配置三个 PIX 之间的 IPSec 全网状连接

目录

简介

利用此配置，三个 Cisco Secure PIX 防火墙设备后的专用网络可在 Internet 或任何使用 IPsec 的公共网络上通过 VPN 隧道进行连接。这三个网络均相互连接。在此方案中，连接到公共 Internet 需要网络地址转换 (NAT)。然而，三个内部网之间的数据流却不需要网络地址转换(NAT)，它们可以使用公共互联网上的VPN隧道传输。

先决条件

要求

为了使工作的IPsec，在您开始此配置前，您必须有连接从隧道终点到隧道终点。

使用的组件

此配置用PIX防火墙版本6.1(2)开发并且测试。

注意： **show version**命令必须显示加密启用。

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。

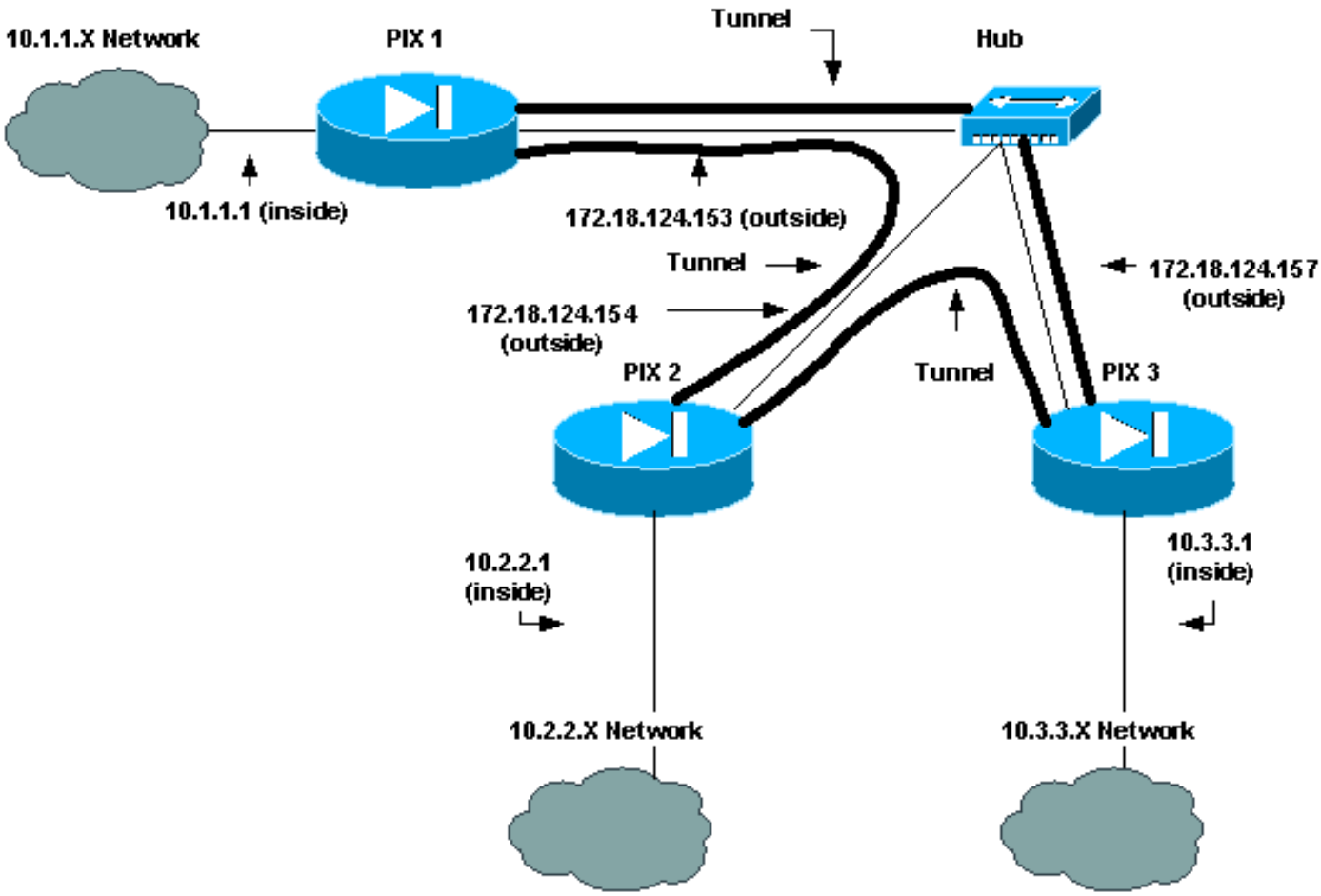
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- PIX1
- PIX2
- PIX3

PIX1 配置

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_1
fixup protocol ftp 21
```

```
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Traffic to PIX 2 private network: access-list 120
permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!--- Traffic to PIX 3 private network: access-list 130
permit ip 10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
!--- Do not perform NAT for traffic to !--- other PIX
Firewall private networks: access-list 100 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 access-
list 100 permit ip 10.1.1.0 255.255.255.0 10.3.3.0
255.255.255.0 pager lines 24 logging on no logging
timestamp no logging standby no logging console no
logging monitor no logging buffered no logging trap no
logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
172.18.124.153 255.255.255.0 ip address inside 10.1.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm no failover failover timeout 0:00:00
failover poll 15 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400 !--
- Do not perform NAT for traffic to other PIX Firewalls:
nat (inside) 0 access-list 100 route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius no snmp-server
location no snmp-server contact snmp-server community
public snmp-server enable traps floodguard enable sysopt
connection permit-ipsec no sysopt route dnat crypto
ipsec transform-set myset esp-des esp-md5-hmac !---
IPsec configuration for tunnel to PIX 2: crypto map
newmap 20 ipsec-isakmp crypto map newmap 20 match
address 120 crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset !--- IPsec
configuration for tunnel to PIX 3: crypto map newmap 30
ipsec-isakmp crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157 crypto map
newmap 30 set transform-set myset crypto map newmap
interface outside isakmp enable outside isakmp key
******** address 172.18.124.154 netmask 255.255.255.255
no-xauth no-config-mode isakmp key ******** address
172.18.124.157 netmask 255.255.255.255 no-xauth no-
config-mode isakmp identity address isakmp policy 10
authentication pre-share isakmp policy 10 encryption des
isakmp policy 10 hash md5 isakmp policy 10 group 1
isakmp policy 10 lifetime 1000 telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:436c96500052d0276324b9ef33221b2d : end
[OK]
```

PIX2 配置

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_2
```

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Traffic to PIX 1: access-list 110 permit ip
10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0 !---
Traffic to PIX 3: access-list 130 permit ip 10.2.2.0
255.255.255.0 10.3.3.0 255.255.255.0 !--- Do not perform
NAT for traffic to other PIX Firewalls: access-list 100
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list 100 permit ip 10.2.2.0 255.255.255.0
10.3.3.0 255.255.255.0 pager lines 24 logging on no
logging timestamp no logging standby no logging console
no logging monitor no logging buffered no logging trap
no logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
172.18.124.154 255.255.255.0 ip address inside 10.2.2.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm no failover failover timeout 0:00:00
failover poll 15 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400 !--
- Do not perform NAT for traffic to other PIX Firewalls:
nat (inside) 0 access-list 100 route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps floodguard enable
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac !-
-- IPsec configuration for tunnel to PIX 1: crypto map
newmap 10 ipsec-isakmp crypto map newmap 10 match
address 110 crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset !--- IPsec
configuration for tunnel to PIX 3: crypto map newmap 30
ipsec-isakmp crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157 crypto map
newmap 30 set transform-set myset crypto map newmap
interface outside isakmp enable outside isakmp key
******** address 172.18.124.153 netmask 255.255.255.255
no-xauth no-config-mode isakmp key ******** address
172.18.124.157 netmask 255.255.255.255 no-xauth no-
config-mode isakmp identity address isakmp policy 10
authentication pre-share isakmp policy 10 encryption des
isakmp policy 10 hash md5 isakmp policy 10 group 1
isakmp policy 10 lifetime 1000 telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:aef12453a0ea29b592dd0d395de881f5 : end
```

PIX 3配置

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_3
fixup protocol ftp 21
```

```
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- IPsec configuration for tunnel to PIX 1: access-
list 110 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0 !--- IPsec configuration for tunnel to PIX
2: access-list 120 permit ip 10.3.3.0 255.255.255.0
10.2.2.0 255.255.255.0 !--- Do not perform NAT for
traffic to other PIX Firewalls: access-list 100 permit
ip 10.3.3.0 255.255.255.0 10.2.2.0 255.255.255.0 access-
list 100 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0 pager lines 24 logging on no logging
timestamp no logging standby no logging console no
logging monitor no logging buffered no logging trap no
logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
172.18.124.157 255.255.255.0 ip address inside 10.3.3.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm no failover failover timeout 0:00:00
failover poll 15 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400 !--
- Do not perform NAT for traffic to other PIX Firewalls:
nat (inside) 0 access-list 100 route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps floodguard enable
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac !-
-- IPsec configuration for tunnel to PIX 1: crypto map
newmap 10 ipsec-isakmp crypto map newmap 10 match
address 110 crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset !--- IPsec
configuration for tunnel to PIX 2: crypto map newmap 20
ipsec-isakmp crypto map newmap 20 match address 120
crypto map newmap 20 set peer 172.18.124.154 crypto map
newmap 20 set transform-set myset crypto map newmap
interface outside isakmp enable outside isakmp key
******** address 172.18.124.153 netmask 255.255.255.255
no-xauth no-config-mode isakmp key ******** address
172.18.124.154 netmask 255.255.255.255 no-xauth no-
config-mode isakmp identity address isakmp policy 10
authentication pre-share isakmp policy 10 encryption des
isakmp policy 10 hash md5 isakmp policy 10 group 1
isakmp policy 10 lifetime 1000 telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:e6ad75852dff21efdb2d24cc95ffbe1c : end
[OK]
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。参考排除故障PIX通过在一个已建立的IPSec隧道的数据流欲知更多信息。

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 命令

请在PIX上使用这些命令，同时 .logging monitor debugging 或 logging console debugging命令在运行。

- **debug crypto ipsec** —调试IPSec处理。
- **debug crypto isakmp** —调试互联网安全协会和密钥管理协议(ISAKMP)处理。
- **debug crypto engine** -显示关于加密引擎的调试消息，进行加密和解密。

清除命令

为了清除安全关联(SA)，请使用在PIX的配置模式中的这些命令。

- **clear [crypto] ipsec sa** - 删除活动 IPsec SA。关键字 crypto 是可选的。
- **clear [crypto] isakmp sa** —删除活动Internet Key Exchange (IKE) SAS。关键字 crypto 是可选的。

注意： 为了使工作的IPsec，在您开始此配置前，您必须有连接从隧道终点到隧道终点。

相关信息

- **排除 PIX 故障以在已建立的 IPSec 隧道上传递数据流量**
- **Cisco PIX 500 系列安全设备**
- **PIX 命令参考**
- **IPsec Negotiations/IKE协议**
- **请求注解 (RFC)**
- **技术支持和文档 - Cisco Systems**