

PIX: Access the PDM from an Outside Interface Over a VPN Tunnel

Document ID: 4719

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

- Command Summary

Troubleshoot

- Sample Debug Output

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This sample configuration documents how to configure a LAN-to-LAN VPN tunnel using two PIX Firewalls. PIX Device Manager (PDM) runs on the remote PIX through the outside interface on the public side and encrypts both regular network and PDM traffic.

PDM is a browser-based configuration tool designed to help you set up, configure, and monitor your PIX Firewall with a GUI. You do not need extensive knowledge of the PIX Firewall command-line interface (CLI).

Prerequisites

Requirements

This document requires a basic understanding of IPsec encryption and PDM.

Ensure that all the devices used in your topology meet the requirements described in Cisco PIX Firewall Hardware Installation Guide, Version 6.3.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco PIX Firewall Software Release 6.3(1) and 6.3(3)
- PIX A and PIX B are Cisco PIX Firewall 515E
- PIX B uses PDM version 2.1(1)

Note: PDM 3.0 does not run with PIX Firewall software versions earlier than Version 6.3. PDM Version 3.0 is a single image that supports only PIX Firewall Version 6.3.

Note: Policy NAT configurations force PDM 3.0 into monitor mode. Policy NAT is supported in PDM version 4.0 and later.

Note: When you are prompted for a username and password for the PIX Device Manager (PDM), the default settings require no username. If an enable password was previously configured, enter that password as the PDM password. If there is no enable password, leave both the username and password entries blank and click **OK** to continue.

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

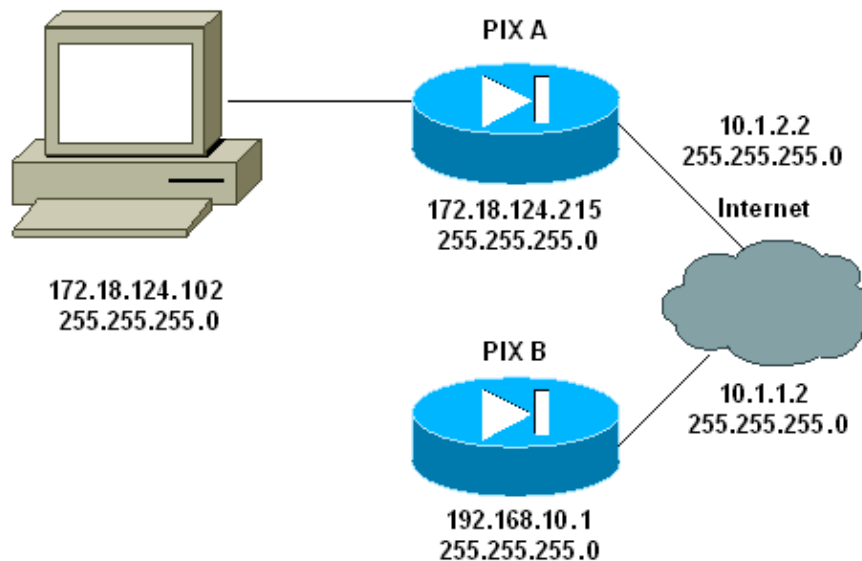
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- 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 8Ry2Yjlyt7RRXU24 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)#
```

Verify

This section provides information you can use to confirm your configuration is working properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto isakmp sa/show isakmp sa** Verifies that phase 1 establishes.
- **show crypto ipsec sa** Verifies that phase 2 establishes.
- **show crypto engine** Displays usage statistics for the cryptography engine that the firewall uses.

Command Summary

Once VPN commands are put into the PIXes, a VPN tunnel should establish when traffic passes between the PDM PC (172.18.124.102) and the outside interface of PIX B (10.1.1.2). At this point, the PDM PC is able to go to <https://10.1.1.2> and reach the PDM interface of PIX B over the VPN tunnel.

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Refer to Troubleshooting PIX Device Manager to troubleshoot PDM related issues.

Sample Debug Output

show crypto isakmp sa

This output shows a tunnel that is formed between 10.1.1.2 and 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

This output shows a tunnel that that passes traffic between 10.1.1.2 and 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:

```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [PIX Command Reference](#)
 - [Cisco PIX 500 Series Security Appliances](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 24, 2006

Document ID: 4719
