

PIX/ASA 7.x with Mail Server Access on Outside Network Configuration Example

Document ID: 70029

Introduction

Prerequisites

Requirements

Components Used

Conventions

Related Products

Configure

Network Diagram

Configurations

ESMTP TLS Configuration

Verify

Troubleshoot

Related Information

Introduction

This sample configuration demonstrates how to set up the PIX Firewall for access to a mail server located on the outside network. Refer to the Cisco Secure PIX Firewall documentation for further information about how to set 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 Firewall 535
- PIX Firewall software release 7.1(1)
- Cisco 2500 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 configuration can also be used with an Adaptive Security Appliance (ASA) that runs version 7.x and later.

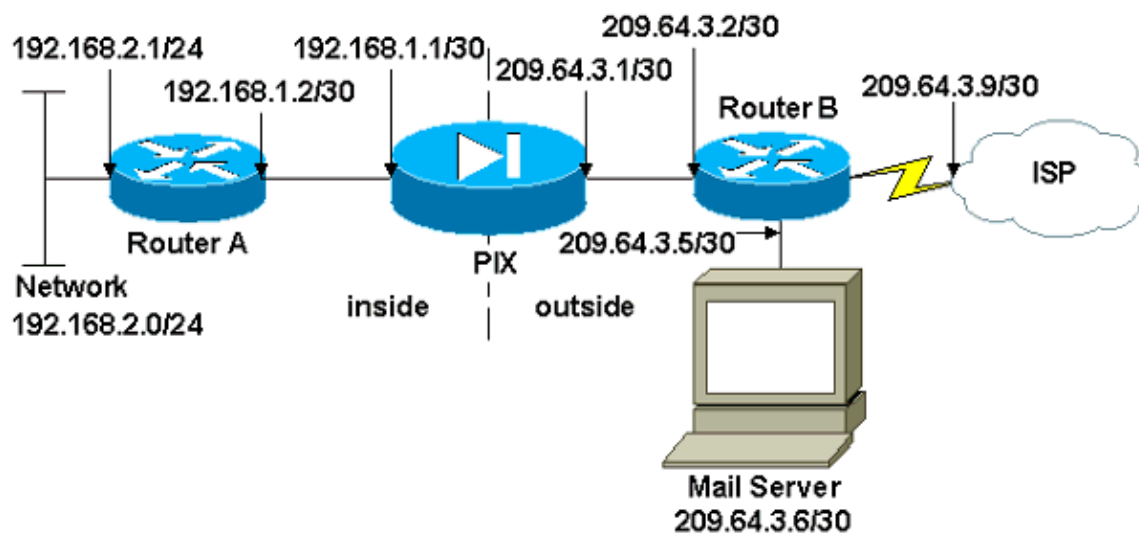
Configure

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 Firewall
- Router A
- 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 192.168.1.1 255.255.255.252
!

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

interface Ethernet4
nameif outside
security-level 0
ip address 209.64.3.1 255.255.255.252
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- This command defines the global for the Network Address Translation
!--- (NAT) statement. In this case, the two commands state that any traffic
!--- from the 192.168.2.x network that passes from the inside interface (Ethernet0)
!--- to the outside interface (Ethernet 1) translates into an address
!--- in the range of 209.64.3.129 through 209.64.3.253 and contains a subnet
!--- mask of 255.255.255.128.

global (outside) 1 209.64.3.129-209.64.3.253 netmask 255.255.255.128

!--- This command reserves the last available address (209.64.3.254) for
!--- for Port Address Translation (PAT). In the previous statement,
!--- each address inside that requests a connection uses one
!--- of the addresses specified. If all of these addresses are in use,
!--- this statement provides a failsafe to allow additional inside stations
!--- to establish connections.

global (outside) 1 209.64.3.254
```

```
!--- This command indicates that all addresses in the 192.168.2.x range  
!--- that pass from the inside (Ethernet0) to a corresponding global  
!--- designation are done with NAT.  
!--- As outbound traffic is permitted by default on the PIX, no  
!--- static commands are needed.
```

```
nat (inside) 1 192.168.2.0 255.255.255.0
```

```
!--- Creates a static route for the 192.168.2.x network with 192.168.1.2.  
!--- The PIX forwards packets with these addresses to the router  
!--- at 192.168.1.2.
```

```
route inside 192.168.2.0 255.255.255.0 192.168.1.2 1
```

```
!--- Sets the default route for the PIX Firewall at 209.64.3.2.
```

```
route outside 0.0.0.0 0.0.0.0 209.64.3.2 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 since "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 rsh  
    inspect rtsp  
    inspect esmtp  
    inspect sqlnet  
    inspect skinny  
    inspect sunrpc  
    inspect xdmcp  
    inspect sip  
    inspect netbios  
    inspect tftp  
!
```

```
service-policy global_policy global  
Cryptochecksum:8a63de5ae2643c541a397c2de7901041  
: end
```

Router A

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname 2522-R4  
!  
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.  
!  
ip subnet-zero  
!  
!  
!  
!  
interface Ethernet0  
  
!--- Assigns an IP address to the inside Ethernet interface.  
  
ip address 192.168.2.1 255.255.255.0  
no ip directed-broadcast  
!  
interface Ethernet1  
  
!--- Assigns an IP address to the PIX-facing interface.  
  
ip address 192.168.1.2 255.255.255.252  
no ip directed-broadcast  
!  
interface Serial0  
no ip address  
no ip directed-broadcast  
shutdown  
!  
interface Serial1  
no ip address  
no ip directed-broadcast  
shutdown  
!  
ip classless  
  
!--- This route instructs the inside router to forward all  
!--- non-local packets to the PIX.  
  
ip route 0.0.0.0 0.0.0.0 192.168.1.1  
!  
!  
line con 0  
transport input none  
line aux 0  
autoselect during-login  
line vty 0 4  
exec-timeout 5 0  
password ww  
login  
!
```

end

Router B

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname 2522-R4  
!  
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.  
!  
ip subnet-zero  
!  
!  
!  
interface Ethernet0  
  
!--- Assigns an IP address to the PIX-facing Ethernet interface.  
  
ip address 209.64.3.2 255.255.255.252  
no ip directed-broadcast  
!  
interface Ethernet1  
  
!--- Assigns an IP address to the server-facing Ethernet interface.  
  
ip address 209.64.3.5 255.255.255.252  
no ip directed-broadcast  
!  
interface Serial0  
  
!--- Assigns an IP address to the Internet-facing interface.  
  
ip address 209.64.3.9 255.255.255.252  
no ip directed-broadcast  
no ip mroute-cache  
!  
interface Serial1  
no ip address  
no ip directed-broadcast  
!  
ip classless  
  
!--- All non-local packets are to be sent out serial 0. In this case,  
!--- the IP address on the other end of the serial interface is not known,  
!--- or you can specify it here.  
  
ip route 0.0.0.0 0.0.0.0 serial 0  
!  
  
!--- This statement is required to direct traffic destined to the
```

```
!--- 209.64.3.128 network (the PIX global pool) to the PIX to be translated
!--- back to the inside addresses.
```

```
ip route 209.64.3.128 255.255.255.128 209.64.3.1
!
!
line con 0
  transport input none
line aux 0
  autoselect during-login
line vty 0 4
  exec-timeout 5 0
  password ww
  login
!
end
```

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.

```
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

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.

Related Information

- [Establishing Connectivity Through Cisco PIX Firewalls](#)
 - [Cisco Secure PIX Firewall Documentation](#)
 - [Cisco PIX Firewall Software](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [Security Product Field Notices \(including PIX\)](#)
 - [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: Oct 01, 2006

Document ID: 70029
