

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

Document ID: 70031

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions
- Related Products

Configure

- Network Diagram
- Configurations
- ESMTP TLS Configuration
- Regulate Email Flows

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/ASA Security Appliance for access to a mail (SMTP) server located on the inside network.

Refer to PIX/ASA 7.x and above: Mail (SMTP) Server Access on the DMZ Configuration Example for more information on how to set up the PIX/ASA Security Appliance for access to a mail/SMTP server located on the DMZ network.

Refer to PIX/ASA 7.x with Mail Server Access on Outside Network Configuration Example 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 Inside Network Configuration Example for more information on the identical configuration on Cisco Adaptive Security Appliance (ASA) with version 8.3 and later.

Note: Refer to the Cisco Secure PIX Firewall documentation for more information to learn more on how to configure for Microsoft Exchange. Choose your software version, then go to the configuration guide and read the chapter on how to configure for 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 Security Appliance 535
- PIX Firewall software release 7.1(1)
- Cisco 2500 Series Routers

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.

Related Products

This document can also be used with the Cisco 5500 Series Adaptive Security Appliance (ASA) with Software Version 7.x and later.

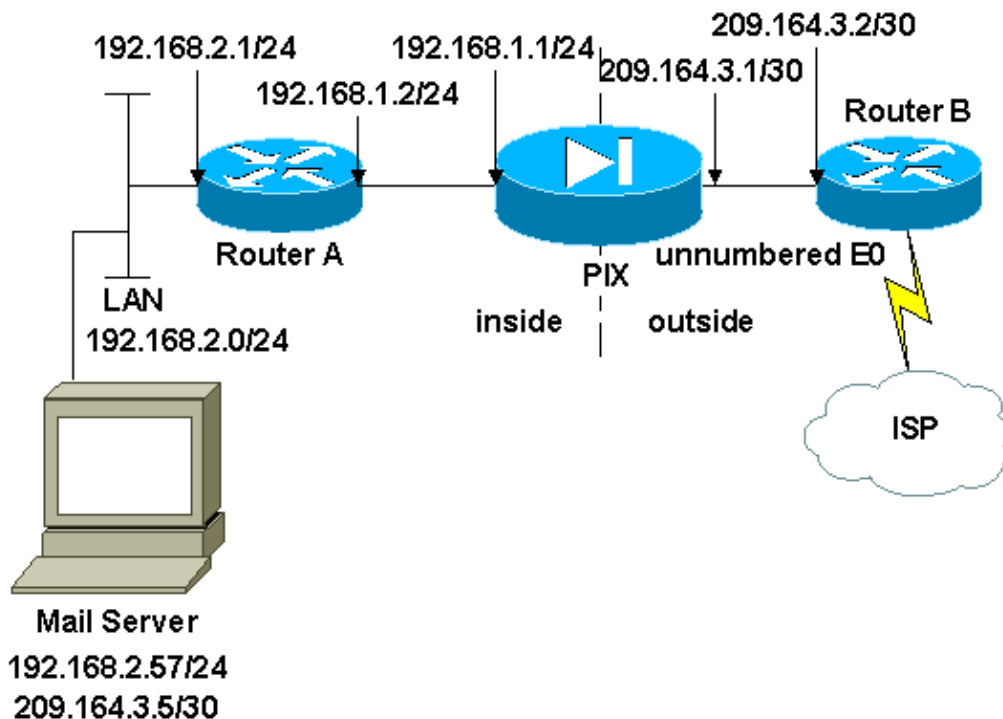
Configure

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 –Security Appliance
- Router B

PIX Firewall

```
PIX Version 7.1(1)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!

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

interface Ethernet3
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!

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

interface Ethernet4
 nameif outside
 security-level 0
 ip address 209.164.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

!--- Create an access list that permits Simple
!--- Mail Transfer Protocol (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.
```

```
access-list smtp extended permit tcp any host 209.164.3.5 eq smtp
```

```
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
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 PIX 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
```

```
!--- 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
```

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

```
route outside 0.0.0.0 0.0.0.0 209.164.3.2 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
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
```

```

!
!--- SMTP/ESMTP is inspected as "inspect esmtp" is included in the map.

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
!

!--- SMTP/ESMTP is inspected as "inspect esmtp" is included in the map.

service-policy global_policy global
Cryptochecksum:f96eaf0268573bd1af005e1db9391284
: end

```

Router B

```

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

```

Note: The Router A configuration is not added. You only have to give the IP addresses on the interfaces and set the default gateway to 192.168.1.1, which is the inside interface of the PIX Firewall.

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

```

Note: In ASA version 8.0.3 and later, the **allow-tls** command is available to allow TLS email with inspect esmtp enabled as shown:

```

policy-map type inspect esmtp tls-esmtp
parameters
  allow-tls
inspect esmtp tls-esmtp

```

Regulate Email Flows

If the volume of emails comes in too fast for the internal server, you can use the **static** command in order to throttle down the PIX to allow a limited number of emails (connections) at a time.

This is an example :

```
static (inside,outside) 209.164.3.5 192.168.2.57 netmask 255.255.255.255 60 0
```

This static command example is taken from the PIX Configuration. This command limits the maximum number of connections to 60 for emails.

The maximum number of simultaneous TCP connections that the local IP hosts are to allow is 0, the default, which means unlimited connections. Idle connections are closed after the time specified by the **timeout conn** command.

Note: If there are intermittent connectivity issues with mail server, make sure that the **sysopt noproxyarp inside** command is present in the configuration. Otherwise, add it to the configuration. Refer to Cisco Security Appliance Command Reference, Version 8.0 for more information about this command.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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.

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 to troubleshoot 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

- **Establishing Connectivity Through Cisco PIX Firewalls**
- **Cisco Secure PIX Firewall Documentation**
- **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](#)

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

Updated: Dec 21, 2011

Document ID: 70031
