PIX:通過VPN隧道從外部介面訪問PDM

目錄

簡介

此示例配置介紹了如何使用兩個PIX防火牆配置LAN到LAN VPN隧道。PIX裝置管理器(PDM)通過公共端的外部介面在遠端PIX上運行，並對常規網路和PDM流量進行加密。

PDM是一種基於瀏覽器的配置工具，旨在幫助您使用GUI設定、配置和監控PIX防火牆。您不需要對PIX防火牆命令列介面(CLI)有豐富的知識。

必要條件

需求

本文檔要求對IPsec加密和PDM有基本瞭解。

確保拓撲中使用的所有裝置都符合Cisco PIX防火牆硬體安裝指南6.3版中描述的要求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco PIX防火牆軟體版本6.3(1)和6.3(3)
- PIX A和PIX B是Cisco PIX防火牆515E
- PIX B使用PDM版本2.1(1)**注意：**PDM 3.0不能使用低於6.3版的PIX防火牆軟體版本運行。PDM 3.0版是僅支援PIX防火牆版本6.3的單個映像。**注意：**策略NAT配置迫使PDM 3.0進入監控模式

。PDM 4.0及更高版本支援策略NAT。**注意**：當系統提示您輸入PIX裝置管理器(PDM)的使用者名稱和密碼時，預設設定不需要使用者名稱。如果先前配置了啟用密碼，請輸入該密碼作為PDM密碼。如果沒有啟用密碼，請將使用者名稱和密碼條目都留空，然後按一下**OK**繼續。

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。

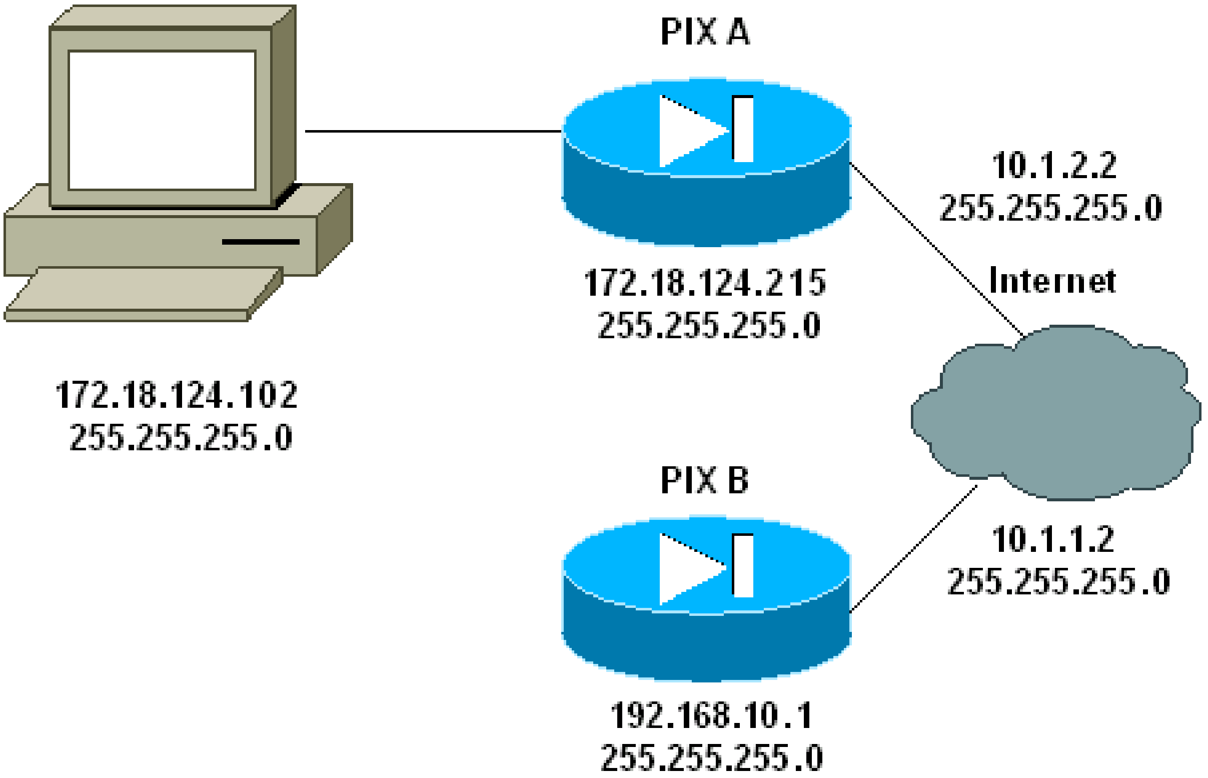
設定

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(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- 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)#
```

驗證

本節提供的資訊可用於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 isakmp sa/show isakmp sa — 驗證第1階段是否建立。
- show crypto ipsec sa — 驗證第2階段是否建立。
- show crypto engine — 顯示防火牆使用的加密引擎的使用統計資訊。

命令摘要

將VPN命令放入PIX後，當流量通過PDM PC(172.18.124.102)和PIX B的外部介面(10.1.1.2)時，應建立VPN隧道。 此時，PDM PC可以通過VPN隧道訪問https://10.1.1.2並訪問PIX B的PDM介面。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。請參閱排除PIX裝置管理器故障，對PDM相關問題進行故障排除。

調試輸出示例

show crypto isakmp sa

此輸出顯示在10.1.1.2和10.1.2.2之間形成的隧道。

```
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

此輸出顯示了通過10.1.1.2和172.18.124.102之間流量的隧道。

```
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:
```

相關資訊

- PIX命令參考
- Cisco PIX 500系列安全裝置
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems