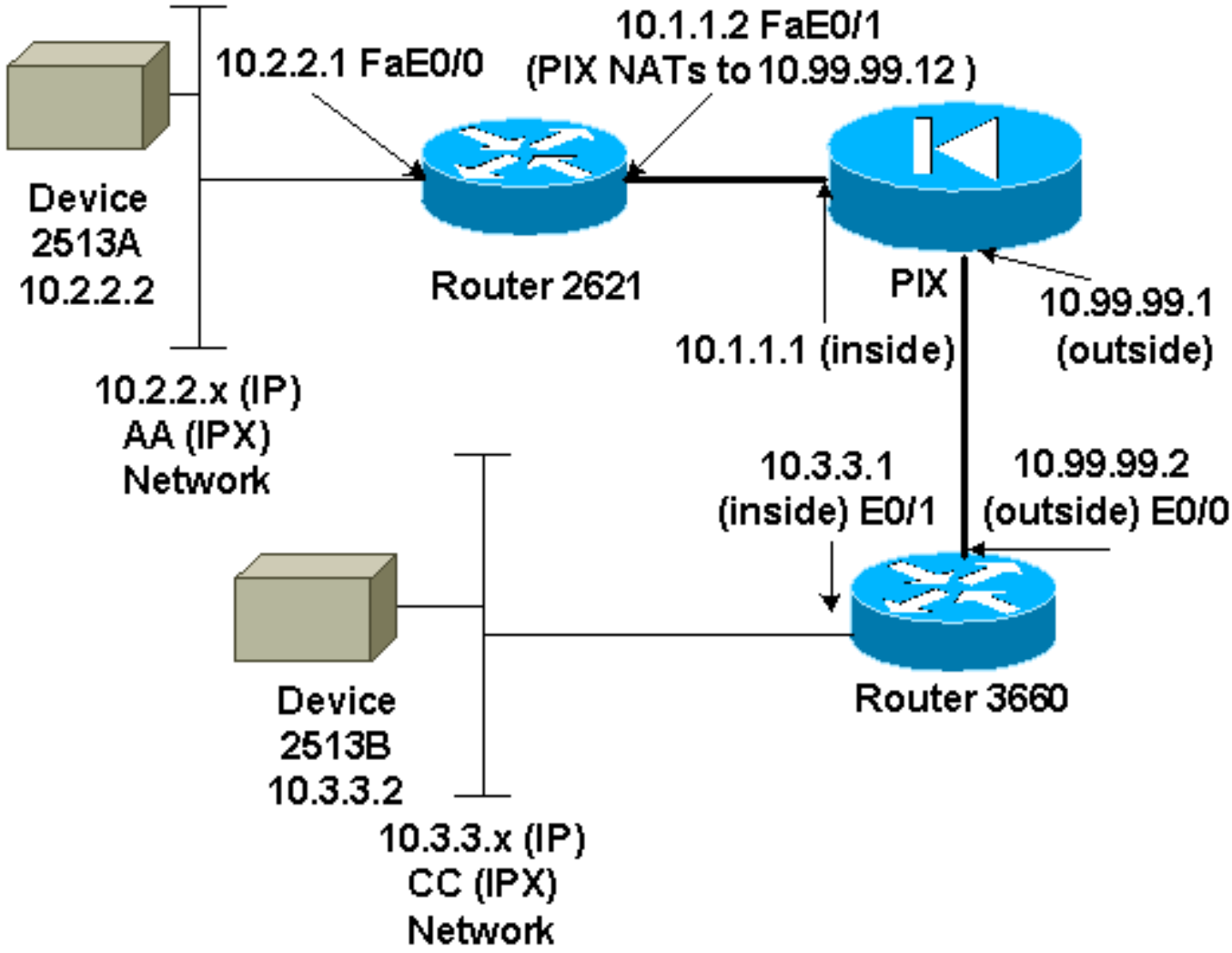
En esta sección encontrará la información para configurar las funciones descritas en este documento.

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

Nota sobre la configuración IOS: Con el IOS 12.2(13)T de Cisco y códigos posteriores (códigos de secuencia T con mayor numeración 12.3 y códigos posteriores), el "mapa criptográfico" IPSEC configurado sólo debe aplicarse a la interfaz física y ya no debe ser aplicado en la interfaz de túnel GRE. Teniendo la “correspondencia de criptografía” en la comprobación y la interfaz del túnel cuando usar el 12.2.(13)T y posterior todavía cifra los trabajos. Sin embargo, se recomienda utilizarlo sólo en la interfaz física.

Diagrama de la red

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



Nota: Las direcciones IP usadas en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Notas del diagrama de la red

- Túnel GRE de 10.2.2.1 a 10.3.3.1 (red IPX BB)
- Túnel IPsec de 10.1.1.2 (10.99.99.12) a 10.99.99.2

Configuraciones

Dispositivo 2513A

```
ipx routing 00e0.b064.20c1
!
interface Ethernet0
 ip address 10.2.2.2 255.255.255.0
 no ip directed-broadcast
 ipx network AA
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!--- Output Suppressed
```

2621

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname 2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ipx routing 0030.1977.8f80
isdn voice-call-failure 0
cns event-service server
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.2
 set transform-set myset
 match address 101
!
controller T1 1/0
!
interface Tunnel0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/0
 tunnel destination 10.3.3.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 ipx network AA
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 crypto map mymap
!
ip classless
ip route 10.3.3.0 255.255.255.0 Tunnel0
ip route 10.3.3.1 255.255.255.255 10.1.1.1
ip route 10.99.99.0 255.255.255.0 10.1.1.1
no ip http server
!
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

```
!--- Output Suppressed
```

PIX

```
pixfirewall# sh run
: Saved
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
10.99.99.2 eq isakmp


route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

!--- Output Suppressed
```

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
```

```
 match address 101
!
interface Tunnel0
 ip address 192.168.100.2 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/1
 tunnel destination 10.2.2.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
 crypto map mymap
!
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 ipx network CC
!
ip nat pool 3660-nat 10.99.99.70 10.99.99.80 netmask
255.255.255.0
ip nat inside source list 1 pool 3660-nat
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route 10.2.2.1 255.255.255.255 10.99.99.1
ip route 10.99.99.12 255.255.255.255 10.99.99.1
no ip http server
!
access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
!--- Output Suppressed
```

Dispositivo 2513B

```
ipx routing 00e0.b063.e811
!
interface Ethernet0
 ip address 10.3.3.2 255.255.255.0
 no ip directed-broadcast
 ipx network CC
!
ip route 0.0.0.0 0.0.0.0 10.3.3.1

!--- Output Suppressed
```

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 ipsec sa - Muestra las asociaciones de seguridad de la fase 2.
- muestre isakmp crypto sa - Muestra las conexiones de sesión encriptada activas actuales para todos los motores de criptografía.
- *Opcionalmente:*
- ruta de IP de la demostración - Muestra todas las Static IP rutas, o ésas instaladas usando la función de la descarga de la ruta AAA (autenticación, autorización y contabilidad).
- ruta de IPX de la demostración - Muestra el contenido del tabla de IPX Routing.

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.

- motor del debug crypto - Muestra el tráfico se cifra que.
- debug crypto ipsec - Muestra los IPSec Negotiations de la fase 2.
- debug crypto isakmp: muestra las negociaciones de fase 1 del protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP).
- *Opcionalmente:* debug ip routing: muestra información sobre las actualizaciones de la tabla de ruteo del Protocolo de Información de Ruteo (RIP) y las actualizaciones de caché de rutas.
- IPX Routing del debug {actividad | eventos} - IPX Routing del debug {actividad | eventos} - información de las demostraciones sobre los paquetes del IPX Routing que el router envía y recibe.

Verificación de Asociaciones de seguridad (SA)

- clear crytpo ipsec sa - Borra todas las asociaciones de seguridad IPSec.
- clear crypto isakmp – Limpia las asociaciones de seguridad IKE.
- *Opcionalmente:* clear ipx route * - Elimina todas las rutas de la tabla de ruteo IPX.

Información Relacionada

- Páginas de soporte de productos de seguridad IP (IPSec)
- Páginas de soporte de GRE
- Soporte Técnico - Cisco Systems