

Cisco Secure PIX Firewall with Two Routers Configuration Example

Document ID: 15244

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

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Network Diagram

- Configurations

Verify

Troubleshoot

Concepts

Network Protocols Whose Use Is Not Recommended with a Firewall

Related Information

Introduction

This example configuration demonstrates how to secure a network with a combination of routers and a Cisco Secure PIX Firewall. There are three levels of defense (two routers and the PIX Firewall) and logging set up to a syslog server to aid in the identification of potential security attacks.

Note: This document does not cover issues such as password selection and other forms of security that are necessary to successfully protect your network from attack.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on PIX Software version 5.3.1 and later.

Note: Commands used in other versions of PIX software vary slightly. Refer to the PIX documentation before you implement this configuration.

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.

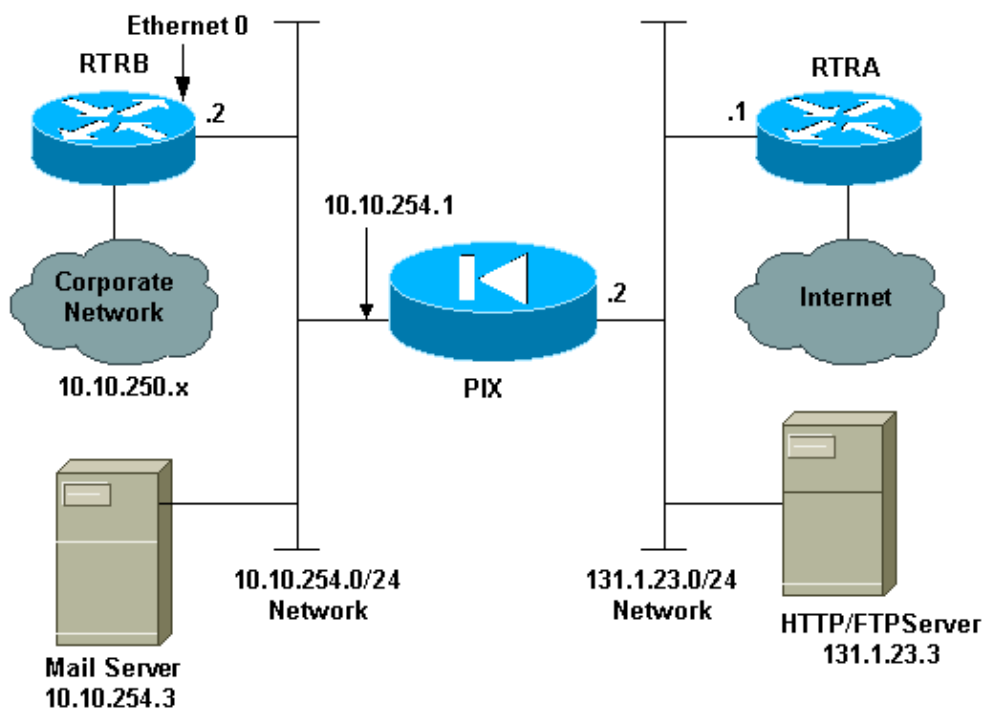
Configure

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

The first configuration is for the PIX Firewall because the router configurations must be understood in relation to the firewall.

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

This document uses these configurations:

- PIX Firewall
- RTRA
- RTRB

PIX Firewall

```

!--- Sets the outside address of the PIX Firewall:
ip address outside 131.1.23.2

!--- Sets the inside address of the PIX Firewall:
ip address inside 10.10.254.1

!--- Sets the global pool for hosts inside the firewall:
global (outside) 1 131.1.23.12-131.1.23.254

!--- Allows hosts in the 10.0.0.0 network to be
!--- translated through the PIX:
nat (inside) 1 10.0.0.0

!--- Configures a static translation for an admin workstation
!--- with local address 10.14.8.50:
static (inside,outside) 131.1.23.11 10.14.8.50

!--- Allows syslog packets to pass through the PIX from RTRA.
!--- You can use conduits OR access-lists to permit traffic.
!--- Conduits has been added to show the use of the command,
!--- however they are commented in the document, since the
!--- recommendation is to use access-list.
!--- To the admin workstation (syslog server):
!--- Using conduit:
!--- conduit permit udp host 131.1.23.11 eq 514 host 131.1.23.1

!--- Using access-list:
Access-list 101 permit udp host 131.1.23.1 host 131.1.23.11 255.255.255.0 eq 514
Access-group 101 in interface outside

!--- Permits incoming mail connections to 131.1.23.10:
static (inside, outside) 131.1.23.10 10.10.254.3

!--- Using conduits
!--- conduit permit TCP host 131.1.23.10 eq smtp any
!--- Using Access-lists, we use access-list 101
!--- which is already applied to interface outside.
Access-list 101 permit tcp any host 131.1.23.10 eq smtp

!--- PIX needs static routes or the use of routing protocols
!--- to know about networks not directly connected.
!--- Add a route to network 10.14.8.x/24.
route inside 10.14.8.0 255.255.255.0 10.10.254.2

!--- Add a default route to the rest of the traffic
!--- that goes to the internet.
Route outside 0.0.0.0 0.0.0.0 131.1.23.1

!--- Enables the Mail Guard feature
!--- to accept only seven SMTP commands
!--- HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT:
!--- (This can be turned off to permit ESMTP by negating with
!--- the no fixup protocol smtp 25 command):

```

```

fixup protocol smtp 25

!--- Allows Telnet from the inside workstation at 10.14.8.50
!--- into the inside interface of the PIX:

telnet 10.14.8.50

!--- Turns on logging:

logging on

!--- Turns on the logging facility 20:

logging facility 20

!--- Turns on logging level 7:

logging history 7

!--- Turns on the logging on the inside interface:

logging host inside 10.14.8.50

```

Note: RTRA is the outside shield router. It must shield the PIX Firewall from directed attacks, protect the FTP/HTTP server, and act as an alarm system. If anyone breaks into RTRA, the system administrator should be notified immediately.

RTRA

```

no service tcp small-servers

!--- Prevents some attacks against the router itself.

logging trap debugging

!--- Forces the router to send a message
!--- to the syslog server for each and every
!--- event on the router. This includes packets denied
!--- access through access lists and
!--- configuration changes. This acts as an early warning system to the system
!--- administrator that someone is trying to break in, or has broken in and is
!--- trying to create a "hole" in their firewall.

logging 131.1.23.11

!--- The router logs all events to this
!--- host, which in this case is the
!--- "outside" or "translated" address of the system
!--- administrator's workstation.

enable secret xxxxxxxxxxxx
!
interface Ethernet 0
 ip address 131.1.23.1 255.255.255.0
!
interface Serial 0
 ip unnumbered ethernet 0
 ip access-group 110 in

!--- Shields the PIX Firewall and the HTTP/FTP
!--- server from attacks and guards
!--- against spoofing attacks.

!

```

```

access-list 110 deny ip 131.1.23.0 0.0.0.255 any log

!--- RTRA and the PIX Firewall.
!--- This is to prevent spoofing attacks.

access-list 110 deny ip any host 131.1.23.2 log

!--- Prevents direct attacks against the
!--- outside interface of the PIX Firewall and
!--- logs any attempts to connect to the
!--- outside interface of the PIX to the syslog server.

access-list 110 permit tcp any 131.1.23.0 0.0.0.255 established

!--- Permits packets which are part
!--- of an established TCP session.

access-list 110 permit tcp any host 131.1.23.3 eq ftp

!--- Allows FTP connections into the FTP/HTTP server.

access-list 110 permit tcp any host 131.1.23.3 eq ftp-data

!--- Allows ftp-data connections into the FTP/HTTP server.

access-list 110 permit tcp any host 131.1.23.3 eq www

!--- Allows HTTP connections into the FTP/HTTP server.

access-list 110 deny ip any host 131.1.23.3 log

!--- Disallows all other connections to
!--- the FTP/HTTP server, and logs any attempt
!--- to connect this server to the syslog server.

access-list 110 permit ip any 131.1.23.0 0.0.0.255

!--- Permits other traffic destined to the
!--- network between the PIX Firewall and RTRA.

!
line vty 0 4
  login
  password xxxxxxxxxxxx
  access-class 10 in

!--- Restricts Telnet access to the router
!--- to those IP addresses listed in
!--- access list 10.

!
access-list 10 permit ip 131.1.23.11

!--- Permits only the workstation of the administrator
!--- to Telnet into the router. This
!--- access list may need to be changed to permit
!--- access from the Internet for
!--- maintenance, but should contain as few
!--- entries as possible.

```

Note: RTRB is the inside shielding router. It is the last line of defense in your firewall, and the entry point into your inside network.

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

RTRB

```
logging trap debugging
logging 10.14.8.50

!--- Log all activity on this router to the
!--- syslog server on the administrator's
!--- workstation, including configuration changes.

!
interface Ethernet 0
 ip address 10.10.254.2 255.255.255.0
 no ip proxy-arp
 ip access-group 110 in

!--- Prevents inside and outside addresses
!--- from mingling; guards against attacks
!--- launched from the PIX Firewall or the
!--- SMTP server as much as possible.

!
access-list 110 permit udp host 10.10.250.5 0.0.0.255

!--- Permits syslog messages destined
!--- to the administrator's workstation.

access-list 110 deny ip host 10.10.254.1 any log

!--- Denies any other packets sourced
!--- from the PIX Firewall.

access-list 110 permit tcp host 10.10.254.3 10.0.0.0 0.255.255.255 eq smtp

!--- Permits SMTP mail connections from the
!--- mail host to internal mail servers.

access-list 110 deny ip host 10.10.254.3 10.0.0.0 0.255.255.255

!--- Denies all other traffic sourced
!--- from the mail server.

access-list 110 deny ip 10.10.250.0 0.0.0.255 any

!--- Prevents spoofing of trusted addresses
!--- on the internal network.

access-list 110 permit ip 10.10.254.0 0.0.0.255 10.10.250.0 0.255.255.255

!--- Permits all other traffic sourced from
!--- the network between the PIX Firewall and RTRB.

!
line vty 0 4
 login
 password xxxxxxxxxxxx
 access-class 10 in

!--- Restricts Telnet access to the router
!--- to those IP addresses listed in
!--- access list 10.

!
```

```
access-list 10 permit ip 10.14.8.50

!--- Permits only the workstation of the administrator
!--- to Telnet into the router. This
!--- access list may need to be changed to permit
!--- access from the Internet for
!--- maintenance, but should contain as few entries as possible.

!--- A static route or routing protocol must be utilized
!--- to make the router aware of network 10.14.8.x (which is
!--- inside the corporate network). This is because
!--- it is not a directly connected network.
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Concepts

The purpose of Firewalls is to prevent unauthorized entry into your network while allowing desired traffic at the same time. It is probably easiest to begin with an analysis of what the objective of a break-in might be, then consider how to make it difficult for a potential criminal to get into your network. Suppose, in the situation described in this document, that the criminal had a server in mind that contained secret information which would be of great value to your competitors. The IP address of this server, the criminal has learned, is 10.100.100.10.

Immediately, the criminal is faced with a serious problem: the IP address of the server is an address which cannot be reached over the Internet, as no organization attached to the Internet forwards packets to a network 10 destination address. This forces the criminal to either attempt to find out what address this translates to on the Internet (a smart system administrator would never let this address be translated onto the Internet), or break directly into your network in order to obtain a "base camp" from which to attack the server containing the sensitive data. Assume that the criminal cannot find any way to attack the server directly, and so starts to attack your network in order to attack the server from within your network.

The first obstacle the criminal faces is the first "demilitarized zone" (DMZ), which is in between RTRA and the PIX Firewall. The criminal can attempt to break into RTRA, but the router is configured to only accept connections from the workstation of the administrator, and to block packets that appear to be sourced from the DMZ itself. If the criminal could break into RTRA, he would only find himself in a position to attack the PIX Firewall itself – he would not be 'in' the network, and he still could not attack the host with the sensitive material directly.

The criminal could also attempt to break into the FTP/HTTP server, which is a possibility to be watched for. This host should be as secure as possible against any such attacks. If the criminal successfully broke into the FTP/HTTP server, he would still not be in a position to attack the host with the sensitive data directly, but he would be in a position to attack the PIX Firewall directly. In either case, the criminal's activities should be logged at some point in the process of getting this far, so the system administrator should be alerted to the presence of an intruder.

If the attacker did successfully break into the outer DMZ, he would find himself in a position to attack the PIX

Firewall and little more, so the second, or inner, DMZ becomes the next goal. He can reach this goal with an attack on the PIX Firewall itself, or an attack on the RTRB, which is programmed to accept Telnet sessions only from the system administrator's workstation again. Once again, his attempts to break into the inner DMZ are logged by both the PIX Firewall and RTRB, so the system administrator should have some warning and be able to stop the attack before the attacker gets to the point where he can attack the sensitive server directly.

The attacker could also bypass the outer DMZ and attempt to break into the inner DMZ by attacking the mail host. This host is protected by the PIX Firewall, and should be protected through careful monitoring and configuration. This is the most vulnerable host in the entire firewall.

The concept is to provide several layers of defense rather than one "super strong" wall. The pieces should interlock together into one strong firewall structure which is flexible enough to permit the traffic you need to allow through, but also provides plenty of alarms and early warning systems.

Network Protocols Whose Use Is Not Recommended with a Firewall

Due to their inherently insecure natures, some network protocols are not appropriate for running across Firewalls from untrusted to trusted networks. Examples of such insecure protocols are:

- NFS
- rlogin
- rsh
- any RPC-based protocol

Recent revisions of the PIX have included support for RPC protocols. Cisco, however, strongly discourages use of this capability, as RPC is very insecure. This feature is meant to be used in only the most unusual of circumstances.

PIX 7.0 uses the **inspect rpc** command to handle RPC packets. The **inspect sunrpc** command enables or disables application inspection for the Sun RPC protocol. Sun RPC services can run on any port on the system. When a client attempts to access an RPC service on a server, it must find out which port that particular service runs on. In order to do this, the client queries the portmapper process on the well-known port number 111. The client sends the RPC program number of the service, and gets back the port number. From this point on, the client program sends its RPC queries to that new port.

Related Information

- [Improving Security on Cisco Routers](#)
- [Characterizing and Tracing Packet Floods Using Cisco Routers](#)
- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – 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.](#)

