PIX: VPN 터널을 통해 외부 인터페이스에서 PDM 액세스

목차

소개

이 샘플 컨피그레이션에서는 두 개의 PIX 방화벽을 사용하여 LAN-to-LAN VPN 터널을 구성하는 방법을 설명합니다. PDM(PIX Device Manager)은 공용 쪽의 외부 인터페이스를 통해 원격 PIX에서 실행되며 일반 네트워크와 PDM 트래픽을 모두 암호화합니다.

PDM은 GUI를 사용하여 PIX 방화벽을 설정, 구성 및 모니터링하는 데 도움이 되도록 설계된 브라우저 기반 구성 도구입니다. PIX 방화벽 CLI(Command-Line Interface)에 대한 폭넓은 지식이 필요하지 않습니다.

사전 요구 사항

요구 사항

이 문서에서는 IPsec 암호화 및 PDM에 대한 기본적인 이해가 필요합니다.

토폴로지에 사용된 모든 디바이스가 Cisco PIX Firewall Hardware Installation Guide, Version 6.3에 설명된 요구 사항을 충족하는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco PIX Firewall Software 릴리스 6.3(1) 및 6.3(3)
- PIX A 및 PIX B는 Cisco PIX Firewall 515E
- PIX B는 PDM 버전 2.1(1) 사용**참고:** PDM 3.0은 버전 6.3 이전의 PIX 방화벽 소프트웨어 버전에서 실행되지 않습니다. PDM 버전 3.0은 PIX Firewall 버전 6.3만 지원하는 단일 이미지입니다.**참고:** 정책 NAT 컨피그레이션은 PDM 3.0을 모니터 모드로 전환합니다. 정책 NAT는 PDM 버전 4.0 이상에서 지원됩니다.**참고:** PDM(PIX Device Manager)에 대한 사용자 이름과 비밀번호를 입력하라는 메시지가 표시되면 기본 설정에 사용자 이름이 필요하지 않습니다. 이전에 enable 비밀번호를 구성한 경우 해당 비밀번호를 PDM 비밀번호로 입력합니다. enable 비밀번호가 없으면 사용자 이름과 비밀번호 항목을 모두 비워 두고 **OK**(확인)를 클릭하여 계속합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

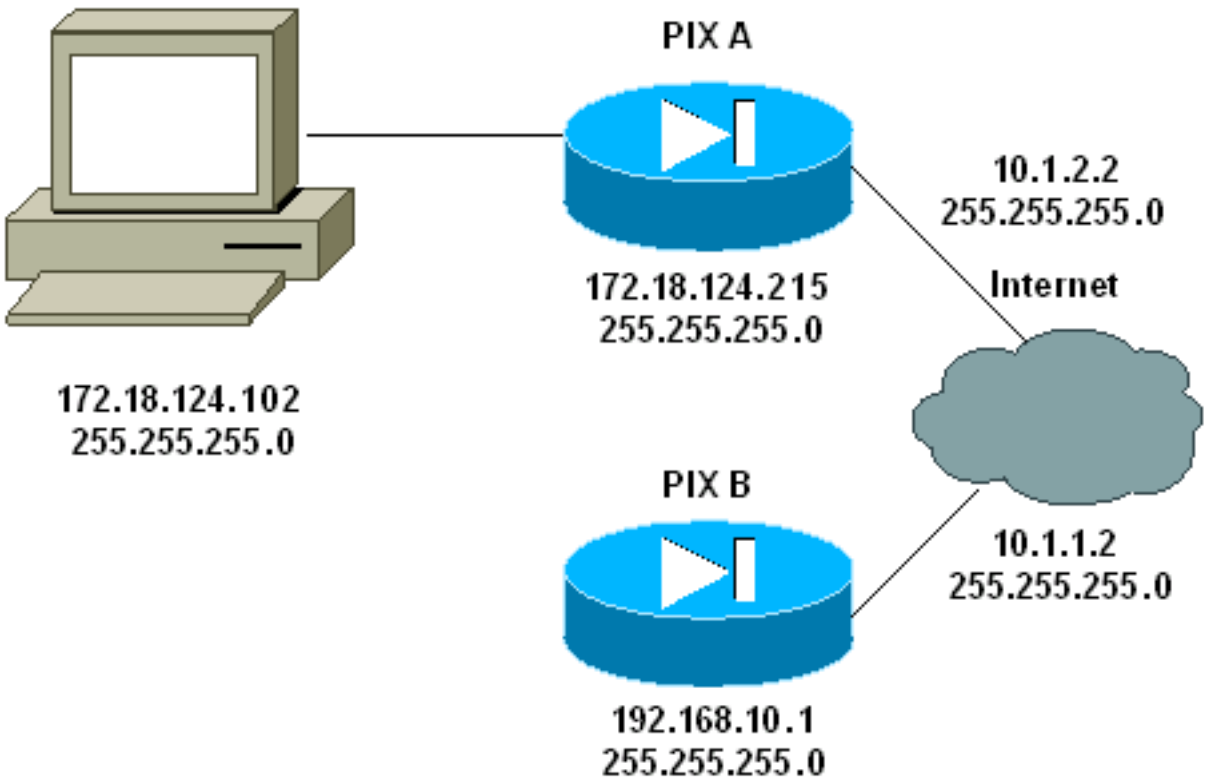
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- 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)#
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto isakmp sa/show isakmp sa** - 1단계가 설정되었는지 확인합니다.
- **show crypto ipsec sa** - 2단계가 설정되었는지 확인합니다.
- **show crypto engine**—방화벽에서 사용하는 암호화 엔진에 대한 사용량 통계를 표시합니다.

명령 요약

PIX에 VPN 명령을 입력하면 PDM PC(172.18.124.102)과 PIX B(10.1.1.2)의 외부 인터페이스 간에 트래픽이 전달될 때 VPN 터널이 설정되어야 합니다. 이 시점에서 PDM PC는 https://10.1.1.2으로 이동하여 VPN 터널을 통해 PIX B의 PDM 인터페이스에 연결할 수 있습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. PDM 관련 문제를 해결하려면 PIX 장치 관리자 문제 해결을 참조하십시오.

디버그 출력 샘플

crypto isakmp sa 표시

이 출력은 10.1.1.2과 10.1.2.2 사이에 형성되는 터널을 보여줍니다.

```
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
```

crypto ipsec sa 표시

이 출력은 10.1.1.2~172.18.124.102 사이의 트래픽을 전달하는 터널을 보여줍니다.

```
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:
```

관련 정보

- PIX 명령 참조
- Cisco PIX 500 Series 보안 어플라이언스
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems