

# PIX: Acesse o PDM de uma interface externa sobre um túnel VPN

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Resumo de comandos](#)

[Troubleshoot](#)

[Exemplo de saída de depuração](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este exemplo de configuração documenta como configurar um túnel VPN LAN a LAN usando dois PIX Firewalls. O PIX Device Manager (PDM) é executado no PIX remoto através da interface externa no lado público e criptografa o tráfego regular de rede e PDM.

O PDM é uma ferramenta de configuração baseada em navegador projetada para ajudá-lo a configurar, configurar e monitorar seu PIX Firewall com uma GUI. Você não precisa de conhecimento extensivo da interface de linha de comando (CLI) do PIX Firewall.

## [Prerequisites](#)

### [Requirements](#)

Este documento requer uma compreensão básica da [criptografia IPsec](#) e PDM.

Certifique-se de que todos os dispositivos usados na topologia atendam aos requisitos descritos no [Cisco PIX Firewall Hardware Installation Guide, Versão 6.3](#).

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco PIX Firewall versão 6.3(1) e 6.3(3)
- PIX A e PIX B são Cisco PIX Firewall 515E
- O PIX B usa PDM versão 2.1(1)**Observação:** o PDM 3.0 não é executado com versões do software PIX Firewall anteriores à versão 6.3. O PDM Versão 3.0 é uma única imagem que suporta apenas o PIX Firewall Versão 6.3.**Observação:** as configurações de NAT de política forçam o PDM 3.0 para o modo de monitor. O NAT de política é suportado no PDM versão 4.0 e posterior.**Observação:** quando for solicitado um nome de usuário e uma senha para o PIX Device Manager (PDM), as configurações padrão não exigem nenhum nome de usuário. Se uma senha de ativação tiver sido configurada anteriormente, insira essa senha como senha PDM. Se não houver senha de ativação, deixe as entradas de nome de usuário e senha em branco e clique em **OK** para continuar.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## [Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

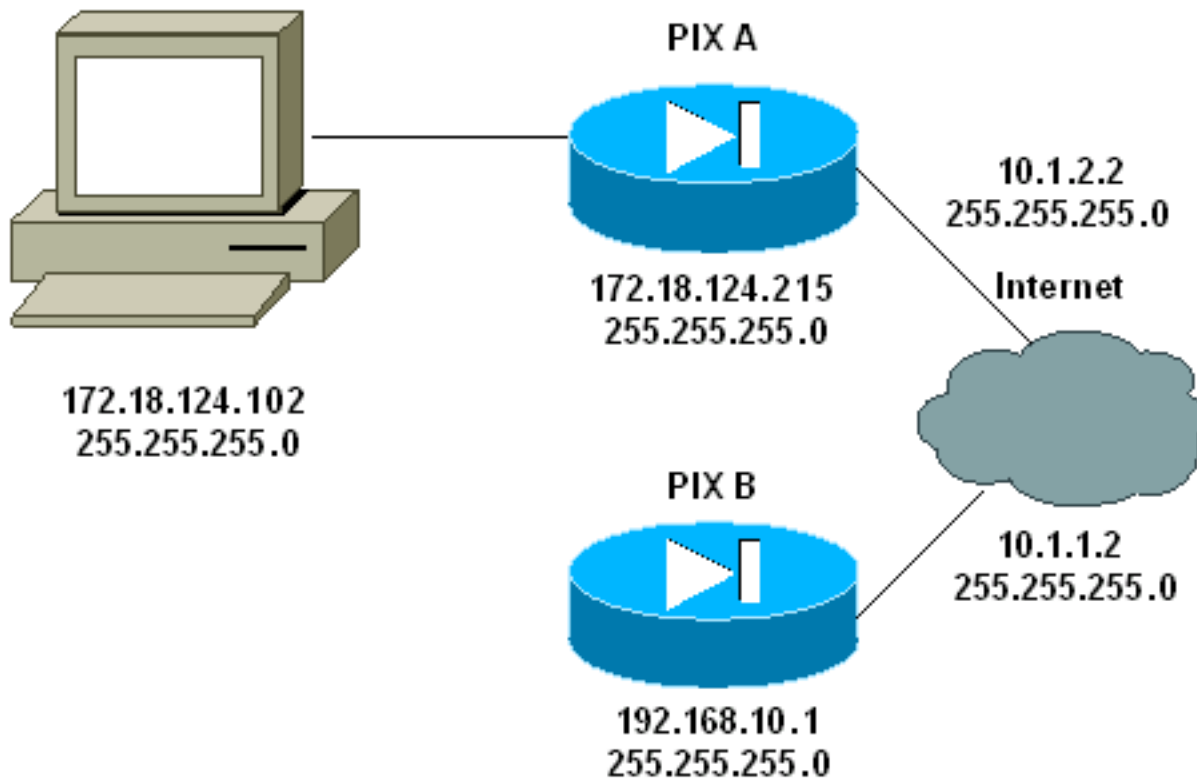
## [Configurar](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

## [Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:



## Configurações

Este documento utiliza as seguintes configurações:

- [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)#
```

## Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a determinados comandos [show](#). Use a OIT para exibir uma análise da saída do comando show.

- [show crypto isakmp sa/show isakmp sa](#) —Verifica se a fase 1 foi estabelecida.
- [show crypto ipsec sa](#) —Verifica se a fase 2 foi estabelecida.
- [show crypto engine](#) —Exibe as estatísticas de uso do mecanismo de criptografia usado pelo firewall.

## Resumo de comandos

Quando os comandos VPN são colocados nos PIXes, um túnel VPN deve ser estabelecido quando o tráfego passa entre o PC PDM (172.18.124.102) e a interface externa do PIX B (10.1.1.2). Neste ponto, o PC PDM pode ir para <https://10.1.1.2> e acessar a interface PDM do PIX B pelo túnel VPN.

## Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. Consulte [Troubleshooting do PIX Device Manager](#) para solucionar problemas relacionados ao PDM.

## Exemplo de saída de depuração

### show crypto isakmp sa

Esta saída mostra um túnel formado entre 10.1.1.2 e 10.1.2.2.

```
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

Esta saída mostra um túnel que passa o tráfego entre 10.1.1.2 e 172.18.124.102.

```
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:

## Informações Relacionadas

- [Referências de comando PIX](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)