

Configuring the PIX Firewall with Mail Server Access on Inside Network

Document ID: 8122

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Network Diagram

- Configurations

Verify

Troubleshoot

Information to Collect if You Open a Technical Support Case

Related Information

Introduction

This sample configuration demonstrates how to set up the PIX Firewall for access to a mail server located on the inside network.

Note: The SMTP inspection configured in this document is not compatible with ESMTP connections to servers such as Microsoft Exchange. Do not configure SMTP inspection if you use a mail server that relies on ESMTP. Alternatively, PIX Software version 7.0 and later supports SMTP and ESMTP inspection.

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 Firewall 10000
- PIX Firewall software release 5.1(4)

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 the Cisco Technical Tips Conventions for more information on document conventions.

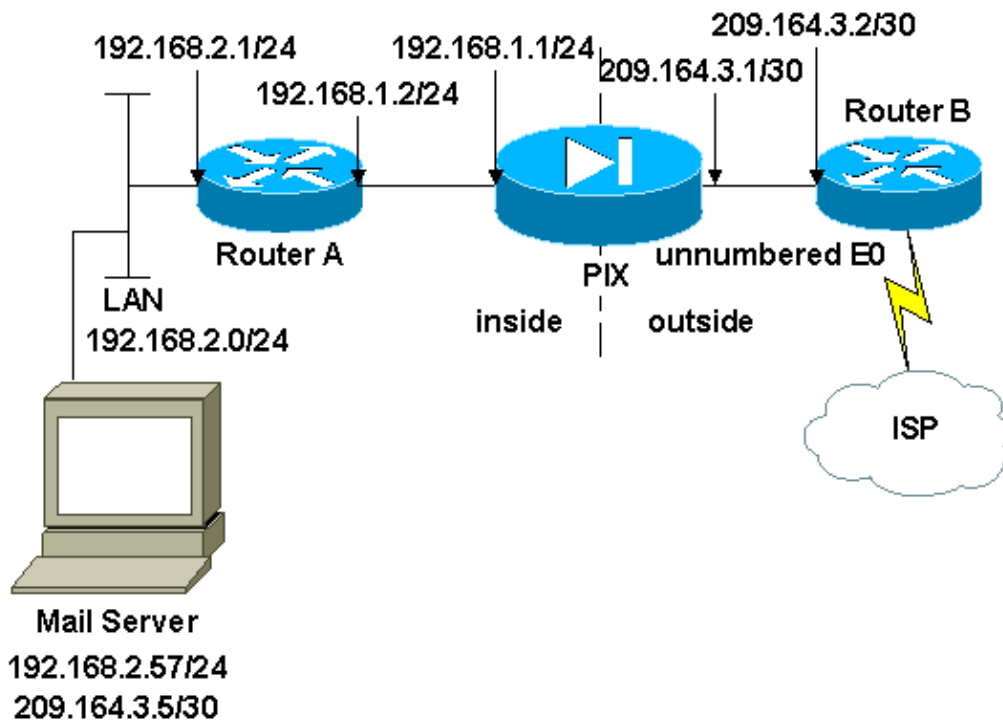
Configure

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 Firewall
- Router

PIX Firewall

```
PIX Version 5.1(4)
```

```
!--- These commands name and set the security level for each PIX interface.
```

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX_1
domain-name noplace.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
no names

!--- Create an access list that permits SMTP traffic from anywhere
!--- to the host at 209.164.3.5 (our server). The name of this list is
!--- smtp. Add additional lines to this access list as required.
!--- Note: There is one and only one access list allowed per
!--- interface per direction (for example, inbound on the outside interface).
!--- Because of limitation, any additional lines that need placement in
!--- the access list need to be specified here. If the server
!--- in question is not SMTP, replace the occurrences of SMTP with
!--- www, DNS, POP3, or whatever else is required. The access-list
!--- command was introduced in PIX Software Release 5.0; it is used
!--- here instead of a conduit statement.

access-list smtp permit tcp any host 209.164.3.5 eq smtp
pager lines 24
logging on
logging timestamp
no logging standby
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging
no logging history
logging facility 23
logging queue 512

!--- Set each Ethernet interface to auto-detect its media type.

interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500

!--- Define the IP address for each interface.

ip address inside 192.168.1.1 255.255.255.0
ip address outside 209.164.3.1 255.255.255.252
no failover
arp timeout 14400

!--- Specify that any traffic that originates inside from the
!--- 192.168.2.x network NATs (PAT) to 209.164.3.129 if
!--- such traffic passes through the outside interface.

global (outside) 1 209.164.3.129
nat (inside) 1 192.168.2.0 255.255.255.0

!--- Define a static translation between 192.168.2.57 on the inside and
!--- 209.164.3.5 on the outside. These are the addresses to be used by
!--- the server located inside the firewall.

static (inside,outside) 209.164.3.5 192.168.2.57 netmask 255.255.255.255

!--- Apply the access list named smtp inbound on the outside interface.

access-group smtp in interface outside

!--- Set the default route to 209.164.3.2.
!--- The PIX assumes that this address is that of a router.

route outside 0.0.0.0 0.0.0.0 209.164.3.2 1

!--- Instruct the PIX to hand any traffic destined for 192.168.x.x

```

```

!--- to the router at 192.168.1.2.

route inside 192.168.0.0 255.255.0.0 192.168.1.2 1
timeout xlate 1:30:00 conn 1:00:00 half-closed 0:10:00 udp 0:00:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
terminal width 200
Cryptochecksum:d66eb04bc477f21ffbd5baa21ce0f85a
: end

!--- Alternate command:
!--- conduit permit tcp host 209.164.3.5 eq smtp any
!--- The conduit command is equivalent to
!--- the access-list statements this configuration shows.
!--- In this case a path known as a conduit is created in order to allow any SMTP
!--- traffic to host 209.164.3.5. Use of this command replaces the
!--- access-list and access-group
!--- statements that this configuration presents.

```

Router

```

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2522-R5
!
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
!
ip subnet-zero
!
!
!
!
interface Ethernet0

!--- Sets the IP address of the Ethernet interface to 209.164.3.2.

ip address 209.164.3.2 255.255.255.252
!
interface Serial0

!--- Instructs the serial interface to use
!--- the address of the Ethernet interface when the need arises.

ip unnumbered ethernet 0
!
interface Serial1
no ip address
no ip directed-broadcast
!
ip classless

```

```
!--- Instructs the router to send all traffic
!--- destined for 209.164.3.x to 209.164.3.1.

ip route 209.164.3.0 255.255.255.0 209.164.3.1

!--- Instructs the router to send
!--- all other remote traffic out serial 0.

ip route 0.0.0.0 0.0.0.0 serial 0
!
!
line con 0
  transport input none
line aux 0
  autoselect during-login
line vty 0 4
  exec-timeout 5 0
  password ww
  login
!
end
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

The **logging console debugging** command directs messages to the PIX console. If connectivity to the mail server is a problem, examine the console debug messages to locate the IP addresses of the sending and receiving stations in order to determine the problem.

Information to Collect if You Open a Technical Support Case

If you still need assistance after you complete the troubleshooting steps in this document and want to open a case with Cisco Technical Support, be sure to include this information for troubleshooting your PIX Firewall.

- Problem description, which includes topology and IP address details of the mail server.
- Complete any troubleshooting before you open the case.
- Output from the **show tech-support** command.
- Output from the **show log** command after it runs with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available)

Attach the collected data to your case in non-zipped, plain text format (.txt). You can attach information to your case by uploading it with the TAC Service Request Tool (registered customers only) . If you cannot access the TAC Service Request Tool, you can send the information in an E-mail attachment to attach@cisco.com with your case number in the subject line of

your message.

Related Information

- [Documentation for PIX Firewall](#)
 - [Establishing Connectivity Through Cisco PIX Firewalls](#)
 - [PIX Command Reference](#)
 - [PIX Support Page](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support – Cisco Systems](#)
-

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

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 30, 2008

Document ID: 8122
