Configuring the PIX Firewall with Mail Server Access on Outside Network

Document ID: 8109

Contents

Introduction

This sample configuration demonstrates how to set up the PIX Firewall for access to a mail server located on the outside 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 applies to these software and hardware versions:

- Cisco Secure PIX 500 Series Firewall
- PIX Firewall software release 6.3(3)
- Cisco 2522 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.

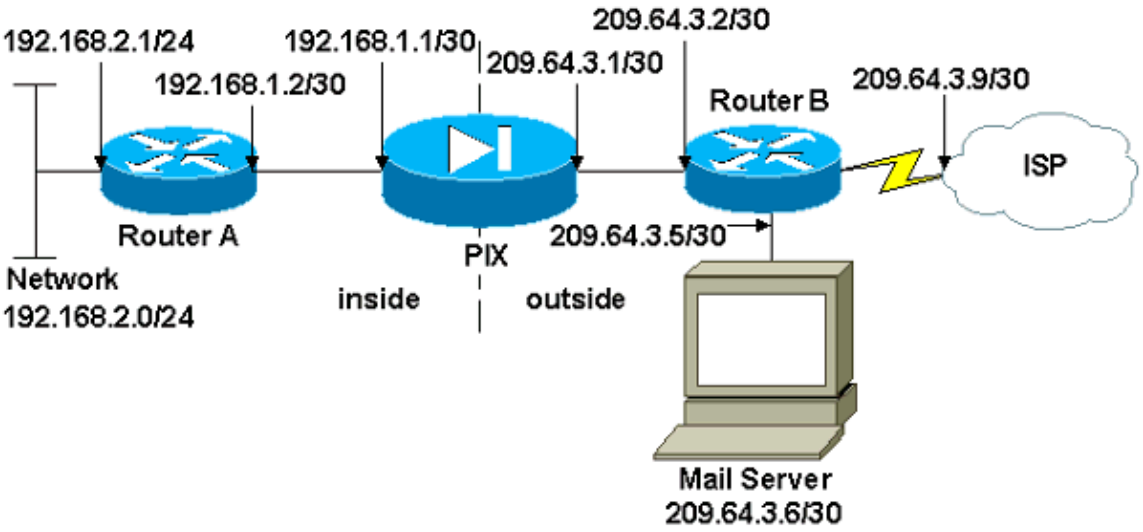
Configure

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 6.3(3)

!--- These commands name the Ethernet interfaces and
  !--- define their security levels.

  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
  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

!--- These commands specify the media type
  !--- for the interfaces...auto = auto-detect.

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

!--- These commands define an IP address for each interface.

  ip address inside 192.168.1.1 255.255.255.252
  ip address outside 209.64.3.1 255.255.255.252
  no failover
  arp timeout 14400

!--- This command defines the global address 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

!--- 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

!--- 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
  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
  snmp-server host inside 161.240.21.246
```

```
  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
```

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 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
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

Related Information

- **Documentation for PIX Firewall**
- **PIX Support Page**
- **PIX Command Reference**
- **Establishing Connectivity Through Cisco PIX Firewalls**
- **Field Notices for PIX**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 21, 2007 Document ID: 8109