

# PIX/ASA : Connecting Single Internal Networks with Internet Configuration Example

Document ID: 10136

---

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

---

## **Introduction**

### **Before You Begin**

Prerequisites

Components Used

Related Products

Conventions

### **Configure**

Network Diagram

PIX 6.x Configuration

Configure PIX/ASA 7.x and Later

### **Verify**

### **Troubleshoot**

### **Related Information**

---

## **Introduction**

This sample configuration demonstrates how to set up the Cisco Security Appliances (PIX/ASA) for use on a single internal network.

For more information about the PIX/ASA Security Appliance Version 7.x and later with multiple internal networks that connect to the Internet (or an external network) with the command line interface (CLI) or Adaptive Security Device Manager (ASDM) 5.x and later, refer to PIX/ASA 7.x and later: Connecting Multiple Internal Networks with Internet Configuration Example.

## **Before You Begin**

### **Prerequisites**

There are no specific prerequisites for this document.

### **Components Used**

The information in this document is based on the software and hardware versions below.

- Cisco PIX Firewall Software Release 6.x and later

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## 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 about document conventions, refer to Cisco Technical Tips Conventions.

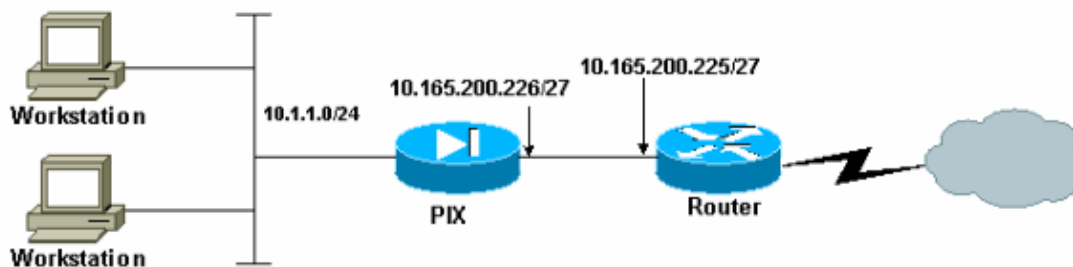
## Configure

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 the diagram below.



**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 below.

If you have the output of a **write terminal** command from your Cisco device, you can use to display potential issues and fixes. To use, you must be a registered customer, be logged in, and have JavaScript enabled.

You can use Output Interpreter to display potential issues and fixes. To use Output Interpreter, you must be a registered customer, be logged in, and have JavaScript enabled.

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

### PIX 6.3 Configuration

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
```

```
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
```

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

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

```
logging on
```

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

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

```
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 100full
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 10.165.200.226 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
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 10.165.200.227-10.165.200.254 netmask 255.255.255.224
```

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

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

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

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

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

```
: end  
[OK]
```

### Router Configuration

```
Building configuration...
```

```
Current configuration:
```

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname R3640_out  
!  
!  
username cisco password 0 cisco  
!  
!  
!  
ip subnet-zero  
ip domain-name cisco.com  
!  
isdn voice-call-failure 0  
!  
!  
interface Ethernet0/1  
 ip address 10.165.200.225 255.255.255.224  
 no ip directed-broadcast  
!  
ip classless  
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**.

```
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 10.165.200.226 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!

!--- Output Suppressed

!--- Enable logging.

logging enable

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

global (outside) 1 10.165.200.227-10.165.200.254 netmask 255.255.255.224

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

nat (inside) 1 0.0.0.0 0.0.0.0 0 0

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

route outside 0.0.0.0 0.0.0.0 10.165.200.225 1

!--- Output Suppressed

: end
```

**NOTE:**For more information about the configuration of NAT and PAT on PIX/ASA, refer to PIX/ASA 7.x NAT and PAT Statements.

For more information about the configuration of 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 about how to troubleshoot PIX/ASA, refer to Troubleshoot Connections through the PIX and ASA.

Certain **show** commands are supported by the Output Interpreter Tool ( registered customers only) , which allows you to view an analysis of **show** command output.

**Note:** Before issuing **debug** commands, please see 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 **conduit permit icmp any any** command to avoid security risks.

---

## Related Information

- [Documentation for PIX Firewall](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [PIX Command Reference](#)
- [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 24, 2008

Document ID: 10136

---