

配置三个 PIX 之间的 IPSec 星形连接

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

此配置允许一个中央Cisco 安全 PIX 防火墙使用IPSec，通过Internet或任何公共网络上的VPN通道，与另外两个PIX防火墙后的网络通讯。二个边远网络无需彼此通信，但是可以连接到中央网络。两个边远网络不能通过中央PIX彼此通信，因为PIX不能将在一个接口上接收的流量路由出同一个接口。如果有需要对于边远网络彼此间的通信，您需要一个充分地网状连接的配置，而不是在本文中显示的星型网配置。PIX上可能已经有 `nat 1`, `global`, `static` 和 `conduit`语句。此示例仅演示如何添加加密。

先决条件

要求

为了使IPsec工作，在开始此配置之前，您必须在隧道终点间建立连接。

使用的组件

本文档中的信息根据PIX防火墙版本5.1.x，5.2.x和6.3.3。

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](#)。

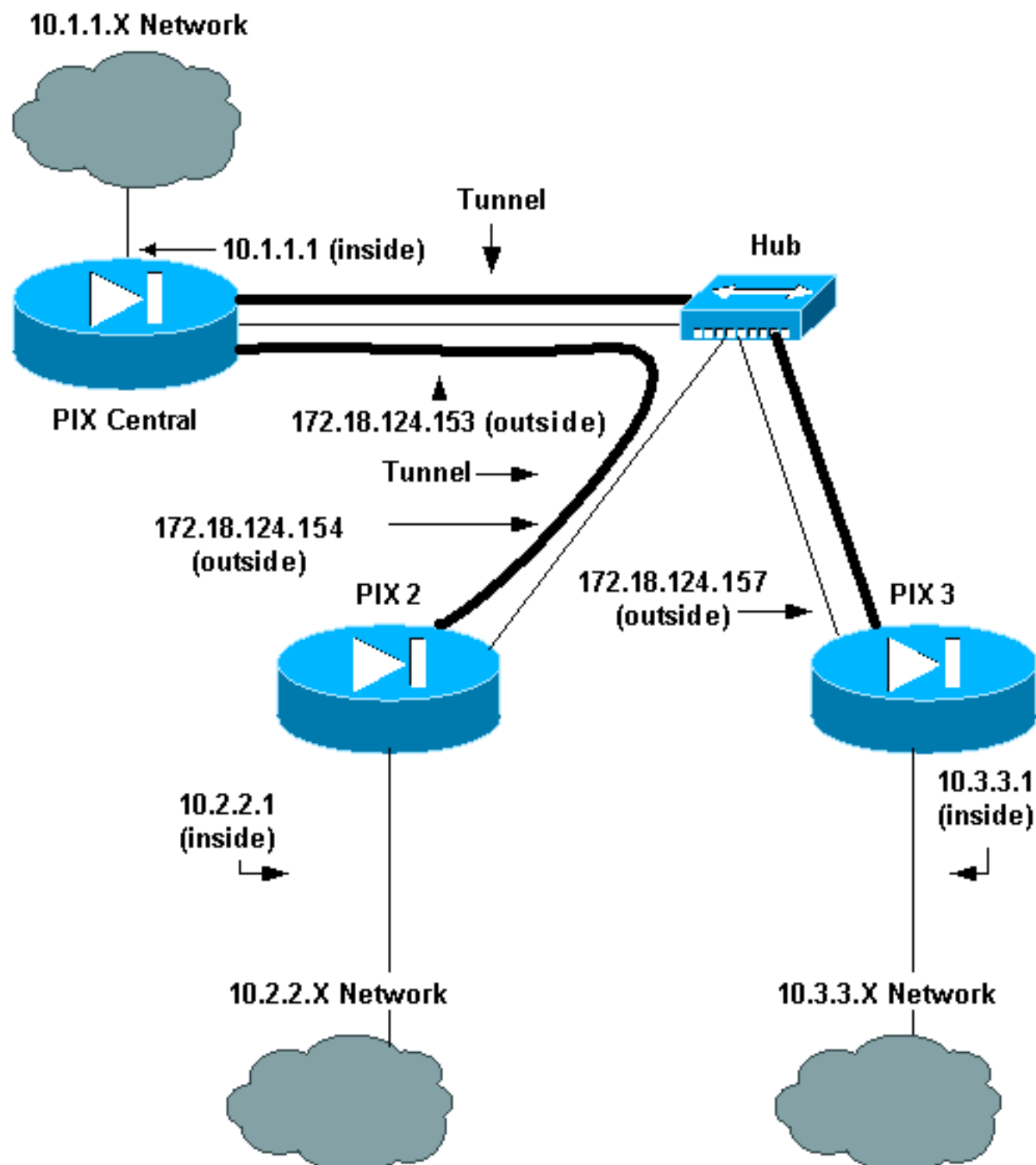
配置

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：

- [PIX中央印制厂](#)
- [PIX2](#)
- [PIX3](#)

PIX中央印制厂

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-central
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
names
!--- This is traffic to PIX 2. access-list 120 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 !--- This
is traffic to PIX 3. access-list 130 permit ip 10.1.1.0
255.255.255.0 10.3.3.0 255.255.255.0 !--- Do not do
Network Address Translation (NAT) on traffic to other
PIXes. 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 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 pdm history enable arp
timeout 14400 !--- Do not do NAT on traffic to other
PIXes. 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 h225 1:00:00 timeout h323 0:05:00 mgcp 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 aaa-server LOCAL protocol local
no snmp-server location no snmp-server contact snmp-
server community public snmp-server enable traps
floodguard enable sysopt connection permit-ipsec crypto
ipsec transform-set myset esp-des esp-md5-hmac !--- This
is traffic 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 !--- This is traffic 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 console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

PIX2

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix2
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
names
!--- This is traffic to PIX Central. access-list 110
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. access-
list 100 permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0 pager lines 24 logging on 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 no
failover ip address outside no failover ip address
inside pdm history enable arp timeout 14400 !--- Do not
do NAT on traffic to PIX Central. 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 h225 1:00:00 timeout
h323 0:05:00 mgcp 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 aaa-
server LOCAL protocol local no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable sysopt
connection permit-ipsec crypto ipsec transform-set myset
```

```
esp-des esp-md5-hmac !--- This is traffic to PIX Central. 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 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 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 console timeout 0 terminal width 80 Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

PIX3

```
Building configuration...  
: Saved  
:  
PIX Version 6.3(3)  
interface ethernet0 auto  
interface ethernet1 auto  
nameif ethernet0 outside security0  
nameif ethernet1 inside security100  
enable password 8Ry2YjIyt7RRXU24 encrypted  
passwd 2KFQnbNIdI.2KYOU encrypted  
hostname pix3  
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  
names  
!--- This is traffic to PIX Central. access-list 110  
permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0  
!--- Do not do NAT on traffic to PIX Central. 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 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 no  
failover ip address outside no failover ip address  
inside pdm history enable arp timeout 14400 !--- Do not  
do NAT on traffic to PIX Central. 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 h225 1:00:00 timeout  
h323 0:05:00 mgcp 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 aaa-  
server LOCAL protocol local no snmp-server location no  
snmp-server contact snmp-server community public no  
snmp-server enable traps floodguard enable sysopt  
connection permit-ipsec crypto ipsec transform-set myset  
esp-des esp-md5-hmac !--- This is traffic to PIX  
Central. 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 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 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 console timeout 0 terminal width 80
Cryptochecksum:aa3bbd8c6275d214b153e1e0bc0173e4 : 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IPSec安全关联(SAS)的当前状态并且是有用的在确定流量是否加密。


```

pix-central#show crypto ipsec sa interface: outside Crypto map tag: newmap, local addr.
172.18.124.153 local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0) current_peer: 172.18.124.157:500 PERMIT,
flags={origin_is_acl,} !--- This verifies that encrypted packets are sent !--- and received
without any errors. #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts
decrypt: 4, #pkts verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed:
0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors 0 local
crypto endpt.: 172.18.124.153, remote crypto endpt.: 172.18.124.157 path mtu 1500, ipsec
overhead 56, media mtu 1500 current outbound spi: 3bcb6913 !--- Shows inbound SAS that are
established. inbound esp sas: spi: 0x3efbe540(1056695616) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: newmap sa timing: remaining key
lifetime (k/sec): (4607999/27330) IV size: 8 bytes replay detection support: Y inbound ah
sas: inbound pcp sas: !--- Shows outbound SAS that are established. outbound esp sas: spi:
0x3bcb6913(1003186451) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 4, crypto map: newmap sa timing: remaining key lifetime (k/sec): (4607999/27321)
IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: local ident
(addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.2.2.0/255.255.255.0/0/0) current_peer: 172.18.124.154:500 PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are sent !--- and received without any errors.
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4, #pkts
verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.
failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.:
172.18.124.153, remote crypto endpt.: 172.18.124.154 path mtu 1500, ipsec overhead 56, media
mtu 1500 current outbound spi: da8d556 !--- Shows inbound SAS that are established. inbound
esp sas: spi: 0x53835c96(1401117846) transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 1, crypto map: newmap sa timing: remaining key lifetime
(k/sec): (4607999/27319) IV size: 8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: !--- Shows outbound SAS that are established. outbound esp sas: spi:
0xda8d556c(3666695532) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2, crypto map: newmap sa timing: remaining key lifetime (k/sec): (4607999/27319)
IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

```
- **show crypto isakmp sa** —显示Internet Key Exchange (IKE) SAS的当前状态。


```

pix-central#show crypto isakmp sa Total : 2 Embryonic : 0 dst src state pending created
172.18.124.153 172.18.124.154 QM_IDLE 0 0 172.18.124.153 172.18.124.157 QM_IDLE 0 0

```

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](#)

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

在PIX (与logging monitor debugging或操作日志控制台调试running命令)：

- 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。

[清除安全关联](#)

请使用这些in命令PIX的配置模式：

- 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 IKE SA。关键字 crypto 是可选的。

[相关信息](#)

- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [安全产品 Field Notices \(包括 PIX\)](#)
- [请求注解 \(RFC\)](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)