

PIX/ASA : Connecting Two Internal Networks with Internet Configuration Example

Document ID: 10138

Interactive: This document offers customized analysis of your Cisco device.

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Configure

- Network Diagram
- PIX 6.x Configuration
- Configure PIX/ASA 7.x and Later

Verify

Troubleshoot

- Troubleshooting Commands

Information to Collect if You Open a Cisco Technical Support Case

Related Information

Introduction

This sample configuration demonstrates how to set up the Cisco Security Appliances (PIX/ASA) for use with two internal networks.

Prerequisites

Requirements

When you add a second internal network behind a PIX Firewall, keep in mind the following points.

- The PIX cannot route any packets.
- The PIX does not support secondary addressing.
- A router has to be used behind the PIX to achieve routing between the existing network and the newly added network.
- The default gateway of all the hosts should be set pointing to the inside router.
- Add a default route on the inside router pointing to the PIX.
- Remember to clear the Address Resolution Protocol (ARP) cache on the inside router.

Components Used

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

- Cisco PIX Firewall Software Release 6.x and later

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.

Related Products

This configuration can also be used with the Cisco 5500 Series Adaptive Security Appliance, which runs Version 7.x and later.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

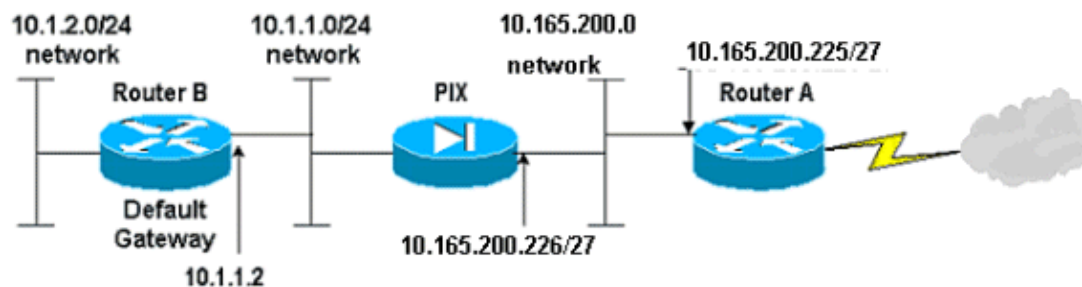
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown in this diagram.



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 6.x Configuration

This document uses the configurations shown here.

If you have the output of a **write terminal** command from your Cisco device, you can use Output Interpreter (registered customers only) to display potential issues and fixes.

- PIX 6.3 Configuration
- Router B Configuration
- Configure PIX/ASA 7.x and Later

PIX 6.3 Configuration
<pre>PIX Version 6.3(3) nameif ethernet0 outside security0 nameif ethernet1 inside security100</pre>

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
```

```
!--- Output Suppressed
```

```
!--- Enable logging.
```

```
logging on
```

```
!--- Output Suppressed
```

```
!--- All interfaces are shutdown by default.
```

```
mtu outside 1500
mtu inside 1500
mtu intf2 1500
```

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

```
ip address outside 10.165.200.226 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0
```

```
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
```

```
arp timeout 14400
```

```
!--- Output Suppressed
```

```
!--- Specify the global address to be used.
```

```
global (outside) 1 10.165.200.227-10.165.200.254 netmask 255.255.255.224
```

```
!--- Specify a pool of addresses on the outside interface
!--- to which the hosts defined in the NAT statement are translated.
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

```
!--- Sets the default route for the PIX Firewall at 10.165.200.225.
```

```
route outside 0.0.0.0 0.0.0.0 10.165.200.225 1
```

```
!--- Creates a static route for the 10.1.2.x network with 10.1.1.2.  
!--- The PIX forwards packets with these addresses to the router  
!--- at 10.1.1.2.
```

```
route inside 10.1.2.0 255.255.255.0 10.1.1.2  
: end  
[OK]
```

```
!--- Output Suppressed
```

Router B Configuration

```
Building configuration...
```

```
Current configuration:
```

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname Router B  
!  
!  
username cisco password 0 cisco  
!  
!  
!  
ip subnet-zero  
ip domain-name cisco.com  
!  
isdn voice-call-failure 0  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
ip address 10.1.1.2 255.255.255.0  
  
no ip directed-broadcast  
!  
interface Ethernet0/1  
  
!--- Assigns an IP address to the PIX-facing Ethernet interface.  
  
ip address 10.1.2.1 255.255.255.0  
  
no ip directed-broadcast
```

```

!
interface BRI1/0
  no ip address
  no ip directed-broadcast
  shutdown
  isdn guard-timer 0 on-expiry accept
!
interface BRI1/1
  no ip address
  no ip directed-broadcast
  shutdown
  isdn guard-timer 0 on-expiry accept
!
interface BRI1/2
  no ip address
  no ip directed-broadcast
  shutdown
  isdn guard-timer 0 on-expiry accept
!
interface BRI1/3
  no ip address
  no ip directed-broadcast
  shutdown
  isdn guard-timer 0 on-expiry accept
!
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 10.1.1.1
no ip http server
!
!
line con 0
  exec-timeout 0 0
  length 0
  transport input none
line aux 0
line vty 0 4
  password ww
  login
!
end

```

Configure PIX/ASA 7.x and Later

Note: Nondefault commands are shown in **bold**.

PIX/ASA
<pre> pixfirewall# sh run : Saved : PIX Version 8.0(2) ! hostname pixfirewall enable password 2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0 nameif outside security-level 0 ip address 10.165.200.226 255.255.255.224 </pre>

```

!
interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!

!--- Output Suppressed

!--- Enable logging.

logging enable

!--- Output Suppressed

!--- Specify the global address to be used.

global (outside) 1 10.165.200.227-10.165.200.254 netmask 255.255.255.224

!--- Specify a pool of addresses on the outside interface
!--- to which the hosts defined in the NAT statement are translated.

nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- Sets the default route for the PIX Firewall at 10.165.200.225.

route outside 0.0.0.0 0.0.0.0 10.165.200.225 1

!--- Creates a static route for the 10.1.2.x network with 10.1.1.2.
!--- The PIX forwards packets with these addresses to the router
!--- at 10.1.1.2.

route inside 10.1.2.0 255.255.255.0 10.1.1.2

: end

!--- Output Suppressed

```

NOTE:For more information on configuring NAT and PAT on PIX/ASA refer the document PIX/ASA 7.x NAT and PAT Statements

For more information on configuring Access Lists on PIX/ASA refer the document PIX/ASA 7.x : Port Redirection(Forwarding) with nat, global, static and access-list Commands

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

NOTE:For more information on how to troubleshoot PIX/ASA, refer to Troubleshoot Connections through the PIX and ASA.

Troubleshooting Commands

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands.

- **debug icmp trace** Shows whether ICMP requests from the hosts reach the PIX. To run this debug, you need to add the **conduit permit icmp any any** command to your configuration. However, when you have finished debugging, remove the **conduit permit icmp any any** command to avoid security risks.

Information to Collect if You Open a Cisco Technical Support Case

If you still need assistance after you follow the troubleshooting steps in this document and want to open a case with Cisco Technical Support, be sure to include this information for troubleshooting your PIX Firewall.

- Problem description and relevant topology details.
- Troubleshooting performed before opening the case.
- Output from the **show tech-support** command.
- Output from the **show log** command after running with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available).
- Output of the **debug icmp trace** command as you attempt to pass ICMP traffic through the firewall.

Attach the collected data to your case in non-zipped, plain text format (.txt). You can attach information to your case by uploading it using the TAC Service Request Tool (registered customers only). If you cannot access the Service Request Tool, you can send the information in an email attachment to attach@cisco.com with your case number in the subject line of your message.

Related Information

- [Documentation for PIX Firewall](#)
- [PIX Command Reference](#)
- [Requests for Comments \(RFCs\)](#)

- **Cisco PIX 500 Series Security Appliances**
 - **Cisco ASA 5500 Series Adaptive Security Appliances**
 - **Technical Support – Cisco Systems**
-

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

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 24, 2008

Document ID: 10138
