在IOS路由器上使用NAT的IPSec/GRE配置示例

目錄

簡介

此組態範例顯示如何設定GRE/IPSec通道執行網路位址轉譯(NAT)的防火牆上使用IP安全性上的通用路由封裝(GRE)(IPSec)。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

此類組態可用於對通常不會通過防火牆(例如IPX（如本例所示）或路由更新)的流量進行通道化和加密。在本範例中，只有從LAN區段上的裝置產生流量（而不是從IPSec路由器進行延伸的IP/IPX Ping）時，2621和3660之間的通道才能使用。在裝置2513A和2513B之間使用IP/IPX ping測試了IP/IPX連線。

注意：此指令不適用於連線埠位址轉譯(PAT)。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本。

- Cisco IOS® 12.4
- Cisco PIX防火牆535
- Cisco PIX防火牆軟體版本7.x及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

設定

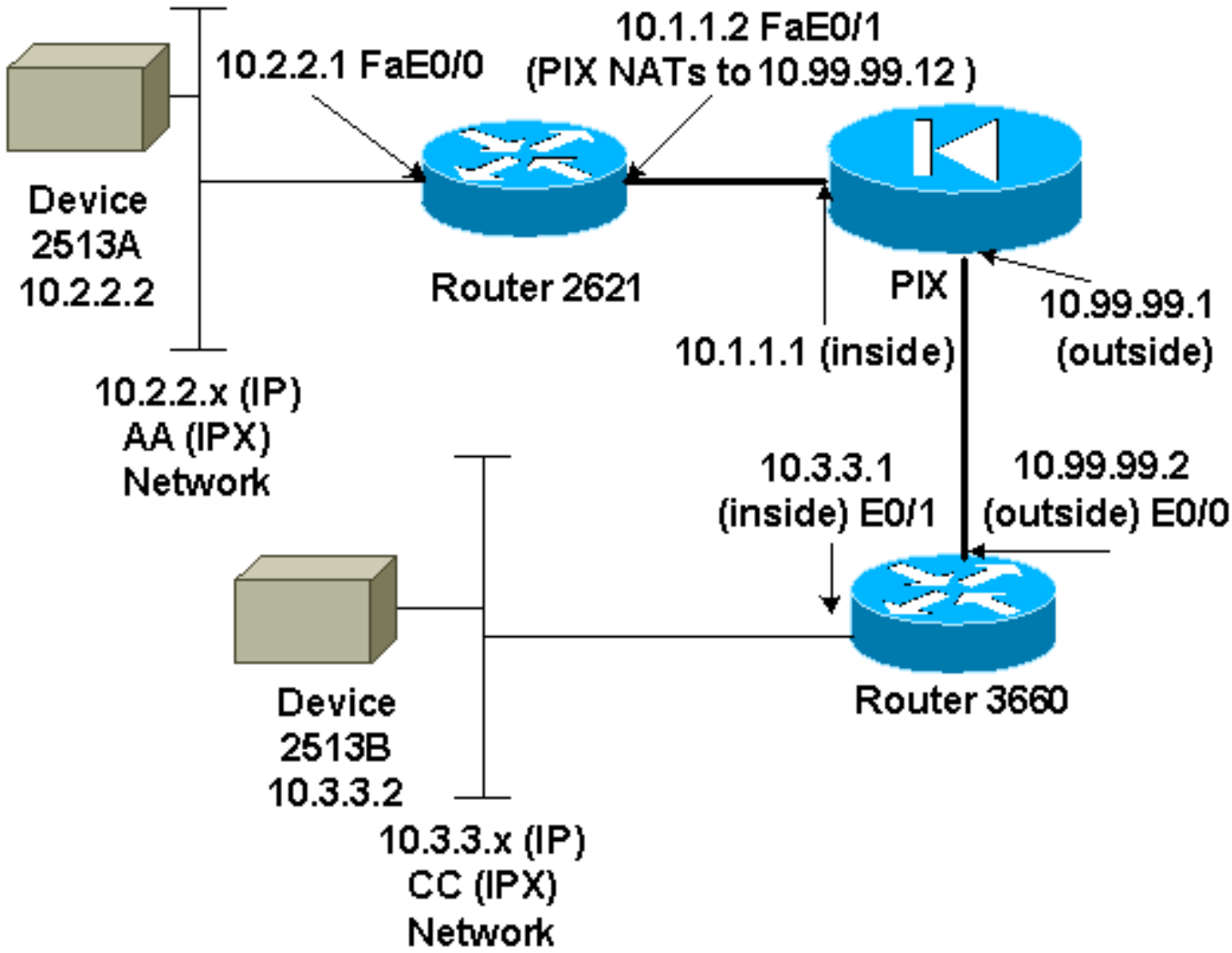
本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

IOS配置說明：若使用Cisco IOS 12.2(13)T和更新代碼（編號更高的T系列代碼、12.3和更新代碼），則配置的IPSEC「加密對映」只需應用於物理介面，而不需要再應用於GRE通道介面。使用12.2.(13)T和更新代碼時，在物理介面和隧道介面上具有「加密對映」仍然有效。但是，強烈建議僅將其應用於物理介面。

網路圖表

本文檔使用下圖所示的網路設定。



注意：此配置中使用的IP地址不能在Internet上合法路由。這些地址是RFC 1918 ，已在實驗室環境

中使用。

網路圖表說明

- 從10.2.2.1到10.3.3.1的GRE隧道（IPX網路BB）
- 從10.1.1.2(10.99.99.12)到10.99.99.2的IPSec隧道

組態

裝置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
```

裝置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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- show crypto ipsec sa — 顯示第2階段安全關聯。
- show crypto isakmp sa — 顯示所有加密引擎的當前活動加密會話連線。
- *（可選）：* show interfaces tunnel *number* — 顯示隧道介面資訊。
- show ip route — 顯示所有靜態IP路由，或使用AAA（身份驗證、授權和記帳）路由下載功能安裝的路由。
- show ipx route — 顯示IPX路由表的內容。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug指令之前，請先參閱有關Debug指令的重要資訊。

- debug crypto engine — 顯示加密的流量。
- debug crypto ipsec — 顯示第2階段的IPSec協商。
- debug crypto isakmp — 顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- *（可選）：* debug ip routing — 顯示有關路由資訊協定(RIP)路由表更新和路由快取更新的資訊。
- debug ipx routing {activity |事件} -debug ipx routing {activity | events} — 顯示路由器傳送和接收的IPX路由資料包的相關資訊。

清除安全關聯(SA)

- clear crytpo ipsec sa — 清除所有IPSec安全關聯。
- clear crypto isakmp — 清除IKE安全關聯。
- *（可選）：* clear ipx route * — 從IPX路由表中刪除所有路由。

相關資訊

- IP安全(IPSec)產品支援頁面
- GRE支援頁面
- 技術支援 - Cisco Systems