

在IOS路由器配置示例中用NAT使用IPSec/GRE

目录

[简介](#)

[开始使用前](#)

[规则](#)

[先决条件](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[清除安全关联 \(SA\)](#)

[相关信息](#)

简介

此配置示例说明如何在 IP 安全 (IPSec) 上配置通用路由封装 (GRE)，此时 GRE/IPSec 隧道会通过执行网络地址转换 (NAT) 的防火墙。

开始使用前

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

先决条件

此类配置可用于通过隧道传输及加密不能正常通过防火墙的流量，例如 IPX（如此示例所示）或路由更新。在本例中，只有数据流从LAN分段上的设备生成（不是来自IPSec路由器扩展的IP/IPX ping）时，2621和3660之间的隧道才可以操作。已利用 IP/IPX ping 对设备 2513A 和 2513B 之间的连通性进行了测试。

注意：这对端口地址转换 (PAT) 无效。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS® 12.4
- Cisco PIX 防火墙 535
- Cisco PIX 防火墙软件版本 7.x 及更高版本

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

配置

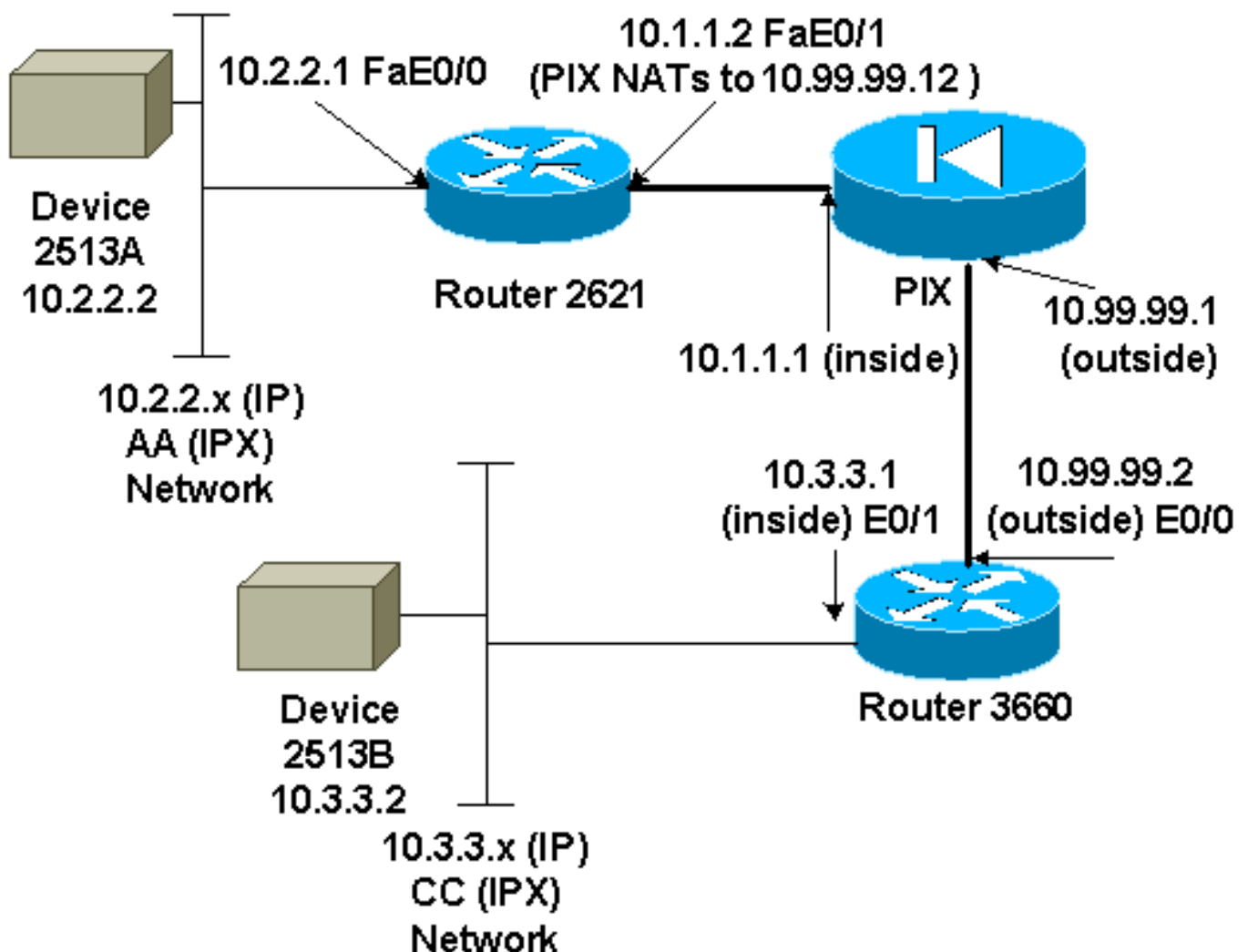
本部分提供有关如何配置本文档所述功能的信息。

注意：要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

IOS 配置说明：利用 Cisco IOS 12.2(13)T 及更高的代码（编号更高的 T 训练代码，即 12.3 及更高的代码），只需将配置的 IPSEC“加密映射”应用到物理接口，而不再需要将其应用到 GRE 隧道接口。使用 12.2.(13)T 且更高的代码仍能正常工作时，在物理和隧道接口上应用“加密映射”。不过，强烈建议仅在物理接口上应用它。

网络图

本文档使用下图所示的网络设置。



注意：此配置中使用的 IP 地址不能在 Internet 上合法地路由。这些地址是在实验室环境中使用的

[RFC 1918](#) 地址。

网络图说明

- 从 10.2.2.1 到 10.3.3.1 的 GRE 隧道 (IPX 网络 BB)
- 从 10.1.1.2 (10.99.99.12) 到 10.99.99.2 的 IPSec 隧道

配置

设备 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
```

设备 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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- [show crypto ipsec sa](#) - 显示第 2 阶段的安全关联。
- [show crypto isakmp sa](#) - 显示所有加密引擎的当前活动的加密会话连接。
- *随意地* : [show interfaces tunnel number](#) - 显示隧道接口信息。
- [show ip route](#) - 显示所有静态 IP 路由，或使用 AAA (身份验证、授权和记账) 路由下载功能安装的路由。
- [show ipx route](#) - 显示 IPX 路由表的内容。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意：在发出 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- [debug crypto engine](#) - 显示加密的流量。
- [debug crypto ipsec](#) - 显示第 2 阶段的 IPSec 协商。
- [debug crypto isakmp](#) - 显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。
- *随意地* : [debug ip routing](#) - 显示关于路由信息协议 (RIP) 路由表更新和路由缓存更新的信息。

- [debug ipx routing {活动|事件}](#) - debug ipx routing {活动|事件} - 显示有关路由器发送和接收的 IPX 路由数据包的信息。

[清除安全关联 \(SA\)](#)

- [clear crypto ipsec sa](#) - 清除所有 IPsec 安全关联。
- [clear crypto isakmp](#) - 清除 IKE 安全关联。
- 随意地：[clear ipx route ? - 从 IPX 路由表删除所有路由。](#)

[相关信息](#)

- [IP 安全 \(IPsec\) 产品支持页面](#)
- [GRE 支持页面](#)
- [技术支持 - Cisco Systems](#)