

PIX/ASA : Configure and Troubleshoot the PIX Firewall with a Single Internal Network

Document ID: 13825

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
- Configuring PIX/ASA 7.x and later

Verify

Troubleshoot

- Troubleshooting Commands

Troubleshooting Common Problems

Information to Collect if You Open a TAC Service Request

Related Information

Introduction

This sample configuration demonstrates how to configure a Security Appliance to separate a corporate network from the Internet.

Prerequisites

Requirements

The internal network has a Web server, a mail server, and an FTP server that users on the Internet can access. All other access to hosts on the internal network is denied from outside users.

- Real address of the Web server – 192.168.1.4; Internet address 10.1.1.3
- Real address of the Mail server – 192.168.1.15; Internet address 10.1.1.4
- Real address of the FTP server – 192.168.1.10; Internet address 10.1.1.5

All users on the internal network are allowed unrestricted access to the Internet. Internal users are allowed to ping devices on the Internet, but users on the Internet are not allowed to ping devices on the inside.

The company used in this configuration has purchased a Class A network from their ISP (10.1.1.x). The .1 and .2 addresses are reserved for the external router and the outside interface of the PIX respectively. Addresses .3 – .5 are used for internal servers that users on the Internet can access. Addresses .6 – .14 are reserved for future use for servers that external users can access.

The PIX Firewall in the example has four network interface cards, but only two of them are in use. The PIX is set up to send syslogs to a syslog server on the inside with an IP address of 192.168.1.220 (not shown in the Network Diagram).

Components Used

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

- Cisco PIX Firewall 535
- 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

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

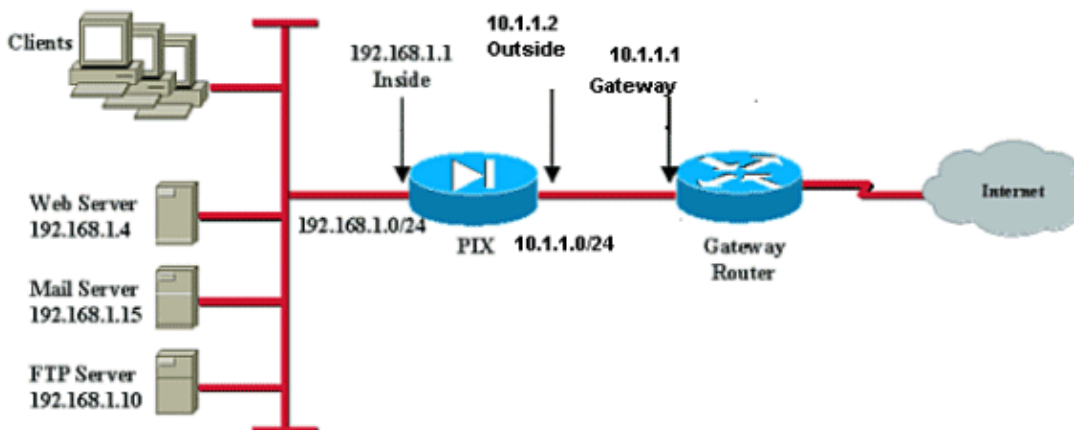
Configure

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 obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 <<http://www.ietf.org/rfc/rfc1918.txt?number=1918>> addresses which have been used in a lab environment.

PIX 6.x Configuration

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

```
PIX
Building configuration...
: Saved
:
PIX Version 6.3(3)
nameif gb-ethernet0 outside security0
nameif gb-ethernet1 inside security100
nameif ethernet0 intf2 security10
nameif ethernet1 intf3 security15
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall

!--- Output Suppressed

!--- Create an access list to allow pings out
!--- and return packets back in.

access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any time-exceeded
access-list 100 permit icmp any any unreachable

!--- Allows anyone on the Internet to connect to
!--- the web, mail, and FTP servers.

access-list 100 permit tcp any host 10.1.1.3 eq www
access-list 100 permit tcp any host 10.1.1.4 eq smtp
access-list 100 permit tcp any host 10.1.1.5 eq ftp
pager lines 24

!--- Enable logging.

logging on
no logging timestamp
no logging standby
no logging console
no logging monitor

!--- Enable error and more severe syslog messages
!--- to be saved to the local buffer.

logging buffered errors

!--- Send notification and more severe syslog messages
!--- to the syslog server.

logging trap notifications
no logging history
logging facility 20
logging queue 512
```

```
!--- Send syslog messages to a syslog server
!--- on the inside interface.

logging host inside 192.168.1.220

!--- All interfaces are shutdown by default.

interface gb-ethernet0 1000auto
interface gb-ethernet1 1000auto
interface ethernet0 auto shutdown
interface ethernet1 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
ip address outside 10.1.1.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
arp timeout 14400

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

global (outside) 1 10.1.1.15-10.1.1.253

!--- Define a Port Address Translation (PAT) address that
!--- is used once the NAT pool is exhausted.

global (outside) 1 10.1.1.254

!--- 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 static translation for the internal
!--- web server to be accessible from the Internet.

static (inside,outside) 10.1.1.3 192.168.1.4
    netmask 255.255.255.255 0 0

!--- Define a static translation for the internal
!--- mail server to be accessible from the Internet.

static (inside,outside) 10.1.1.4 192.168.1.15
    netmask 255.255.255.255 0 0

!--- Define a static translation for the internal
!--- FTP server to be accessible from the Internet.
```

```

static (inside,outside) 10.1.1.5 192.168.1.10
netmask 255.255.255.255 0 0

!--- Apply access list 100 to the outside interface.

access-group 100 in interface outside

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

route outside 0.0.0.0 0.0.0.0 10.1.1.1 1

!--- Output Suppressed

!--- Allow the host 192.168.1.254 to be able to
!--- Telnet to the inside of the PIX.

telnet 192.168.1.254 255.255.255.255 inside
: end
[OK]

!--- Output Suppressed

```

Configuring 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 10.1.1.2 255.255.255.0 ! interface Ethernet1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 ! !--- Output Suppressed !--- Create an access list to allow pings out !--- and return packets back in. </pre>

```
access-list 100 extended permit icmp any any echo-reply
access-list 100 extended permit icmp any any time-exceeded
access-list 100 extended permit icmp any any unreachable
```

```
!--- Allows anyone on the Internet to connect to
!--- the web, mail, and FTP servers.
```

```
access-list 100 extended permit tcp any host 10.1.1.3 eq www
access-list 100 extended permit tcp any host 10.1.1.4 eq smtp
access-list 100 extended permit tcp any host 10.1.1.5 eq ftp
pager lines 24
```

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

```
logging enable
```

```
!--- Enable error and more severe syslog messages
!--- to be saved to the local buffer.
```

```
logging buffered errors
```

```
!--- Send notification and more severe syslog messages
!--- to the syslog server.
```

```
logging trap notifications
```

```
!--- Send syslog messages to a syslog server
!--- on the inside interface.
```

```
logging host inside 192.168.1.220
```

```
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
```

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

```
global (outside) 1 10.1.1.15-10.1.1.253
```

```
!--- Define a Port Address Translation (PAT) address that
```

```
!--- is used once the NAT pool is exhausted.

global (outside) 1 10.1.1.254

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

nat (inside) 1 0.0.0.0 0.0.0.0

!--- Define a static translation for the internal
!--- web server to be accessible from the Internet.

static (inside,outside) 10.1.1.3 192.168.1.4 netmask 255.255.255.255

!--- Define a static translation for the internal
!--- mail server to be accessible from the Internet.

static (inside,outside) 10.1.1.4 192.168.1.15 netmask 255.255.255.255

!--- Define a static translation for the internal
!--- FTP server to be accessible from the Internet.

static (inside,outside) 10.1.1.5 192.168.1.10 netmask 255.255.255.255

!--- Apply access list 100 to the outside interface.

access-group 100 in interface outside

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

route outside 0.0.0.0 0.0.0.0 10.1.1.1 1

!--- Output Suppressed

!--- Allow the host 192.168.1.254 to be able to
!--- Telnet to the inside of the PIX.

telnet 192.168.1.254 255.255.255.255 inside
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

```
!  
: end  
  
!--- Output Suppressed
```

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

For more information on 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.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show interface** Shows interface statistics.
- **show traffic** Shows how much traffic passes through the PIX.
- **show xlate** Shows the current translations built through the PIX.
- **show conn** Shows the current connections through the PIX.

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

Troubleshooting Commands

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug icmp trace** Shows all Internet Control Message Protocol (ICMP) echo requests and replies to or through the PIX.

Troubleshooting Common Problems

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

- The NAT pool (and PAT address – with the exception of interface PAT) must use IP addresses that are not used by any other device on the network. This includes static addresses (for translations) or addresses used on the interfaces.

If you have PIX software versions 5.2 or later, the outside interface address of the PIX can be used for PAT. This is useful if you have only one external address available, or need to conserve your IP address space.

In order to enable PAT on the outside interface address, remove the global NAT pool and PAT address from the configuration, and use the outside interface IP address as the PAT address.

```
ip address outside 10.1.1.2
nat (inside) 1 0 0 global (outside) 1 interface
```

Note: Some multimedia applications can conflict with port mappings provided by PAT. PAT does not work with the **established** command. PAT works with Domain Name System (DNS), FTP and passive FTP, HTTP, email, remote–procedure call (RPC), rshell, Telnet, URL filtering, and outbound traceroute. Several PIX versions support H.323 with PAT on several versions. H.323v2 with PAT support was added in version 6.2.2, while H.323v3 and v4 with PAT support was added in version 6.3.

- You must have an access list (or conduit) to permit access into your servers. Inbound access is not permitted by default.

Note: The **conduit** command has been superseded by the **access–list** command. Cisco recommends that you migrate your configuration away from the **conduit** command to maintain future compatibility.

- After *any* access list, there is an implicit **deny ip any any** command.
- If the DNS server is on the outside of the PIX, and internal users want to access the internal servers with their DNS name, then the **alias** command must be used to doctor the DNS response from the DNS server.
- If you still have problems after you review these common problems, complete these steps:
 1. Verify that you have IP connectivity between the two devices. In order to do this, either console into the PIX, or Telnet into the PIX. Issue the **terminal monitor** and **debug icmp trace** commands.
 2. If internal users have difficulty accessing servers on the Internet, ping the server you are trying to access and see if you get a response. If you do not receive a response, look at the debug statements and make sure you see the ICMP Echo Request go out through the PIX. If you do not see the Echo Requests, then check the default gateway of the source machine. Typically, it is the PIX.

Also, use **nslookup** on the client, and make sure it can resolve the IP address of the server you are trying to reach.

3. When you have IP connectivity, turn off **debug icmp trace** and turn on **logging console debug** (if connected to the console) or **logging monitor debug** (if connected to the PIX via Telnet). This causes the syslog messages to be displayed to your screen. Try to connect to the server, and watch the syslogs to see if any traffic is denied. If so, the syslogs should give you a good idea of why this is happening. You can also look at the description of the syslog messages.
4. If outside users are unable to access your internal servers:
 - a. Verify the syntax of your **static** command.
 - b. Double–check that you have permitted access with your **access–list** command statements.
 - c. Double–check that you have applied the access list with the **access–group** command.
5. If you are a registered user and you are logged in, you can troubleshoot your PIX problems with the TAC Case Collection [🔗](#) (registered customers only) .

Information to Collect if You Open a TAC Service Request

If you still need assistance after you follow the troubleshooting

steps in this document and want to open a service request with the Cisco TAC, be sure to include this information for troubleshooting your PIX Firewall.

- Problem description and relevant topology details
- Troubleshooting performed before opening the service request
- 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)

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

Related Information

- [PIX 500 Series Security Appliance Support Page](#)
- [Documentation for PIX Firewall](#)
- [Cisco Security PIX Firewall 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: Nov 14, 2008

Document ID: 13825
