IPsec/GRE met NAT in het configuratievoorbeeld van IOS-router

Inhoud

Inleiding

Deze voorbeeldconfiguratie toont hoe u generieke Routing Encapsulation (GRE) via IP Security (IPSec) kunt configureren waar de GRE/IPSec-tunnel door een firewall gaat die netwerkadresomzetting (NAT) doet.

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Deze configuratie zou kunnen worden gebruikt om verkeer te tunnelen en te versleutelen dat normaal niet door een firewall zou gaan, zoals IPX (zoals in ons voorbeeld hier) of routingupdates. In dit voorbeeld werkt de tunnel tussen 2621 en 3660 alleen wanneer er verkeer wordt gegenereerd vanuit apparaten op de LAN-segmenten (geen uitgebreide IP/IPX-ping van de IPSec-routers). IP/IPX-connectiviteit is getest met IP/IPX-ping tussen apparaten 2513A en 2513B.

N.B.: Dit werkt niet bij PAT-adresomzetting.

Gebruikte componenten

De informatie in dit document is gebaseerd op de onderstaande software- en hardwareversies.

- Cisco IOS® 12.4
- Cisco PIX-firewall 535
- Cisco PIX-firewall-softwarerelease 7.x en hoger

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Configureren

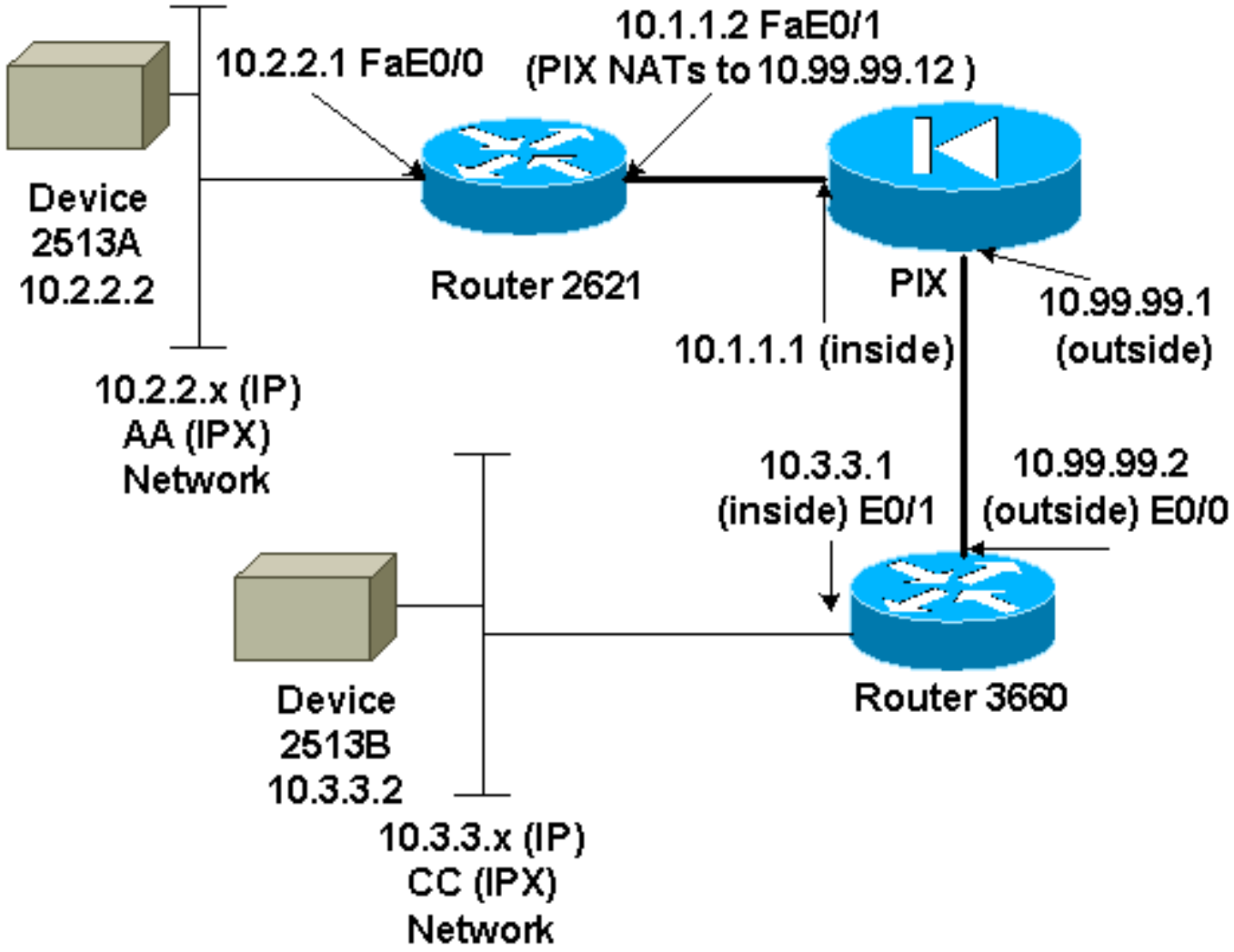
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

IOS-configuratienummer: Met Cisco IOS 12.2(13)T en latere codes (hoger genummerde T-treincodes, 12.3 en hoger codes) hoeft de geconfigureerde IPSEC-"crypto-map" alleen op de fysieke interface te worden toegepast en is deze niet langer vereist op de GRE-tunnelinterface. De "crypto map" op de fysieke en tunnelinterface bij gebruik van de 12.2.1(13)T en latere codes werken nog steeds. Het wordt echter ten zeerste aanbevolen dit alleen op de fysieke interface toe te passen.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in het onderstaande schema zijn weergegeven.



Opmerking: de IP-adressen die in deze configuratie gebruikt worden, zijn niet wettelijk routeerbaar op internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Opmerkingen netwerkdiagrammen

- GRE-tunnel van 10.2.2.1 tot 10.3.3.1 (IPX-netwerk B)
- IPsec-tunnel van 10.1.1.2 (10.99.9.12) tot 10.9.99.2

Configuraties

Apparaat 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
```

Apparaat 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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- toon crypto ipsec sa - toont de fase 2 veiligheidsassociaties .
- toon crypto isakmp sa - toont de huidige actieve gecodeerde sessies voor alle cryptomotoren .
- *Optioneel:* toon *aantal* interfaces - toont tunnelinterfaceinformatie.
- ip-route tonen - Toont alle statische IP-routes of de routes die zijn geïnstalleerd met behulp van de AAA-downloadfunctie (verificatie, autorisatie en accounting).
- toon ipx route - toont de inhoud van de IPX routingtabel.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

- debug-encryptie - Geeft het versleutelde verkeer weer.
- debug crypto ipsec - toont de IPSec-onderhandelingen van fase 2.
- debug crypto isakmp - toont de onderhandelingen over fase 1 van de Internet Security Association en Key Management Protocol (ISAKMP).
- *Optioneel:* debug ip routing - toont informatie over Routing Information Protocol (RIP) bij het routeren van tabelupdates en routecache-updates.
- debug ipx routing {activiteit | gebeurtenissen - deken ipx routing | gebeurtenissen} - Toont informatie over IPX-routingpakketten die de router stuurt en ontvangt.

Clearing Security Associations (SA's)

- cryopo ipsec sa - hiermee worden alle IPSec-beveiligingsassociaties goedgekeurd.
- duidelijke crypto isakmp - hiermee wordt de IKE-veiligheidsorganisaties ontmanteld.
- *Optioneel:* duidelijke ipx route * - Verwijdert alle routes uit de IPX routingtabel.

Gerelateerde informatie

- Productondersteuningspagina's voor IP Security (IPSec)
- GRE-ondersteuningspagina's
- Technische ondersteuning - Cisco-systemen