IPSec/GRE com o NAT no exemplo de configuração do IOS Router

Índice

Introdução

Essa configuração de exemplo mostra como configurar Generic Routing Encapsulation (GRE) sobre IP Security (IPSec), onde o túnel GRE/IPSec passa por um firewall que executa Network Address Translation (NAT).

Antes de Começar

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Pré-requisitos

Este tipo de configuração poderia ser usado para escavar um túnel e cifrar o tráfego que normalmente não atravessaria um Firewall, tal como o IPX (como em nosso exemplo aqui) ou as atualizações de roteamento. Neste exemplo, no túnel entre os 2621 e os 3660 somente trabalhos quando o tráfego for gerado dos dispositivos nos segmentos de LAN (não um sibilo prolongado IP/IPX dos roteadores de IPSec). A conectividade de IP/IPX foi testada com o ping de IP/IPX entre os dispositivos 2513A e 2513B.

Nota: Isso não funciona com a conversão de endereço de porta (PAT).

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Liberação de Software do firewall Cisco PIX 7.x e mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Configurar

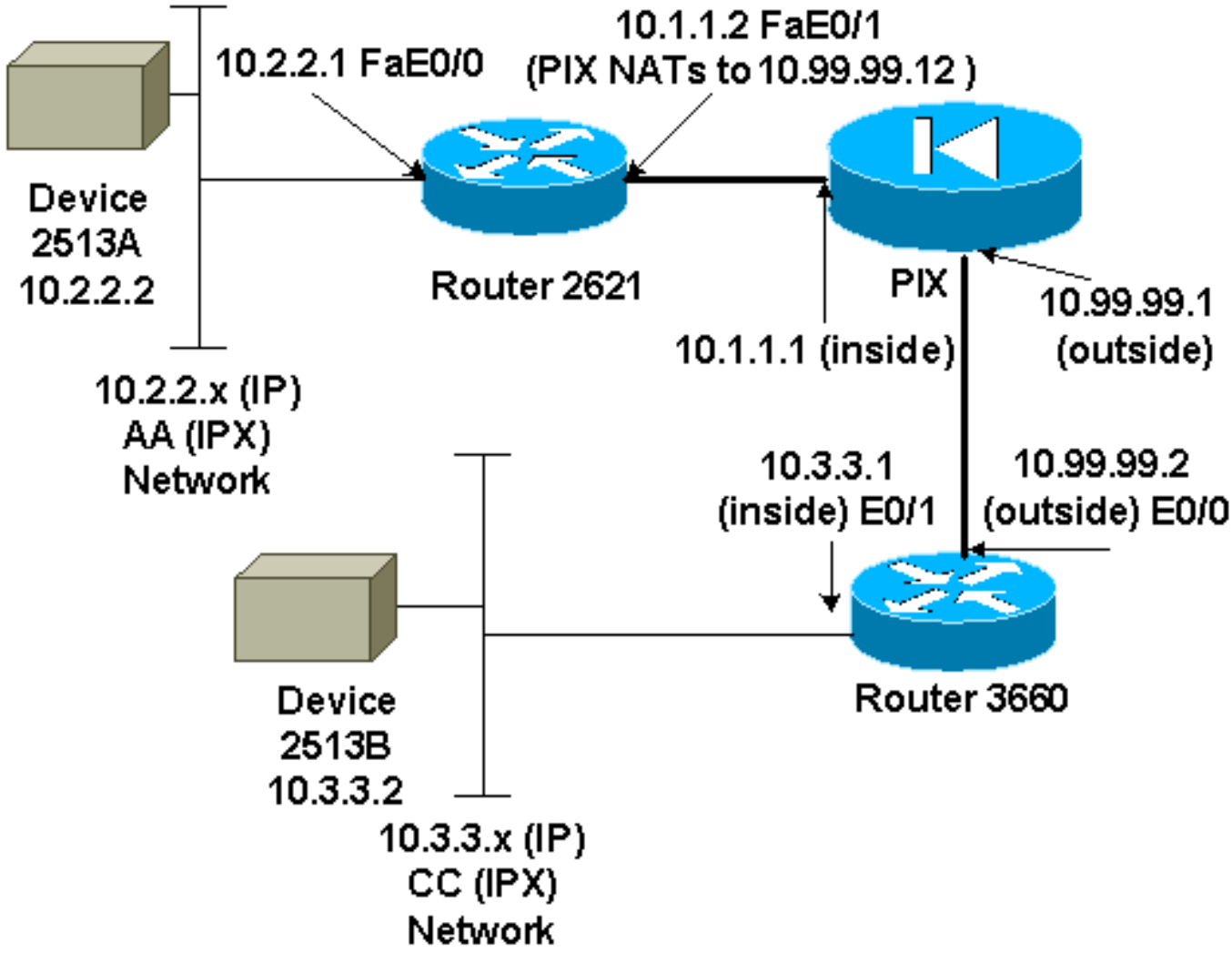
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Nota de configuração do IOS: Com o Cisco IOS 12.2(13)T e códigos posteriores (códigos T-train com numeração mais alta, 12.3 e posteriores), o "mapa de criptografia" do IPSEC configurado só precisa ser aplicado à interface física e não precisa mais ser aplicado à interface de túnel GRE. Tendo o “crypto map” no exame e na interface de túnel ao usar os trabalhos 12.2.(13)T e de códigos mais recente ainda. Entretanto, é altamente recomendado aplicá-lo só na interface física.

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



Nota: Os endereços IP de Um ou Mais Servidores Cisco ICM NT usados nesta configuração não são legalmente roteável no Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Notas de Diagrama de Rede

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

Configurações

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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- show crypto ipsec sa – Mostra as associações de segurança da fase 2.
- mostre isakmp cripto sa - Mostra as conexões de sessão de criptografia ativas atuais para todas as crypto-engines.
- *Opcionalmente:* show interfaces tunnel number - Mostra as informações da interface de túnel.
- mostre a rota IP - Mostra todas as rotas IP estático, ou aquelas instaladas usando a função da transferência da rota AAA (autenticação, autorização e relatório).

- mostre a rota IPX - Mostra os índices da tabela de roteamento de IPX.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Antes de emitir **comandos debug**, consulte Informações importantes sobre comandos debug.

- motor do debug crypto - Mostra o tráfego que é cifrado.
- debug crypto ipsec – Exibe as negociações de IPSec da fase 2.
- debug crypto isakmp – Mostra as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- *Opcionalmente:* debug ip routing Mostra informações sobre atualizações da tabela de roteamento do Routing Information Protocol (RIP) e atualizações do cache de rotas.
- debugar o roteamento IPX {atividade | eventos} - debugar o roteamento IPX {atividade | eventos} - informação das mostras nos pacotes do roteamento IPX que o roteador envia e recebe.

Limpando associações de segurança (SAs)

- clear crytpo ipsec sa - Cancela todas as associações de segurança IPSec.
- clear crypto isakmp Limpa as associações de segurança do IKE.
- *Opcionalmente:* clear ipx route * - Exclui todas as rotas da tabela de roteamento IPX.

Informações Relacionadas

- Páginas de Suporte do Produto IPSec (Protocolo de Segurança IP)
- Páginas de suporte de GRE
- Suporte Técnico - Cisco Systems