Exemplo de configuração de IPSec/GRE com NAT no roteador IOS

Contents

Introduction
Antes de Começar
Conventions
Prerequisites
Componentes Utilizados
Configurar
Diagrama de Rede
Configurações
Verificar
Troubleshoot
Comandos para Troubleshooting
Limpando associações de segurança (SAs)
Informações Relacionadas

Introduction

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

Conventions

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

Prerequisites

Esse tipo de configuração pode ser usado para fazer o túnel e criptografar o tráfego que normalmente não passaria por um firewall, como o IPX (como em nosso exemplo aqui) ou atualizações de roteamento. Neste exemplo, o túnel entre o 2621 e o 3660 só funciona quando o tráfego é gerado de dispositivos nos segmentos da LAN (não um ping IP/IPX estendido dos roteadores IPSec). A conectividade de IP/IPX foi testada com o ping de IP/IPX entre os dispositivos 2513A e 2513B.

Observação: isso não funciona com Port Address Translation (PAT).

Componentes Utilizados

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

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Software Cisco PIX Firewall versão 7.x e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Configurar

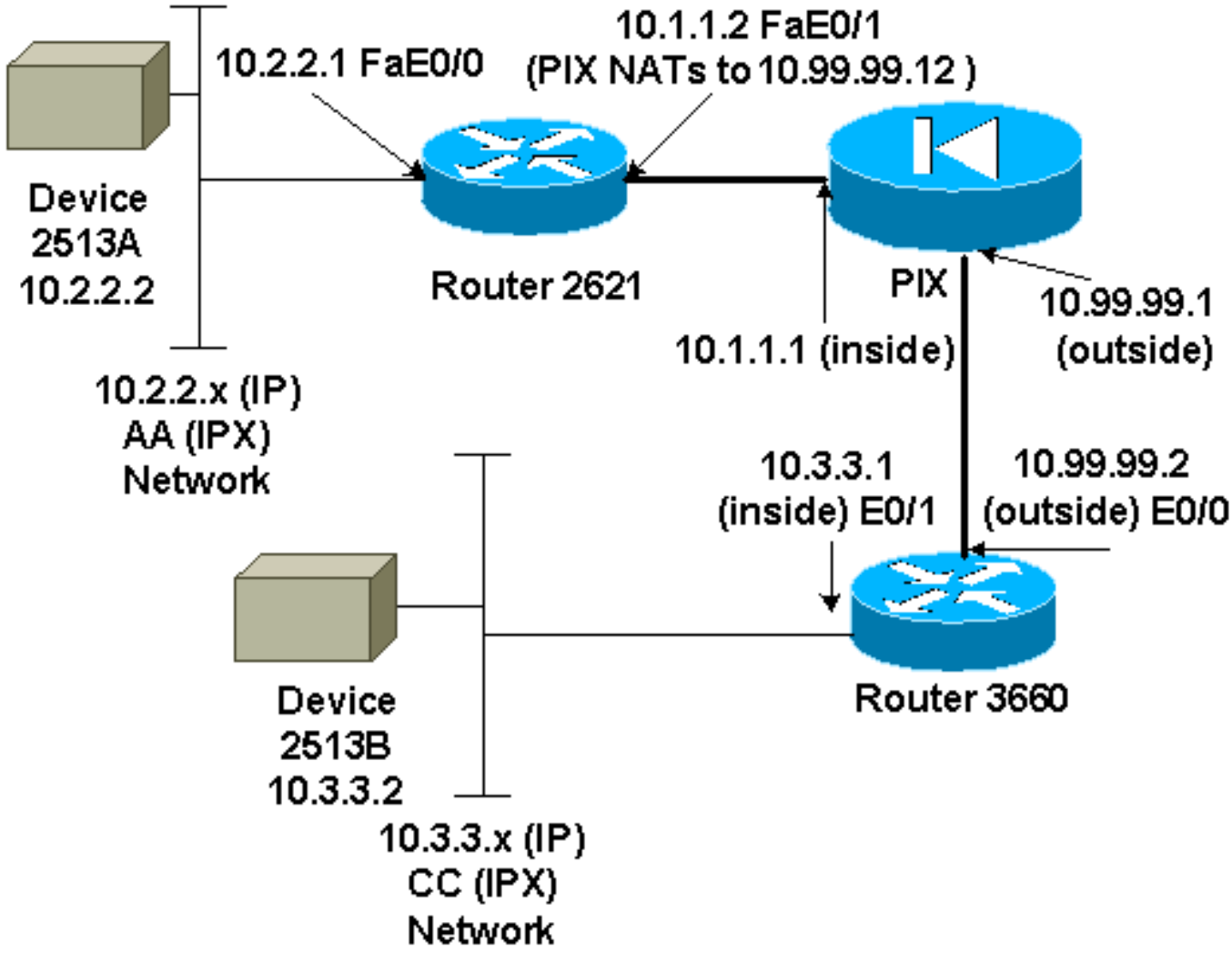
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (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. Ter o "mapa de criptografia" na interface física e de túnel ao usar o 12.2.1(13)T e códigos posteriores ainda funciona. Entretanto, é altamente recomendado aplicá-lo só na interface física.

Diagrama de Rede

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



Observação: os endereços IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços 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 (IPX network BB)
- Túnel 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.
- show crypto isakmp sa - Mostra as conexões de sessão criptografada ativas atuais para todos os mecanismos de criptografia.
- *Opcionalmente:* show interfaces tunnel number - Mostra as informações da interface de túnel.
- show ip route - Mostra todas as rotas IP estáticas ou aquelas instaladas usando a função de download de rota AAA (authentication, authorization, and accounting).
- show ipx route - Mostra o conteúdo da tabela de roteamento IPX.

Troubleshoot

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.

Observação: antes de emitir comandos **debug**, consulte Informações importantes sobre comandos debug.

- debug crypto engine - Mostra o tráfego que está criptografado.
- 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.
- debug ipx routing {activity | events} - debug ipx routing {activity | events} - Mostra informações sobre os pacotes de roteamento IPX que o roteador envia e recebe.

Limpando associações de segurança (SAs)

- clear crytpo ipsec sa - Limpa 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