PIX ：从VPN隧道上的一个外部接口访问PDM

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](#)
[命令汇总](#)
[故障排除](#)
[调试输出示例](#)
[相关信息](#)

简介

此示例配置介绍了如何使用两个 PIX 防火墙配置 LAN 到 LAN VPN 隧道。PIX 设备管理器 (PDM) 通过公共端的外部接口在远程 PIX 上运行，并对常规网络和 PDM 数据流都进行加密。

PDM 是一种基于浏览器的配置工具，专用于帮助您通过 GUI 来设置、配置并监控 PIX 防火墙。您不需要全面了解 PIX 防火墙命令行界面 (CLI)。

先决条件

要求

本文档要求对 IPSec 加密和 PDM 有基本的了解。

确保您的拓扑中使用的所有设备都符合 Cisco PIX 防火墙硬件安装指南 6.3 版所规定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco PIX 防火墙软件版本 6.3(1) 和 6.3(3)
- PIX A 和 PIX B 都属于 Cisco PIX 防火墙 515E
- PIX B 使用 PDM 2.1(1) 版**注意**：PDM 3.0不使用低于6.3版的PIX防火墙软件版本运行。PDM 3.0版是仅支持PIX防火墙6.3版的单个映像。**注意**：策略NAT配置强制PDM 3.0进入监控模式。

PDM 4.0 版及更高版本支持策略 NAT。**注意：**当系统提示您输入PIX设备管理器(PDM)的用户名和密码时，默认设置不需要用户名。如果预先配置了启用口令，请将其作为 PDM 口令输入。如果没有启用口令，请将用户名和口令条目都留空，然后单击 **OK 继续。**

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。

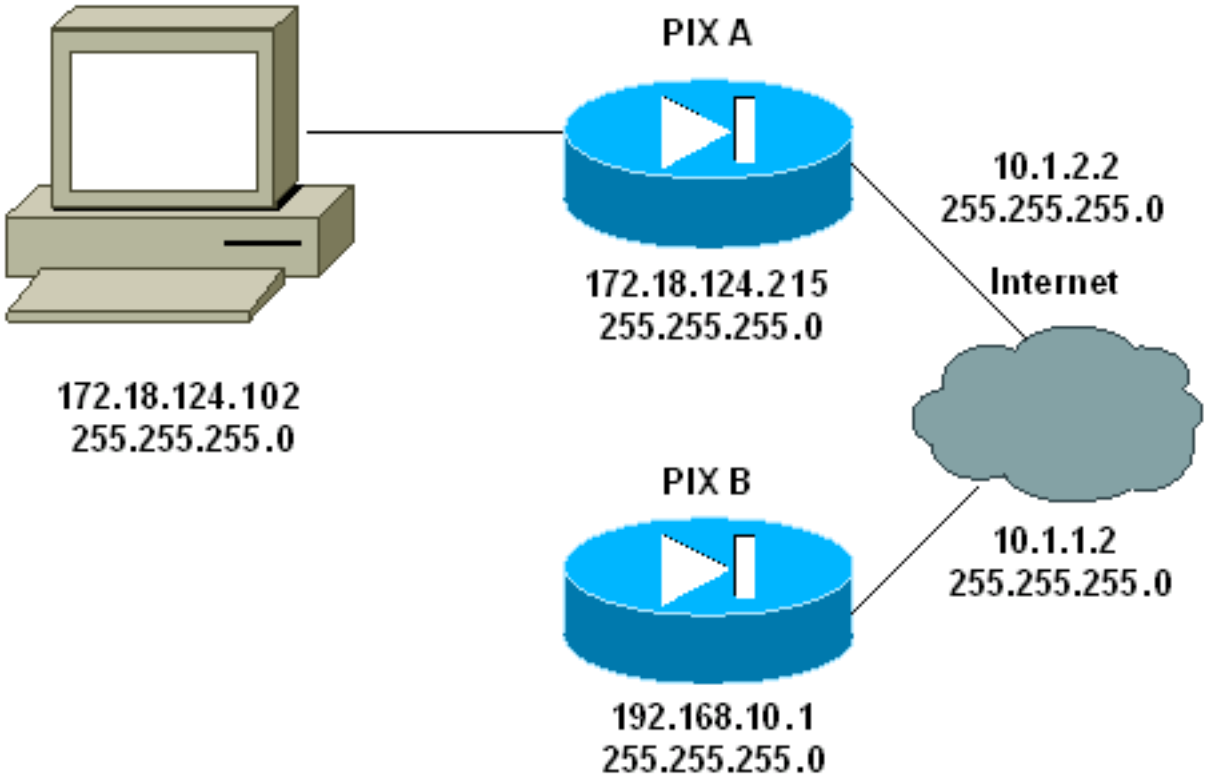
配置

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(仅限注册客户)可获取有关本节中使用的命令的详细信息。

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 A
- PIX B

PIX A

```
PIX A

PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXA
domain-name cisco.com
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
fixup protocol skinny 2000
names
!--- Allow traffic from the host PC that is going to !--
- run the PDM to the outside interface of PIX B. access-
list 101 permit ip host 172.18.124.102 host 10.1.1.2
!--- Allow traffic from the private network behind PIX A
!--- to access the private network behind PIX B. access-
list 101 permit ip 172.18.124.0 255.255.255.0
192.168.10.0 255.255.255.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.1.2.2 255.255.255.0
ip address inside 172.18.124.215 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
!--- Do not use NAT !--- on traffic which matches access
control list (ACL) 101. nat (inside) 0 access-list 101
!--- Configures a default route towards the gateway
router. route outside 0.0.0.0 0.0.0.0 10.1.2.1 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
!--- Enable the HTTP server required to run PDM. http
server enable
!--- This is the interface name and IP address of the
host or !--- network that initiates the HTTP connection.
http 172.18.124.102 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Implicitly permit any packet that came from an
IPsec !--- tunnel and bypass the checking of an
associated access-list, conduit, or !--- access-group
command statement for IPsec connections. sysopt
connection permit-ipsec
!--- Specify IPsec (phase 2) transform set. crypto ipsec
```

```
transform-set vpn esp-3des esp-md5-hmac
!--- Specify IPsec (phase 2) attributes. crypto map vpn
10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 10.1.1.2
crypto map vpn 10 set transform-set vpn
crypto map vpn interface outside
!--- Specify ISAKMP (phase 1) attributes. isakmp enable
outside
isakmp key ******** address 10.1.1.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:24e43efa87d6ef07dfabe097b82b5b40
: end
[OK]
PIXA(config)#
```

PIX B

```
PIX B
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXB
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80P
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Allow traffic from the host PC that is going to !--
- run the PDM to the outside interface of PIX B. access-
list 101 permit ip host 10.1.1.2 host 172.18.124.102
!--- Allow traffic from the private network behind PIX A
!--- to access the private network behind PIX B. access-
list 101 permit ip 192.168.10.0 255.255.255.0
172.18.124.0 255.255.255.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.1.1.2 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Assists PDM with network topology discovery by
associating an external !--- network object with an
interface. Note: The pdm location !--- command does not
```

```
control which host can launch PDM.

pdm location 172.18.124.102 255.255.255.255 outside
pdm history enable
arp timeout 14400
!--- Do not use NAT on traffic which matches ACL 101.
nat (inside) 0 access-list 101
!--- Configures a default route towards the gateway
router. route outside 0.0.0.0 0.0.0.0 10.1.1.1 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
!--- Enables the HTTP server required to run PDM. http
server enable
!--- This is the interface name and IP address of the
host or !--- network that initiates the HTTP connection.
http 172.18.124.102 255.255.255.255 outside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Implicitly permit any packet that came from an
IPsec !--- tunnel and bypass the checking of an
associated access-list, conduit, or !--- access-group
command statement for IPsec connections. sysopt
connection permit-ipsec
!--- Specify IPsec (phase 2) transform set. crypto ipsec
transform-set vpn esp-3des esp-md5-hmac
!--- Specify IPsec (phase 2) attributes. crypto map vpn
10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 10.1.2.2
crypto map vpn 10 set transform-set vpn
crypto map vpn interface outside
isakmp enable outside
!--- Specify ISAKMP (phase 1) attributes. isakmp key
******** address 10.1.2.2 netmask 255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:d5ba4da0d610d0c6140e1b781abef9d0
: end
[OK]
PIXB(config)#
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

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 isakmp sa/show isakmp sa - 验证第 1 阶段是否建立。
- show crypto ipsec sa - 验证第 2 阶段是否建立。
- show crypto engine - 显示防火墙所使用的加密引擎的使用情况统计信息。

命令汇总

一旦对 PIX 发出 VPN 命令后，当数据流在 PDM PC (172.18.124.102) 和 PIX B 的外部接口 (10.1.1.2) 之间传递时，就会建立一个 VPN 隧道。 这时，PDM PC 就能够转到 https://10.1.1.2，通过 VPN 隧道到达 PIX B 的 PDM 接口。

故障排除

本部分提供的信息可用于对配置进行故障排除。要对 PDM 相关问题进行故障排除，请参阅 PIX 设备管理器故障排除。

调试输出示例

show crypto isakmp sa

此输出表示在 10.1.1.2 和 10.1.2.2 之间已形成一个隧道。

```
PIXA#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst         src         state     pending    created
        10.1.1.2    10.1.2.2    QM_IDLE         0           1
```

show crypto ipsec sa

此输出表示在 10.1.1.2 和 172.18.124.102 之间传递数据流的隧道。

```
PIXA#show crypto ipsec sa

interface: outside
    Crypto map tag: vpn, local addr. 10.1.2.2

   local  ident (addr/mask/prot/port): (172.18.124.102/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/0/0)
   current_peer: 10.1.1.2
>     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14472, #pkts encrypt: 14472, #pkts digest 14472
    #pkts decaps: 16931, #pkts decrypt: 16931, #pkts verify 16931
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 9, #recv errors 0

     local crypto endpt.: 10.1.2.2, remote crypto endpt.: 10.1.1.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 4acd5c2a

     inbound esp sas:
      spi: 0xcff9696a(3489229162)
        transform: esp-3des esp-md5-hmac ,
```

```
    in use settings ={Tunnel, }
    slot: 0, conn id: 2, crypto map: vpn
    sa timing: remaining key lifetime (k/sec): (4600238/15069)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x4acd5c2a(1254972458)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 1, crypto map: vpn
    sa timing: remaining key lifetime (k/sec): (4607562/15069)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

相关信息

- PIX 命令参考
- Cisco PIX 500 系列安全设备
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems