# PIX Accesso a PDM da un'interfaccia esterna su un tunnel VPN

## Sommario



## Introduzione

In questa configurazione di esempio viene descritto come configurare un tunnel VPN da LAN a LAN con due firewall PIX. PIX Device Manager (PDM) viene eseguito sul PIX remoto tramite l'interfaccia esterna sul lato pubblico e crittografa sia il traffico di rete regolare che il traffico PDM.

PDM è uno strumento di configurazione basato su browser progettato per semplificare la configurazione, la configurazione e il monitoraggio del firewall PIX tramite un'interfaccia utente grafica. non è necessaria una conoscenza approfondita dell'interfaccia della riga di comando (CLI) di PIX Firewall.

## Prerequisiti

### Requisiti

Questo documento richiede una comprensione di base della crittografia IPSec e di PDM.

Verificare che tutti i dispositivi utilizzati nella topologia soddisfino i requisiti descritti nella Cisco PIX Firewall Hardware Installation Guide, versione 6.3.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Software Cisco PIX Firewall release 6.3(1) e 6.3(3)
- I PIX A e PIX B sono Cisco PIX Firewall 515E
- PIX B utilizza PDM versione 2.1(1)**Nota:** PDM 3.0 non viene eseguito con software PIX Firewall versioni precedenti alla versione 6.3. PDM versione 3.0 è una singola immagine che supporta solo PIX Firewall versione 6.3.**Nota:** le configurazioni NAT dei criteri forzano l'attivazione della modalità di monitoraggio di PDM 3.0. Policy NAT è supportato in PDM versione 4.0 e successive.**Nota:** quando vengono richiesti un nome utente e una password per PIX Device Manager (PDM), le impostazioni predefinite non richiedono alcun nome utente. Se in precedenza è stata configurata una password di abilitazione, immettere tale password come password PDM. Se non è disponibile una password di abilitazione, lasciare vuote entrambe le voci relative al nome utente e alla password e fare clic su **OK** per continuare.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

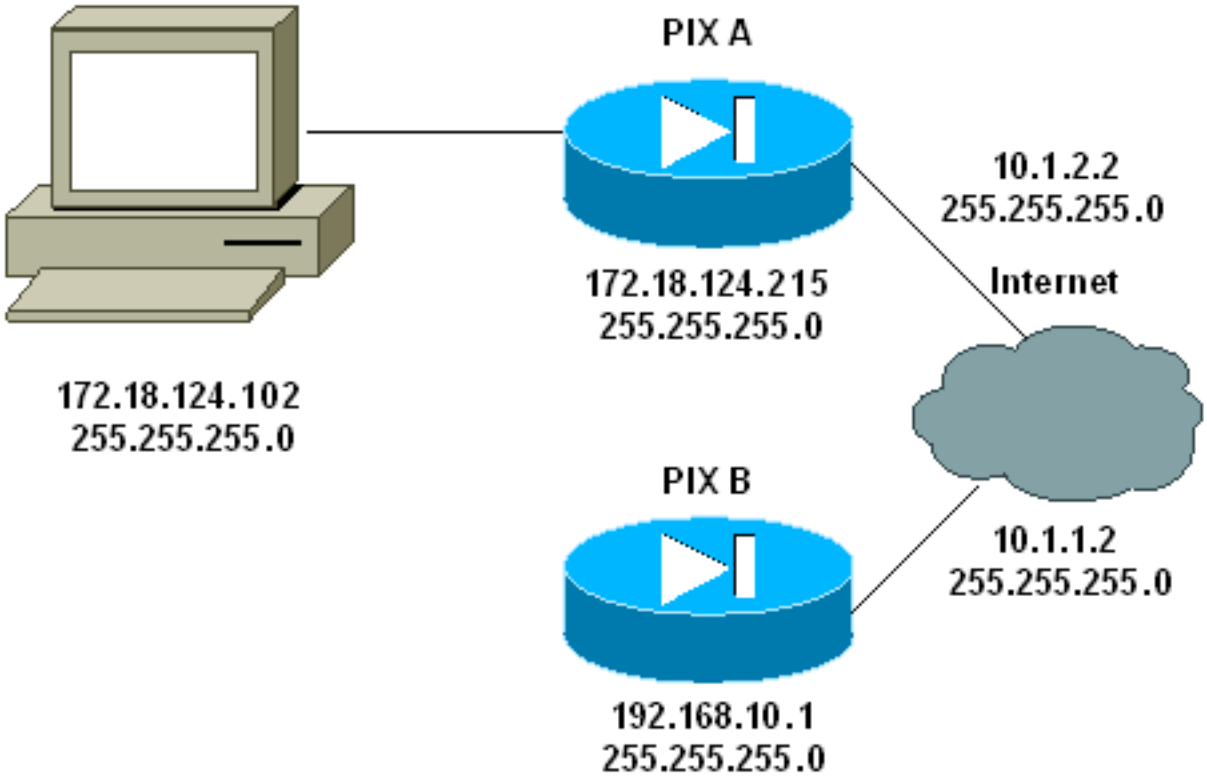
## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota: per** ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

### Esempio di rete

Nel documento viene usata questa impostazione di rete:




## Configurazioni

Nel documento vengono usate queste configurazioni:

- 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)#
```

# Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- show crypto isakmp sa/show isakmp sa: verifica che la fase 1 sia stata stabilita.
- show crypto ipsec sa: verifica che la fase 2 sia stata stabilita.
- show crypto engine: visualizza le statistiche di utilizzo del motore di crittografia utilizzato dal firewall.

## Riepilogo comandi

Una volta inseriti i comandi VPN nei PIX, un tunnel VPN deve stabilire quando il traffico passa tra il PC PDM (172.18.124.102) e l'interfaccia esterna del PIX B (10.1.1.2). A questo punto, il PC PDM è in grado di accedere a https://10.1.1.2 e raggiungere l'interfaccia PDM del PIX B sul tunnel VPN.

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Per la risoluzione dei problemi relativi a PDM, consultare il documento sulla risoluzione dei problemi relativi a PIX Device Manager.

## Output di esempio del comando debug

### show crypto isakmp sa

L'output mostrato di seguito mostra un tunnel formato tra 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

L'output mostrato di seguito mostra un tunnel che attraversa il traffico tra le versioni 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:
```

## Informazioni correlate

- Informazioni di riferimento sui comandi PIX
- Cisco PIX serie 500 Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems