

Configuring PIX Firewall with Mail Server Access on the DMZ

Document ID: 12430

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Network Diagram

- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This sample configuration demonstrates how to set up the PIX Firewall for access to a mail server located on the DMZ 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 prerequisites for this document.

Components Used

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

- PIX Firewall 515
- PIX Firewall software release 6.3(3)
- Cisco 3640 Router

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.

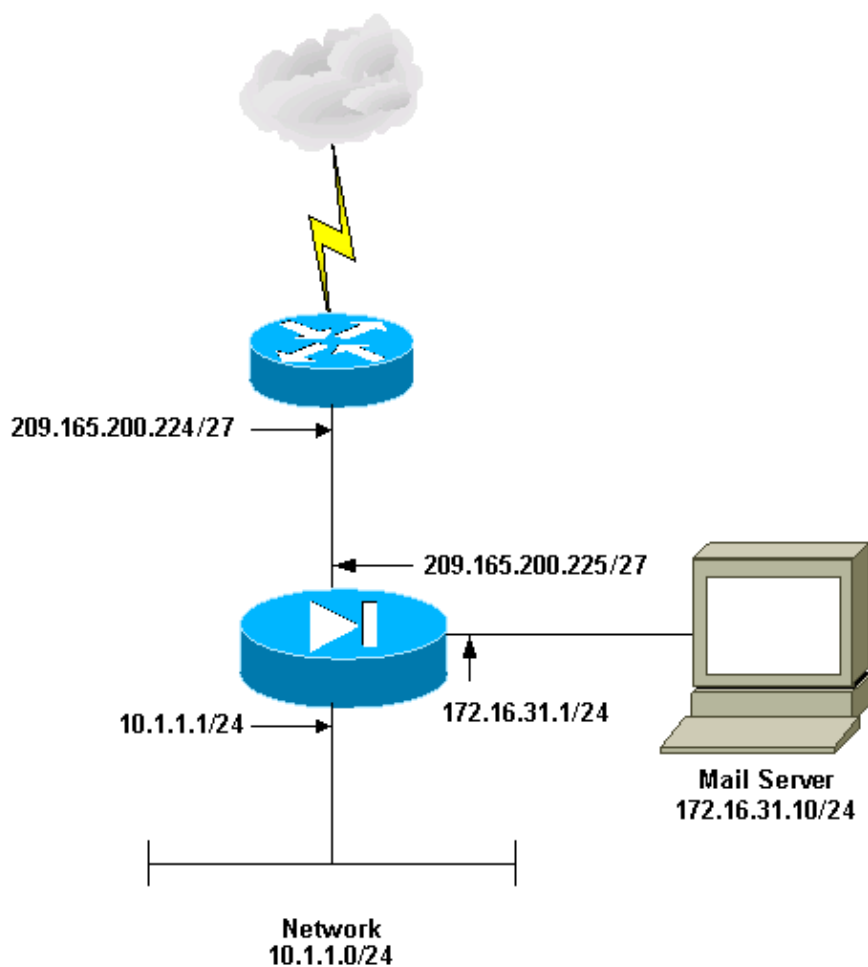
Configure

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 this configuration.

PIX Configuration
<pre>PIX Version 6.3(3) interface ethernet0 10baset interface ethernet1 10baset interface ethernet2 100full nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 dmz security10 enable password 2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pixfirewall</pre>

```

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 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

!--- This access list allows hosts to access
!--- IP address 209.168.200.227 for the SMTP port.

access-list outside_int permit tcp any host 209.165.200.227 eq smtp

!--- This access list allows host IP 172.16.31.10
!--- sourcing the SMTP port to access any host.

access-list dmz_int permit tcp host 172.16.31.10 eq smtp any
pager lines 24
logging on
logging buffered debugging
logging trap debugging
logging host inside 10.1.1.55
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 209.165.200.225 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0
ip address dmz 172.16.31.1 255.255.255.0
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 dmz
pdm history enable
arp timeout 14400
global (outside) 1 209.165.200.228-209.165.200.253 netmask 255.255.255.224
global (outside) 1 209.165.200.254
nat (inside) 1 10.1.1.0 255.255.255.0 0 0

!--- This network static does not use address translation.
!--- Inside hosts appear on the DMZ with their own addresses.

static (inside,dmz) 10.1.1.0 10.1.1.0 netmask 255.255.255.0 0 0

!--- This network static uses address translation.
!--- Hosts accessing the mail server from the outside
!--- use the 209.165.200.227 address.

static (dmz,outside) 209.165.200.227 172.16.31.10 netmask 255.255.255.255 0 0
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0 209.165.200.226 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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
crypto map mymap 30 ipsec-isakmp
! Incomplete
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:8c1aa55b41d6855f6745e04ce6eea614
: end
[OK]
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

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.

- **debug icmp trace** Shows whether Internet Control Message Protocol (ICMP) requests from the hosts reach the PIX. In order to run this debug, you need to add the **access-list** command to permit ICMP in your configuration.
- **logging buffer debugging** Shows connections that are established and denied to hosts that go through the PIX. The information is stored in the PIX log buffer, and the output can be seen with the **show log** command.

Refer to Setting Up the PIX Syslog for more information on how to set up logging.

Related Information

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

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

