

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

Document ID: 10137

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

- PIX/ASA 7.x (and above) Configuration

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This sample configuration demonstrates how to configure the Cisco Security Appliances (PIX/ASA) with three internal networks. Static routes are used on the routers for simplicity.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the PIX 515 with PIX Software version 6.x and above.

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 that runs version 7.x and above.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

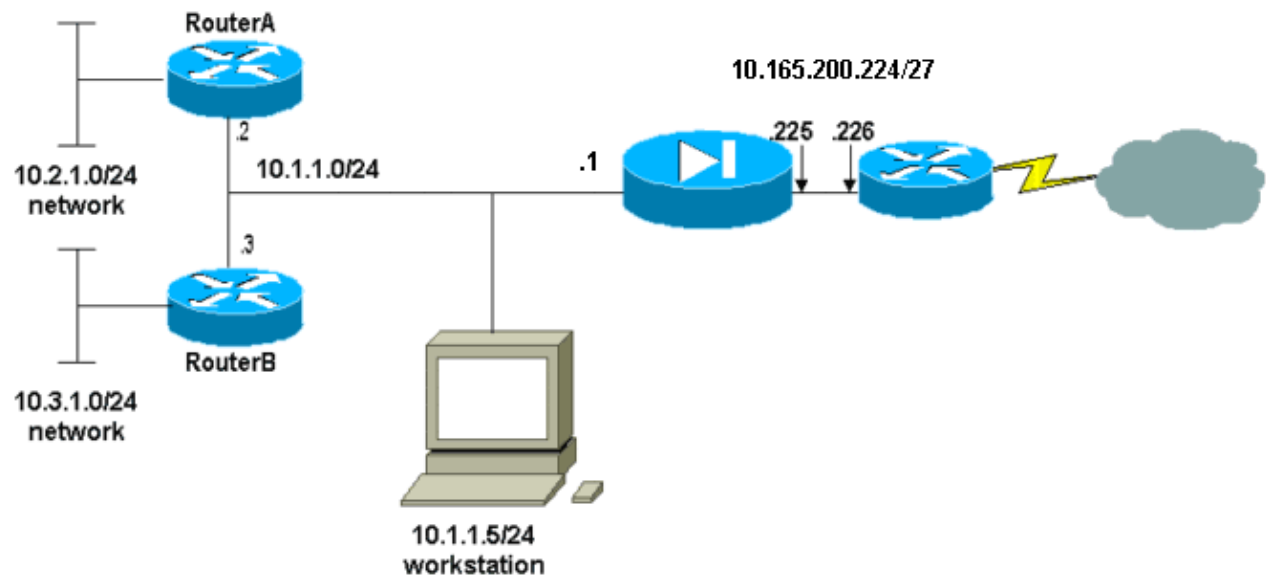
In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup.

Note: The default gateway of the hosts on the 10.1.1.0 network points to RouterA. A default route on RouterB is added that points to RouterA. RouterA has a default route that points to the PIX inside interface.



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

PIX 6.x Configuration

This document uses these configurations.

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.

- RouterA Configuration
- RouterB Configuration
- PIX 6.3 Configuration
- PIX/ASA 7.x (and above) Configuration

RouterA Configuration

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
```

```
!  
control-plane  
!  
!  
!  
line con 0  
line 33  
no activation-character  
no exec  
transport preferred none  
transport input all  
transport output all  
line aux 0  
line vty 0 4  
password ww  
login  
!  
!  
end  
  
RouterA#
```

RouterB Configuration

```
RouterB#show running-config  
Building configuration...  
  
Current configuration : 1132 bytes  
!  
version 12.3  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname RouterB  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no network-clock-participate slot 1  
no network-clock-participate wic 0  
no network-clock-participate wic 1  
no network-clock-participate wic 2  
no network-clock-participate aim 0  
no network-clock-participate aim 1  
no aaa new-model  
ip subnet-zero  
ip cef  
!  
!  
!  
!  
ip audit po max-events 100  
no ip domain lookup  
no ftp-server write-enable  
!  
!  
!  
!  
no crypto isakmp enable  
!  
!
```

```

!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#

```

PIX 6.3 Configuration

```

pixfirewall(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100

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 pix/intf2 1500
ip address outside 10.165.200.225 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0

ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside

pdm history enable
arp timeout 14400

!--- Output Suppressed

*!--- Define a Network Address Translation (NAT) pool that
!--- internal hosts use when going out to the Internet.*

global (outside) 1 10.165.200.228-10.165.200.254 netmask 255.255.255.224

global (outside) 1 10.165.200.227

*!--- Allow all internal hosts to use
!--- the NAT or PAT addresses specified previously.*

nat (inside) 1 10.0.0.0 255.0.0.0 0 0

!--- Output Suppressed

```
!--- Define a default route to the ISP router.

route outside 0.0.0.0 0.0.0.0 10.165.200.226 1

!--- Define a route to the ISP router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the ISP router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

!--- Output Suppressed

: end
[OK]

!--- Output Suppressed
```

PIX/ASA 7.x (and above) Configuration

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

PIX/ASA
<pre>pixfirewall#show run : Saved : PIX Version 8.0(2) ! hostname pixfirewall enable password 2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0 nameif outside security-level 0 ip address 10.165.200.225 255.255.255.224 ! interface Ethernet1 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 ! <i>!--- Output Suppressed</i></pre>

```

!--- Enable logging.

logging enable

!--- Define a Network Address Translation (NAT) pool that
!--- internal hosts use when going out to the Internet.

global (outside) 1 10.165.200.228-10.165.200.254 netmask 255.255.255.224
global (outside) 1 10.165.200.227

!--- Allow all internal hosts to use
!--- the NAT or PAT addresses specified previously.

nat (inside) 1 10.0.0.0 255.0.0.0 0 0

!--- Output Suppressed

!--- Define a default route to the ISP router.

route outside 0.0.0.0 0.0.0.0 10.165.200.226 1

!--- Define a route to the ISP router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the ISP router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end

```

Note: For more information on how to configure NAT and PAT on PIX/ASA, refer to PIX/ASA 7.x NAT and PAT Statements.

For more information on how to configure access lists on PIX/ASA, refer to 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

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 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.
- **logging buffer debugging** Shows connections being 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 using the **show log** command.

Refer to Setting Up the PIX Syslog for more information on how to set up logging.

Related Information

- [Documentation for PIX Firewall](#)
- [PIX Product Support Page](#)
- [Requests for Comments \(RFCs\)](#)
- [PIX Command Reference](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [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 24, 2008

Document ID: 10137
