

PIX 6.2: NTP with and without an IPsec Tunnel Configuration Example

Document ID: 45400

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Troubleshooting Commands

Related Information

Introduction

This document provides a sample configuration for synchronizing the PIX Firewall's clock with a network time server using Network Time Protocol (NTP). PIX 1 communicates directly with the network time server. PIX 2 passes NTP traffic through an IPsec tunnel to PIX 1, which in turn forwards the packets to the network time server.

Note: A router can also be used as an NTP server to synchronize the clock of the PIX Firewall. Refer to [How to Configure a Router as an NTP Server](#) for more information.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- End-to-end IPsec connectivity must be established before starting this NTP configuration.
- NTP support was added in PIX version 6.2. The PIX Firewall must run version 6.2 or later.
- The PIX Firewall license must be enabled for Data Encryption Standard (DES) encryption (at a minimum encryption level).

Components Used

The information in this document is based on Cisco PIX Firewall Software Release 6.3(3).

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

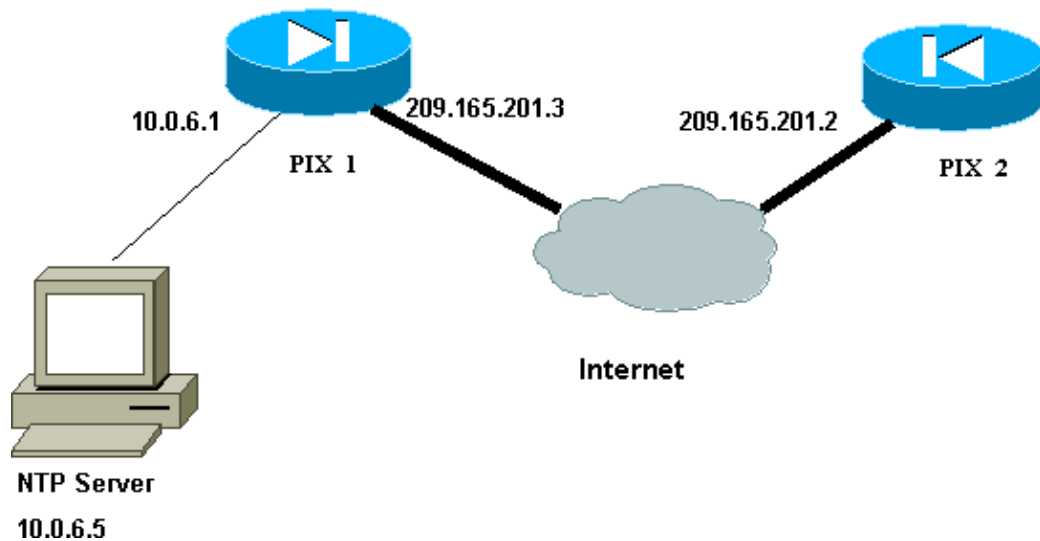
Configure

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

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses the configurations shown here.

- PIX 1 Configuration
- PIX 2 Configuration

PIX 1 Configuration

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz0 security10
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix1
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21<br>fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
```

```
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list nonat permit ip 10.0.6.0 255.255.255.0 host 209.165.201.2
access-list ipsec permit ip 10.0.6.0 255.255.255.0 host 209.165.201.2
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz0 1500
ip address outside 209.165.201.3 255.255.255.224
ip address inside 10.0.6.1 255.255.255.0
no ip address dmz0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address dmz0
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.161 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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
aaa-server LOCAL protocol local
ntp authentication-key 1 md5 *****
ntp trusted-key 1
ntp server 10.0.6.5 key 1 source inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment chain 1
sysopt connection permit-ipsec
crypto ipsec transform-set vpn esp-3des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address ipsec
crypto map cisco 10 set peer 209.165.201.2
crypto map cisco 10 set transform-set vpn
crypto map cisco interface outside
isakmp enable outside
isakmp key ***** address 209.165.201.2 netmask 255.255.255.255
isakmp keepalive 10
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
```

```
terminal width 80
Cryptochecksum:bf28afe92a93af6170d8de380afeb424
: end
```

PIX 2 Configuration

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix2
domain-name vpn.cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list ipsec permit ip host 209.165.201.2 10.0.6.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip address outside 209.165.201.2 255.255.255.224
ip address inside 10.1.1.10 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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
aaa-server RADIUS (inside) host 1.1.1.1 cisco timeout 10
aaa-server LOCAL protocol local
ntp authentication-key 1 md5 *****
ntp trusted-key 1
ntp server 10.0.6.5 key 1 source outside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set vpn esp-3des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address ipsec
```

```

crypto map cisco 10 set peer 209.165.201.3
crypto map cisco 10 set transform-set vpn
crypto map cisco interface outside
isakmp enable outside
isakmp key ***** address 209.165.201.3 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:26d03e15146cf920b3d7ab61eaf75905
: end
[OK]
pix2(config)#

```

Verify

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

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show ntp status** Displays the NTP clock information.

```

pix1#show ntp status
Clock is synchronized, stratum 9, reference is 10.0.6.5
  nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
  reference time is af99ca9d.ab979ef4 (06:47:57.670 UTC Tue May 11 1993)
  clock offset is -27.3950 msec, root delay is 1.04 msec
  root dispersion is 7906.14 msec, peer dispersion is 7878.71 msec

```

- **show ntp associations [detail]** Displays the configured network time server associations.

```

pix1#show ntp associations detail
10.0.6.5 configured, authenticated, our_master, sane, valid, stratum 8
  ref ID 127.127.7.1, time af99cb13.44a14229 (06:49:55.268 UTC Tue May 11 1993)
  our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
  root delay 0.00 msec, root disp 0.03, reach 17, sync dist 2123.413
  delay 1.07 msec, offset -311.1441 msec, dispersion 2122.85
  precision 2**18, version 3
  org time af99cb1d.53083e9b (06:50:05.324 UTC Tue May 11 1993)
  rcv time af99cb1d.a2d2a9b5 (06:50:05.636 UTC Tue May 11 1993)
  xmt time af99cb1d.a27b176f (06:50:05.634 UTC Tue May 11 1993)
  filtdelay =   1.07   1.05   1.04   1.04   0.00   0.00   0.00   0.00
  filtoffset = -311.14 -30.13 -27.39 -19.99   0.00   0.00   0.00   0.00
  filterror =   0.02   0.99   1.97   2.94 16000.0 16000.0 16000.0 16000.0

```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

- **debug ntp validity** Displays NTP peer clock validity.

This is **debug** output from the key mismatch:

```
NTP: packet from 10.0.6.5 failed validity tests 10
      Authentication failed
```

- **debug ntp packet** Displays NTP packet information.

When there is no response from the server, only the NTP `xmit` packet is seen on the PIX with no NTP `rcv` packet.

```
NTP: xmit packet to 10.0.6.5:
  leap 0, mode 3, version 3, stratum 9, ppoll 64
  rtdel 0077 (1.816), rtdsp 3e290 (3885.010), refid 0a000605 (10.0.6.5)
  ref c3390a82.f50ac415 (12:16:02.957 UTC Thu Oct 16 2003)
  org c3390a82.f70e3cc7 (12:16:02.965 UTC Thu Oct 16 2003)
  rec c3390a82.f50ac415 (12:16:02.957 UTC Thu Oct 16 2003)
  xmt c3390ac2.f6363336 (12:17:06.961 UTC Thu Oct 16 2003)
NTP: rcv packet from 10.0.6.5 to 209.165.201.2 on ntp0:
  leap 0, mode 4, version 3, stratum 8, ppoll 64
  rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 7f7f0701 (127.127.7.1)
  ref c3390ac0.65629071 (12:17:04.396 UTC Thu Oct 16 2003)
  org c3390ac2.f6363336 (12:17:06.961 UTC Thu Oct 16 2003)
  rec c3390ac2.f8c541ec (12:17:06.971 UTC Thu Oct 16 2003)
  xmt c3390ac2.f8d6f76f (12:17:06.972 UTC Thu Oct 16 2003)
  inp c3390ac3.5d1f1568 (12:17:07.363 UTC Thu Oct 16 2003)
```

Related Information

- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support – Cisco Systems](#)

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 19, 2008

Document ID: 45400
