PIX 6.x :使用訪問清單和NAT配置IPsec隧道通過PIX防火牆的示例

目錄

簡介

本文檔提供通過執行網路地址轉換(NAT)的防火牆的IPSec隧道的配置示例。 **如果您使用早於12.2(13)T且不包括12.2(13)T的Cisco IOS®軟體版本，則此組態不適用於連線埠位址轉譯(PAT)。**此類配置可用於傳輸IP流量。不能用它來加密沒有通過防火牆的流量，例如IPX或路由更新。通用路由封裝(GRE)通道適用於此類組態。在本文檔的示例中，Cisco 2621和3660路由器是加入兩個專用網路的IPSec隧道終端，其間的PIX上具有管道或訪問控制清單(ACL)，以允許IPSec流量。

注意：NAT是一對一地址轉換，不要與PAT混淆，後者是許多（防火牆內部）對一轉換。有關NAT操作和配置的詳細資訊，請參閱驗證NAT操作和基本NAT故障排除或NAT的工作原理。

注意：帶PAT的IPSec可能無法正常工作，因為外部隧道終端裝置無法處理來自一個IP地址的多個隧道。您需要聯絡您的供應商，以確定隧道終端裝置是否與PAT相容。此外，在12.2(13)T及更高版本中，NAT透明功能也可以用於PAT。有關詳細資訊，請參閱IPSec NAT透明度。有關12.2(13)T及更高版本中這些功能的詳細資訊，請參閱通過NAT支援IPSec ESP。此外，在使用TAC建立案例之前，請參閱NAT常見問題，其中包含許多常見問題的答案。

有關如何在PIX/ASA版本7.x上使用NAT配置IPSec隧道穿越防火牆的詳細資訊，請參閱使用訪問清單和MPF和NAT的IPsec隧道穿越安全裝置配置示例。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本12.0.7.T [最高但不包括12.2(13)T]有關最新版本，請參閱IPSec NAT透明度。
- 運行Cisco IOS軟體版本12.4的Cisco 2621路由器
- 執行Cisco IOS軟體版本12.4的Cisco 3660路由器
- 運行6.x的Cisco PIX防火牆

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

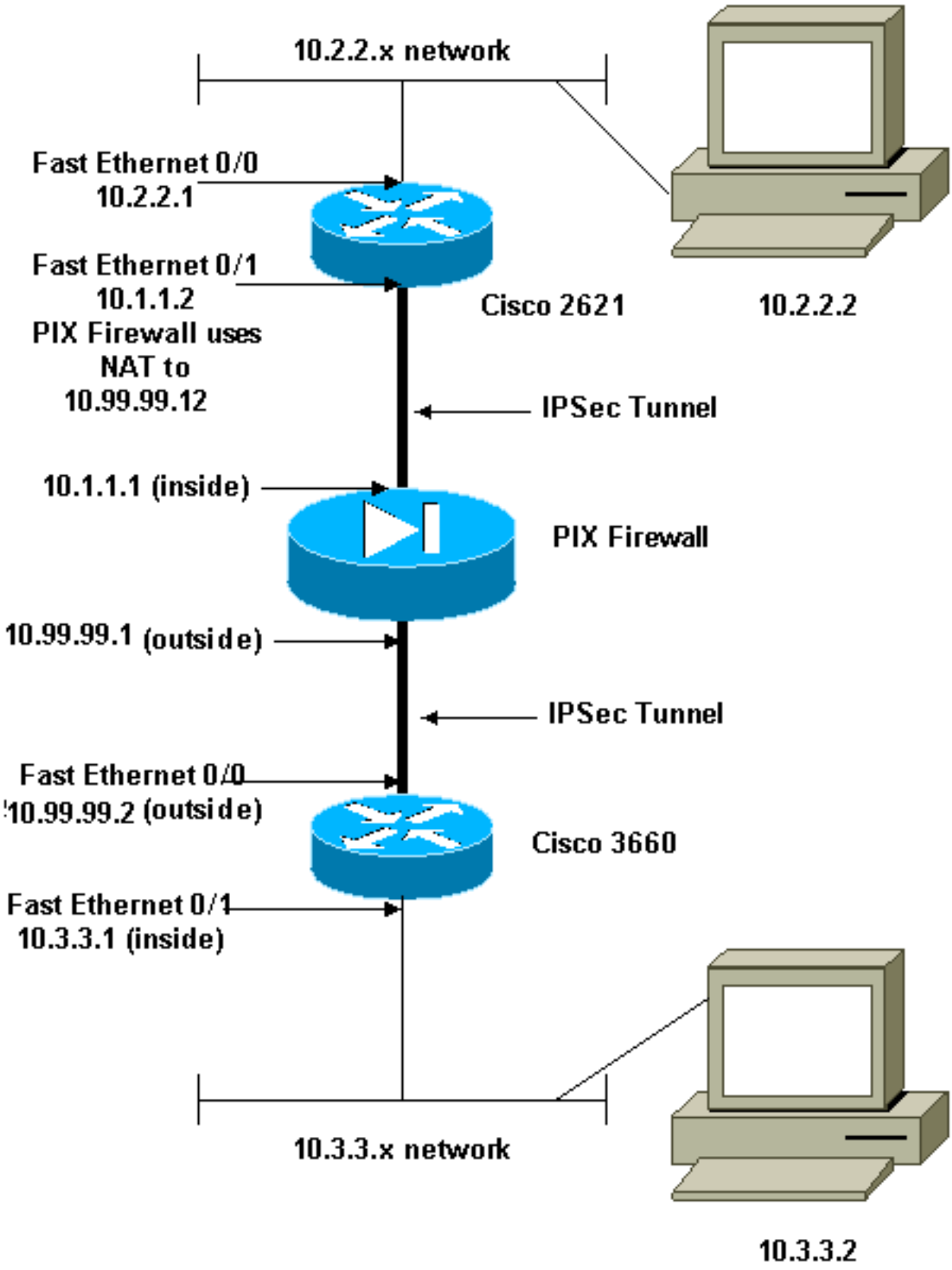
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。以下是RFC 1918 位址，已在實驗室環境中使用。

組態

本檔案會使用以下設定：

- 思科2621配置
- Cisco PIX防火牆部分配置
- 思科3660配置

思科2621配置

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy 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
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
 end
```

Cisco PIX防火牆部分配置

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. 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

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

注意：fixup protocol esp-ike命令預設處於禁用狀態。如果發出fixup protocol esp-ike命令，則會開啟該修正，並且PIX防火牆保留網際網路金鑰交換(IKE)的源埠。 它還為ESP流量建立PAT轉換。此外，如果啟用esp-ike修正，則在任何介面上都無法啟用Internet安全關聯和金鑰管理協定(ISAKMP)。

思科3660配置

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !
 !--- IKE Policy 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
!--- IPSec Policy crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
!--- Apply to interface. 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
!
interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial3/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Ethernet3/1
 no ip address
 no ip directed-broadcast
interface Ethernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface TokenRing4/0
 no ip address
 no ip directed-broadcast
 shutdown
 ring-speed 16
!
!--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
!--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 10.99.99.1
no ip http server
!
!--- Include the private-network-to-private-network
```

```
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 end
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT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 — 顯示第1階段安全關聯。
- show crypto engine connections active — 用於檢視加密和解密的資料包。

疑難排解

使用本節內容，對組態進行疑難排解。

疑難排解指令

附註：使用 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 — 用於檢視階段2的IPSec協商。
- debug crypto isakmp — 用於檢視階段1的ISAKMP協商。

清除安全關聯

- clear crypto isakmp — 清除IKE安全關聯。
- clear crypto ipsec sa — 清除IPSec安全關聯。

相關資訊

- Cisco PIX 500系列安全裝置
- Cisco Secure PIX防火牆命令參考
- NAT支援頁面

- 要求建議(RFC)
- 技術支援與文件 - Cisco Systems