

PIX 6.x : 使用访问列表和NAT配置示例使IPSec隧道穿过一个PIX防火墙

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[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](#)

[相关信息](#)

简介

本文档提供通过防火墙执行网络地址转换 (NAT) 的 IPSec 隧道示例配置。如果使用低于 (不包括) 12.2(13)T 的 Cisco IOS® 软件版本, 则此配置无法进行端口地址转换 (PAT)。这种配置可用于通过隧道传输 IP 数据流。此配置无法用于加密不通过防火墙的数据流, 例如 IPX 或路由更新。通用路由封装 (GRE) 隧道适合于此类配置。在本文档的示例中, Cisco 2621 和 3660 路由器是连接两个专用网络的 IPsec 隧道终点, 并且在之间的 PIX 上具有管道或访问控制列表 (ACL) 以允许传输 IPsec 数据流。

注意: NAT是一对一地址转换, 与多对一 (在防火墙内) 地址转换的PAT不同。有关 NAT 操作和配置的详细信息, 请参阅[验证 NAT 运行和基本的 NAT 故障排除](#)或[NAT 的工作原理](#)。

注意: 因为外部隧道终点设备处理来自一个 IP 地址的多个隧道, 所以使用 PAT 的 IPsec 可能无法正确工作。您需要联系您的供应商, 以确定隧道终点设备是否适用于 PAT。此外, 在 12.2(13)T 及更高版本中, NAT 透明模式功能也可用于 PAT。有关详细信息, 请参阅[IPSec NAT 透明模式](#)。有关 12.2(13)T 及更高版本中这些功能的详细信息, 请参阅[通过 NAT 支持 IPSec ESP](#)。此外, 通过 TAC 建立案例之前, 请参阅[NAT 常见问题](#), 其中包含许多常见问题解答。

有关如何在 PIX/ASA 版本 7.x 中配置通过防火墙 (执行 NAT) 的 IPSec 隧道的详细信息, 请参阅[IPsec 隧道使用访问列表和 MPF 通过执行 NAT 的安全设备配置示例](#)。

先决条件

要求

本文档没有任何特定的要求。

[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 软件版本 12.0.7.T (最高为 12.2(13)T , 但不包括该版本) 有关更新版本的信息 , 请参阅 [IPSec NAT 透明模式](#)。
- 运行 Cisco IOS 软件版本 12.4 的 Cisco 2621 路由器
- 运行 Cisco IOS 软件版本 12.4 的 Cisco 3660 路由器
- 运行 6.x 的 Cisco PIX 防火墙

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您使用的是真实网络 , 请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息 , 请参阅 [Cisco 技术提示规则](#)。

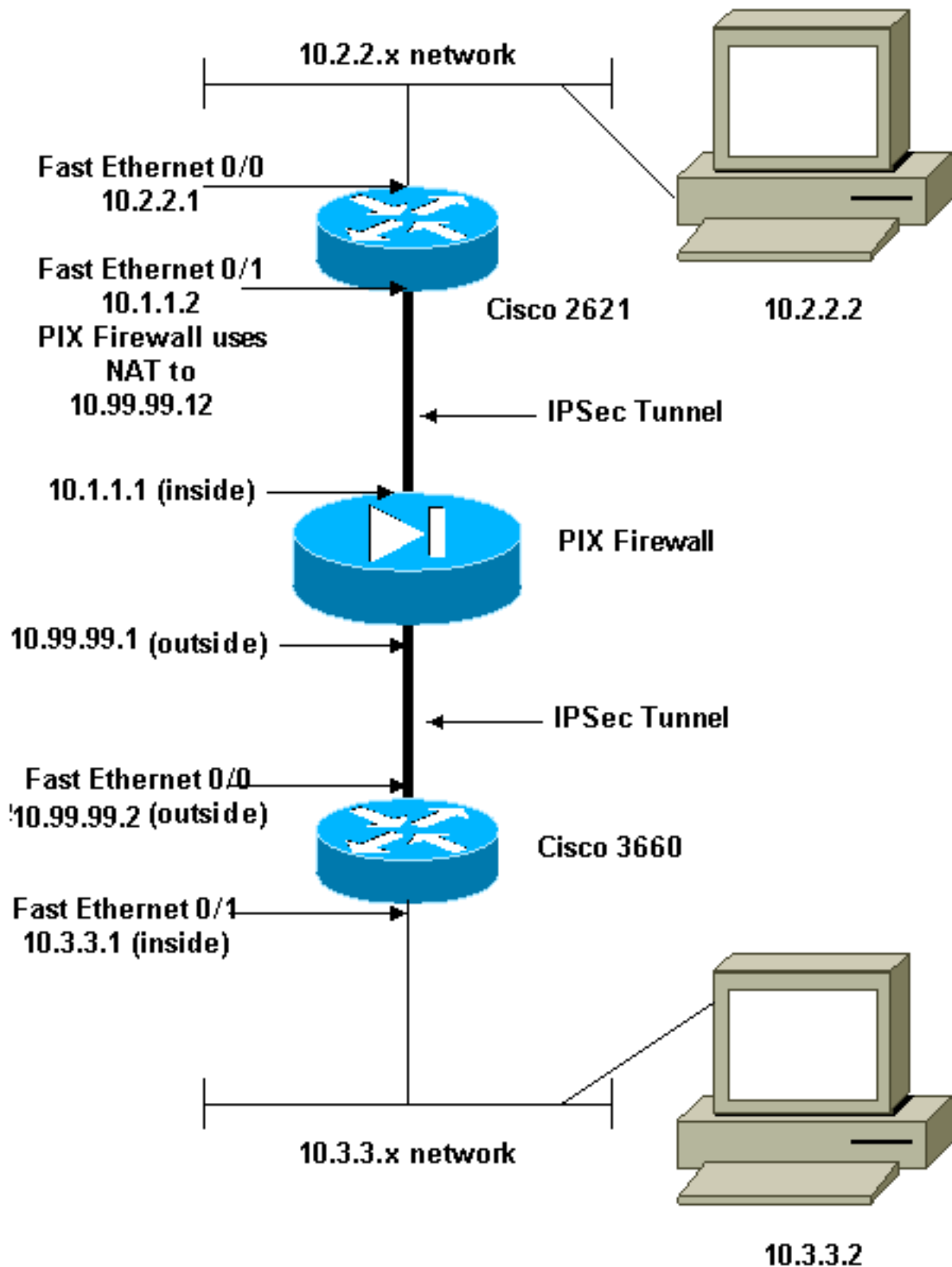
[配置](#)

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息 , 请使用 [命令查找工具](#) ([仅限注册用户](#)) 。

[网络图](#)

本文档使用以下网络设置：



注意：此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些是已在实验室环境中使用的 [RFC 1918](#) 地址。

配置

本文档使用以下配置：

- [Cisco 2621 配置](#)
- [Cisco PIX 防火墙部分配置](#)
- [Cisco 3660 配置](#)

Cisco 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 防火墙部分配置

```
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：默认情况下，fixup protocol esp-ike 命令处于禁用状态。如果发出 fixup protocol esp-ike 命令，则启用修正，并且 PIX 防火墙保留 Internet 密钥交换 (IKE) 的源端口。它还为 ESP 数据流创建 PAT 转换。此外，如果启用 esp-ike 修正，则 Internet 安全连接和密钥管理协议 (ISAKMP) 在所有接口均不能启用。

Cisco 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
```

[验证](#)

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示第 2 阶段安全连接。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。
- **show crypto engine connections active** - 用于查看加密和解密的数据包。

[故障排除](#)

使用本部分可排除配置故障。

[故障排除命令](#)

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

- **debug crypto engine** - 显示已加密的数据流。
- **debug crypto ipsec** - 用于查看第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 用于查看第 1 阶段的 ISAKMP 协商。

[清除安全关联](#)

- **clear crypto isakmp** - 清除 IKE 安全关联。
- **clear crypto ipsec sa** — 清除 IPsec 安全关联。

[相关信息](#)

- [Cisco PIX 500 系列安全设备](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [NAT 支持页](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)