

PIX/ASA 7.x and above: Mail (SMTP) Server Access on the DMZ Configuration Example

Document ID: 69374

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- PIX Configuration
- ESMTP TLS Configuration

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This sample configuration demonstrates how to set up the PIX/ASA Security Appliance for access to a mail/SMTP server located on the Demilitarized Zone (DMZ) network.

Refer to PIX/ASA 7.x and above: Mail Server Access on Inside Network Configuration Example for instructions on how to set up the PIX/ASA Security Appliance for access to a mail/SMTP server located on the Inside network.

Refer to PIX/ASA 7.x with Mail Server Access on Outside Network Configuration Example for instructions on how to set up the PIX/ASA Security Appliance for access to a mail/SMTP server located on the Outside network.

Refer to ASA 8.3 and Later: Mail (SMTP) Server Access on the DMZ Configuration Example for more information on the identical configuration on Cisco Adaptive Security Appliance (ASA) with version 8.3 and later.

Note: Refer to Cisco Documentation for Cisco Secure PIX Firewall for more information on how to set up Microsoft Exchange. Choose your software version, then go to the configuration guide and read the chapter on configuring Microsoft Exchange.

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 535
- PIX Firewall software release 7.1(1)

Note: The PIX 500 Series version 7.x/8.x runs the same software seen in ASA 5500 Version 7.x/8.x. The configurations in this document apply to both product lines.

- Cisco 2600 router
- Cisco IOS® Software Release 12.3.14T

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.

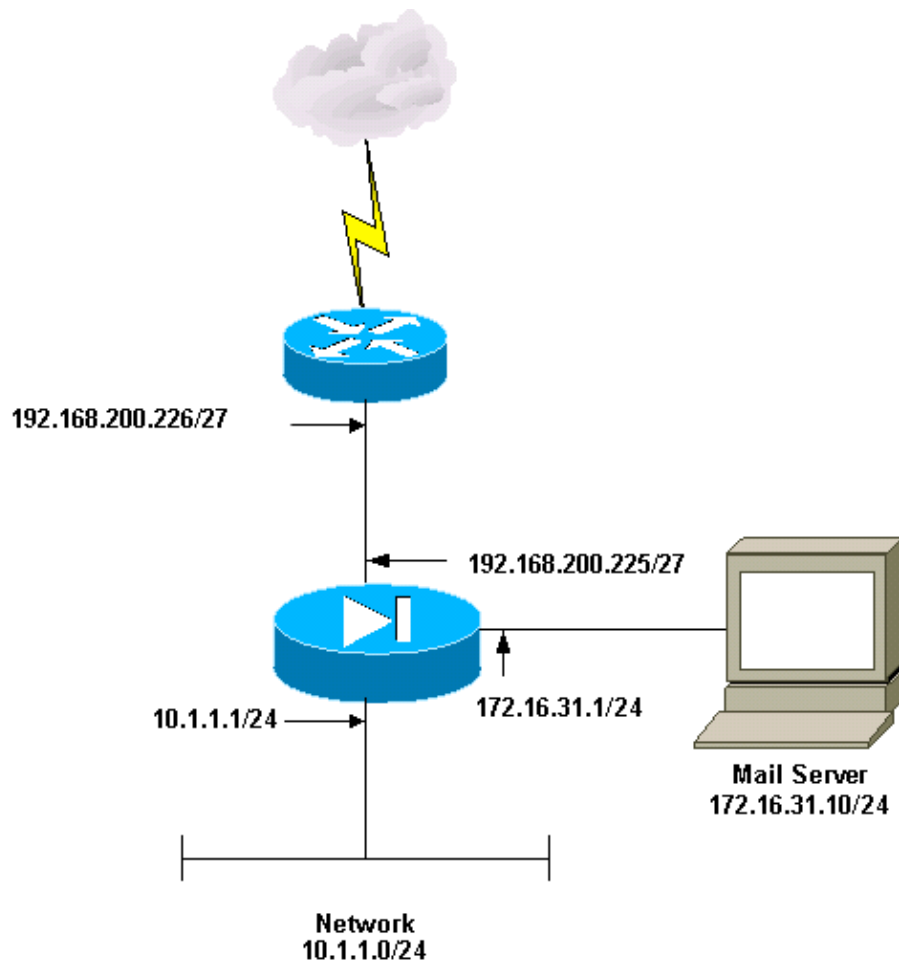
Configure

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:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

PIX Configuration

This document uses this configuration:

PIX Configuration
<pre> PIX Version 7.1(1) ! hostname pixfirewall enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0 shutdown nameif BB security-level 0 no ip address ! interface Ethernet1 shutdown no nameif no security-level no ip address ! interface Ethernet2 no nameif no security-level </pre>

```

no ip address
!
interface Ethernet3
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet4
 nameif outside
 security-level 0
 ip address 192.168.200.225 255.255.255.224
!
interface Ethernet5
 nameif dmz
 security-level 10
 ip address 172.16.31.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system flash:/pix711.bin
ftp mode passive

!--- This access list allows hosts to access
!--- IP address 192.168.200.227 for the
!--- Simple Mail Transfer Protocol (SMTP) port.

access-list outside_int extended permit tcp any host 192.168.200.227 eq smtp

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

access-list dmz_int extended permit tcp host 172.16.31.10 any eq smtp

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400
global (outside) 1 192.168.200.228-192.168.200.253 netmask 255.255.255.224
global (outside) 1 192.168.200.254
nat (inside) 1 10.1.1.0 255.255.255.0

!--- 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

!--- This network static uses address translation.
!--- Hosts accessing the mail server from the outside
!--- use the 192.168.200.227 address.

static (dmz,outside) 192.168.200.227 172.16.31.10 netmask 255.255.255.255
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0 192.168.200.226 1

```

```

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
!--- The inspect esmtp command (included in the map) allows
!--- SMTP/ESMTP to inspect the application.

policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
  !
!--- The inspect esmtp command (included in the map) allows
!--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
: end
[OK]

```

ESMTP TLS Configuration

Note: If you use Transport Layer Security (TLS) encryption for e-mail communication then the ESMTP inspection feature (enabled by default) in the PIX drops the packets. In order to allow the e-mails with TLS enabled, disable the ESMTP inspection feature as this output shows. Refer to Cisco bug ID CSCtn08326 (registered customers only) for more information.

```

pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(config-pmap)#exit

```

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. You need to add the **access-list** command to permit ICMP in your configuration in order to run this debug.

Note: In order to use this debug, make sure you allow ICMP in the `access-list outside_int` as this output shows:

```
access-list outside_int extended permit tcp any host 192.168.200.227 eq smtp
access-list outside_int extended permit icmp any any
```

- **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 PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – 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: Oct 01, 2006

Document ID: 69374
