

Handle VoIP Traffic with the PIX Firewall

Document ID: 48583

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

- Verify H.323
- Verify the SIP

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

In this sample configuration, a PIX Firewall is configured in order to allow the traversal of two different Voice over IP (VoIP) protocols H.323, and Session Initiation Protocol (SIP). Due to the fact that VoIP protocols are made up of signaling and IP address/port combinations, there are a number of issues with VoIP and Network Address Translations (NAT). The PIX Firewall fixup protocol addresses these issues.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- PIX Software Release 6.3.1
- Cisco 2651XM IOS® 12.3(3)
- Cisco Analog Telephone Adaptor (ATA) 186 version 2.16.1

Note: For PIX Firewall (with VoIP application–layer gateway [ALG] or fixup protocol), these version/feature combinations are supported:

- **Version 5.2** Supports H.323 version 2, Registration and Status (RAS), and NAT (no PAT)
- **Version 6.0 and 6.1** Adds SIP with NAT (no PAT), Skinny Client Control Protocol (SCCP) with NAT (no PAT), and no Media Gateway Control Protocol (MGCP) support
- **Version 6.2** PAT support for H.323 version 2 and SIP.

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.

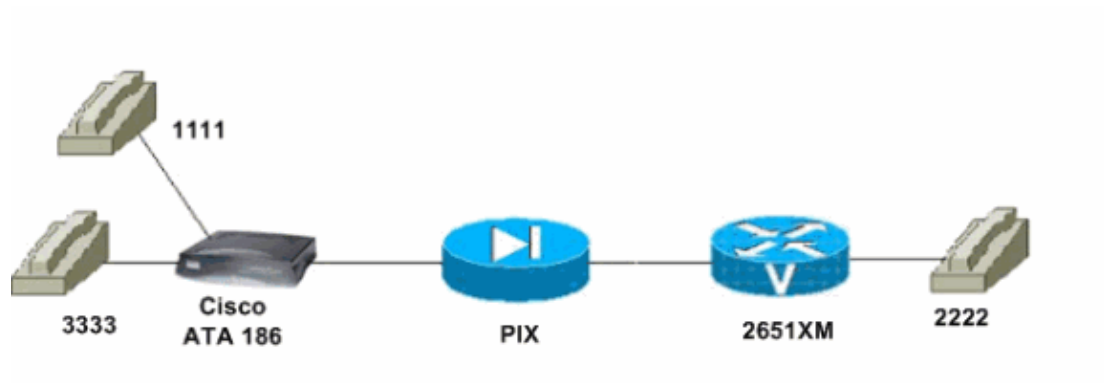
Configure

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:

- Cisco PIX Firewall
- Cisco 2651
- Cisco ATA 186

```
Cisco PIX Firewall

PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719

!--- Fixup protocol required for H.323.

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 required for SIP.

fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit tcp host 100.1.1.2 host 100.1.1.5 eq h323

!--- Permits inbound H.323 calls.

access-list 101 permit tcp host 100.1.1.2 host 100.1.1.5 eq 5060

!--- Permits inbound SIP calls.

pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 100.1.1.1 255.255.255.0
ip address inside 192.168.0.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
static (inside,outside) 100.1.1.5 192.168.0.2 netmask 255.255.255.255 0 0

!--- Static used to demonstrate NAT.

access-group 101 in interface outside
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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
pixfirewall#

```

Cisco 2651

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!

```

```
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
interface FastEthernet0/0
ip address 100.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
no ip http server
ip classless
!
!
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
!
!
!
!
dial-peer voice 1111 voip
destination-pattern 1111
session target ipv4:100.1.1.5
codec g711ulaw
!

!--- H.323 dial-peer

dial-peer voice 2222 pots
destination-pattern 2222
port 1/0/0
!
dial-peer voice 3333 voip
destination-pattern 3333
session protocol sipv2
session target ipv4:100.1.1.5
codec g711ulaw
!

!--- SIP dial-peer

!
line con 0
line aux 0
```

```

line vty 0 4
!
!
!
end
Gateway#

```

Cisco ATA 186

Note: This ATA 186 configuration applies for outgoing calls that use SIP. For H.323 calls the UseSIP field needs to be changed to **0** and the IP address of the 2651XM (100.1.1.2) changed from GkOrProxy to the **Gateway** field.

UIPassword:	*	ToConfig:	1
UseTftp:	0	TftpURL:	0
CfgInterval:	3600	EncryptKey:	*
Dhcp:	0	StaticIP:	192.168.0.2
StaticRoute:	192.168.0.1	StaticNetMask:	255.255.255.0
UID0:	1111	PWDO:	*
UID1:	3333	PWD1:	*
GkOrProxy:	100.1.1.2	Gateway:	0
GateWay2:	0.0.0.0	UseLoginID:	0
LoginID0:	0	LoginID1:	0
AltGk:	0	AltGkTimeOut:	0
GkTimeToLive:	300	GkId:	.
UseSIP:	1	SIPRegInterval:	3600
MaxRedirect:	5	SIPRegOn:	0
NATIP:	0.0.0.0	SIPPort:	5060
MediaPort:	16384	OutBoundProxy:	0
NatServer:	0	NatTimer:	0x00000000
LBRCodec:	3	AudioMode:	0x00150015
RxCodec:	1	TxCodec:	1

Verify

Use this section to confirm that your configuration works 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 xlate** Displays the translation that takes place.

```

pixfirewall#show xlate
1 in use, 1 most used
Global 100.1.1.5 Local 192.168.0.2

!--- Translation in place

```

Verify H.323

Use these commands in order to verify the H.323:

- **show call active voice brief** Displays the contents of the active call table. The information presented includes call times, dial peers, connections, quality of service parameters, and gateway handling of jitter.
- **show h225** Displays calls that go through the PIX Firewall.
- **show conn detail** Displays the NAT of both the VoIP signaling and media addresses.

This is the output of the **show call active voice brief** command.

```

Gateway#show call active voice brief

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
2828 : 1574769hs.1 +142 pid:1111 Answer 1111 active
dur 00:00:06 tx:159/24803 rx:343/54880
IP 100.1.1.5:16384 rtt:0ms pl:3860/0ms lost:0/1/0 delay:64/64/65ms g711ulaw

2828 : 1574770hs.1 +141 pid:2222 Originate 2222 active
dur 00:00:06 tx:343/54880 rx:167/26083
Tele 1/0/0 (48): tx:8200/3290/0ms g711ulaw noise:-50 acom:13 i/0:-42/-55 dBm

```

This is the output of the **show h225** command.

```

pixfirewall#show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
Local: 192.168.0.2/16230 Foreign: 100.1.1.2/1720
1. CRV 5735
Local: 192.168.0.2/16230 Foreign: 100.1.1.2/1720

!--- This output indicates that there is currently one active
!--- H.323 call going through the PIX Firewall between the local
!--- endpoint 192.168.0.2 and foreign host 100.1.1.2. For these
!--- particular endpoints, there is one concurrent call between them,
!--- with a Call Reference Value (CRV) for that call of 5735.

```

This is the output of the **show conn detail** command.

```

pixfirewall#show conn detail
7 in use, 12 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
E - outside back connection, F - outside FIN, f - inside FIN,

```

G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data, i - incomplete, k - Skinny media, M - SMTP data, m - SIP media, O - outbound data, P - inside back connection, q - SQL*Net data, R - outside acknowledged FIN, R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN, s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
 UDP outside:100.1.1.2/17047 inside:192.168.0.2/16385 flags **H**
 UDP outside:100.1.1.2/17046 inside:192.168.0.2/16384 flags **H**
 TCP outside:100.1.1.2/1720 inside:192.168.0.2/14785 flags **UIOh**
 UDP outside:100.1.1.2/0 inside:192.168.0.2/16384 flags **Hi**
 TCP outside:100.1.1.2/11012 inside:192.168.0.2/14793 flags **UIO**
 TCP outside:100.1.1.2/11012 inside:192.168.0.2/0 flags **ssiaA**
 TCP outside:100.1.1.2/11012 inside:192.168.0.2/0 flags **ssiaA**

Verify the SIP

Use these commands in order to verify the SIP.

- **show call active voice brief** Displays the contents of the active call table. The information presented includes call times, dial peers, connections, quality of service parameters, and gateway handling of jitter.
- **show conn detail** Displays the NAT of both the VoIP signaling and media addresses.
- **show sip** Displays an active SIP call.

This is the output of the **show call active voice brief** command.

```
Gateway#show call active voice brief

Telephony call-legs: 1
SIP call-legs: 1
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1210 : 1589226hs.1 +133 pid:1111 Answer 1111 active
dur 00:00:13 tx:344/53687 rx:639/102001
IP 100.1.1.5:16384 rtt:0ms pl:11420/0ms lost:0/1/0 delay:45/45/65ms g711ulaw

1210 : 1589227hs.1 +132 pid:2222 Originate 2222 active
dur 00:00:13 tx:639/102001 rx:344/53687
Tele 1/0/0 (50): tx:14760/6780/0ms g711ulaw noise:-49 acom:13 i/0:-45/-50 dBm
```

This is the output of the **show sip** command.

```
pixfirewall#show sip
Total: 1
call-id 648032863@192.168.0.2
state Active, idle 0:00:58
```

This is the output of the **show conn detail** command.

```
pixfirewall#show conn detail
7 in use, 12 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
E - outside back connection, F - outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data, i - incomplete,
k - Skinny media, M - SMTP data, m - SIP media, O - outbound data,
P - inside back connection, q - SQL*Net data, R - outside acknowledged FIN,
R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
UDP outside:100.1.1.2/5060 inside:192.168.0.2/0 flags ti
UDP outside:100.1.1.2/0 inside:192.168.0.2/5060 flags Tti
```

```
UDP outside:100.1.1.2/0 inside:192.168.0.2/16384 flags mi
UDP outside:100.1.1.2/5060 inside:192.168.0.2/5060 flags Tt
UDP outside:100.1.1.2/17490 inside:192.168.0.2/16384 flags m
UDP outside:100.1.1.2/17491 inside:192.168.0.2/0 flags m
UDP outside:100.1.1.2/17490 inside:192.168.0.2/0 flags mi
```

Troubleshoot

Troubleshooting Commands

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

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Use these **debug** commands to troubleshoot the PIX.

- **debug sip** Displays the SIP messages generated from the gateways.
- **debug h323 h225 asn1** Displays the H.225 message generated from the gateways.
- **debug** Displays the traffic that is encrypted.

Use these **debug** commands in order to troubleshoot the Cisco IOS gateway.

- **debug voip ccapi inout** Displays the call setup and teardown operations performed on both the telephony and network call legs.
- **debug h225 asn1** Displays the ASN.1 contents of any H.225 message sent or received.

Refer to Cisco ATA 186 Troubleshooting for details on ATA 186 debugging.

Related Information

- [PIX 500 Series Security Appliances Support Page](#)
- [Documentation for PIX Firewall](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – 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: Sep 26, 2008

Document ID: 48583
