brainbuzz.com™
Cramsession

Cramsession™ for Cisco Secure PIX Firewall Fundamentals and Advanced

This study guide will help you to prepare for the Cisco exam 9E0-571, Secure PIX Firewall Advanced Exam. This exam is one in a series of four exams required to achieve the Security Specialty focusing on building and maintaining Cisco security solutions, including standalone firewall products and IOS software features. It focuses on how the PIX Firewall functions within network security; knowledge and skills needed to install, configure and operate the Cisco PIX Firewall Version 5.0(1); and basic commands.

Check for the newest version of this Cramsession
http://cramsession.brainbuzz.com/checkversion.asp?V=2451970&FN=cisco/cspfa.pdf

Rate this Cramsession
http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=Cisco+CSPFA

Feedback Forum for this Cramsession/Exam
http://boards.brainbuzz.com/boards/vbt.asp?b=1193

More Cramsession Resources:

Search for Related Jobs
http://jobs.brainbuzz.com/JobSearch.asp?R=&CSRE

CramChallenge - practice questions
http://www.cramsession.com/signup/default.asp#day

IT Resources & Tech Library
http://itresources.brainbuzz.com

Certification & IT Newsletters
http://www.cramsession.com/signup/

SkillDrill - skills assessment
http://skilldrill.brainbuzz.com

Discounts, Freebies & Product Info
http://www.cramsession.com/signup/prodinfo.asp

Contents:

What is a PIX Firewall?

Fundamentals

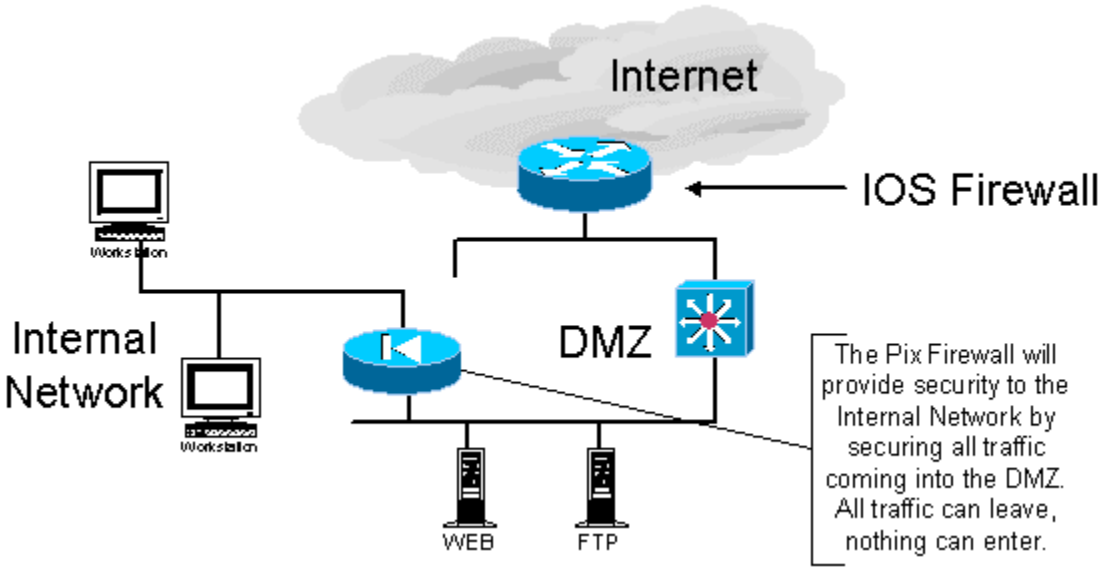
- The PIX Firewall series delivers
    - Strong security
    - Easy-to-install
    - An integrated hardware/software appliance
    - A safe, embedded system
- Cisco Secure PIX Firewalls use an embedded system that is non-UNIX, very secure, and real-time
- Proxy servers are very CPU and memory intensive and perform extensive processing on each data packet at the application level. PIX will enable you to have a dedicated appliance that has a very small footprint. This also leaves out all the bugs, back doors and holes that are found on a daily basis within operating system based Firewall systems

How does it work?

- The heart of the PIX Firewall series is a protection scheme based on ASA (ASA tracks the source and destination address, TCP sequence numbers, port numbers, and additional TCP flags of each packet), which offers stateful connection-oriented security
- This information is stored in a table, and all inbound and outbound packets are compared against entries in the table

Basic Pix Implementation: (A Simple Configuration)

The following is just to give you an idea of what a PIX implementation might look like. Every setup will be different because they are based on your individual needs. This is a two-tier set up where the router filters unwanted traffic from the Internet. If your first line of defense is penetrated, the PIX stands guard as a second line of defense protecting the Internal network from the possibility that either the router, switch or bastion hosts have been compromised.



The Pix enforces standard policies:

- Inbound connections are denied unless they are specifically mapped or authenticated
- Unless specifically denied, outbound connections are allowed once you configure global pools

Remember that the PIX is not necessarily your first line of defense. Your gateway to the Internet should provide the initial security for your network. In the event an attacker is able to breach the first line of defense, you should have a PIX protecting the Internal network.

If Security is new to you, I suggest reading from start to finish Cisco's SAFE documentation that takes you through Cisco's vision on Security.

PIX Firewall Security Features and Options

An Embedded System

A PIX firewall:

- Eliminates most of the risks associated with an operating system based firewall
- Can handle up to 256,000 connections simultaneously

Adaptive Security Algorithm

- The ASA (Adaptive Security Algorithm) is the heart of the PIX Firewall
- ASA is stateful and connection oriented
- The ASA design creates session flows based on:
    - Source and destination addresses
    - TCP sequence numbers
    - Port numbers
    - TCP flags
- By applying the security policy to the connection table entries, inbound and outbound traffic can be controlled

Cut-Through Proxy

Pix uses cut-through proxy which is a method of verifying users at the firewall and permitting and/or denying access to any TCP or UDP application

Simplified Installation

The PIX Setup Wizard has a GUI based design which increases the speed of initial firewall setup

URL Filtering

- The PIX checks outgoing URL requests against the policy defined on the server running on either Windows NT or UNIX (WebSENSE)
- The PIX Firewall either permits or denies connections based on policy
- The burden is not placed on the PIX Firewall but on a separate box performing the URL filtering

Failover/Hot Standby Upgrade Option

- The failover option can provide high availability and eliminates a single point of failure
- If one PIX malfunctions, if things are configured correctly, an automatic failover to the other PIX takes place

Configuring the PIX Firewall

Initial Config

Use the **nameif** and **ip address** commands to identify each interface in your PIX Firewall that will connect to a network segment; you will need unique IP addresses for the IP address command to assign to each interface you use

Example: *nameif Ethernet 0/0 outside sec0*

- This names the interface and sets security level

nameif Ethernet 0/1 inside sec100

- This names the interface and sets security level

interface Ethernet 0/0 auto

- Identifies speed and duplex settings

interface Ethernet 0/1 auto

- Identifies speed and duplex settings

ip address inside 10.1.1.1 255.255.255.0

- Assigns the IP address to the NIC cards for “Inside”

ip address outside 192.168.1.1 255.255.255.0

- Assigns the IP address to the NIC cards for “Outside”

global (outside) 1 192.168.1.x – 192.168.1.x 255.255.255.0

- Assigns a pool of registered IP’s for outbound connections

nat (inside) 1 0.0.0.0 0.0.0.0

- This allows an entering packet to get one of the addresses from the above pool

route outside 0.0.0.0 0.0.0.0 192.168.1.x

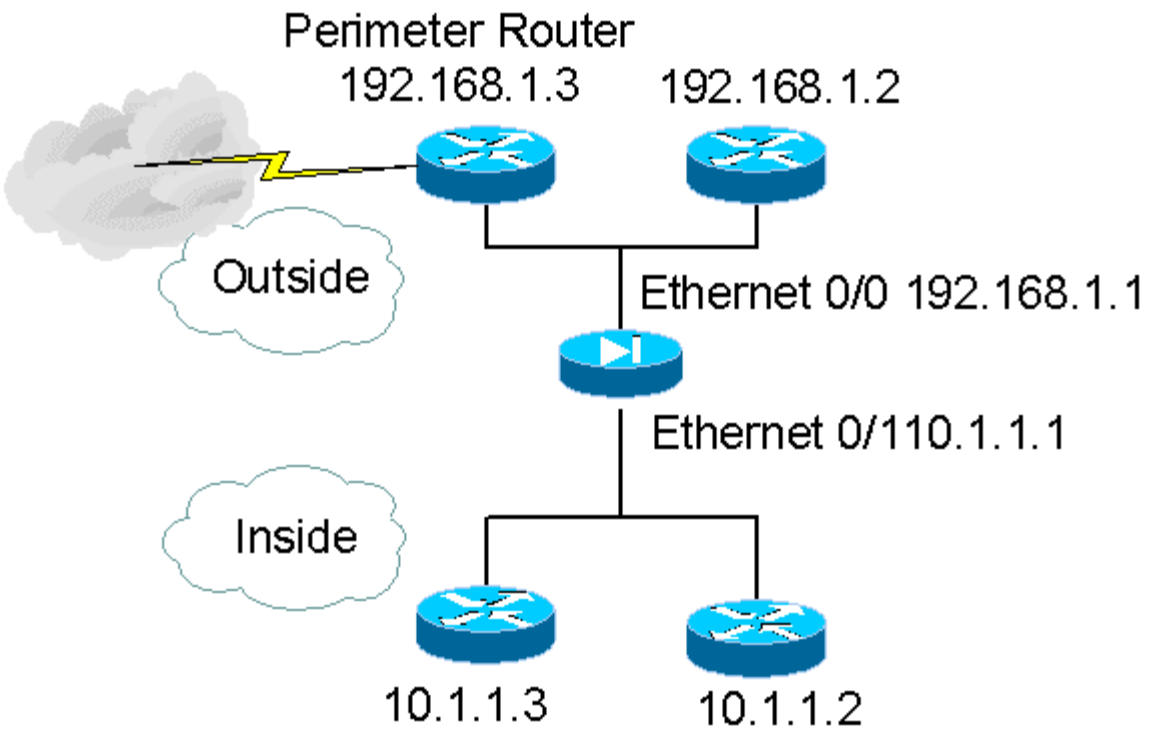
- Allows you to assign a default route outside

route inside 0.0.0.0 0.0.0.0 10.1.1.x

- Allows you to assign a default route inside

Remember with **nameif**, you have to set a security level. The more secure level should be the originator and the less secure, the destination. You could say that all traffic originating from the outside network could has a security level of 0 and the traffic going to the inside network has a security level of 100. This would be a way to create rules.

Lets look at the diagram of the above config:



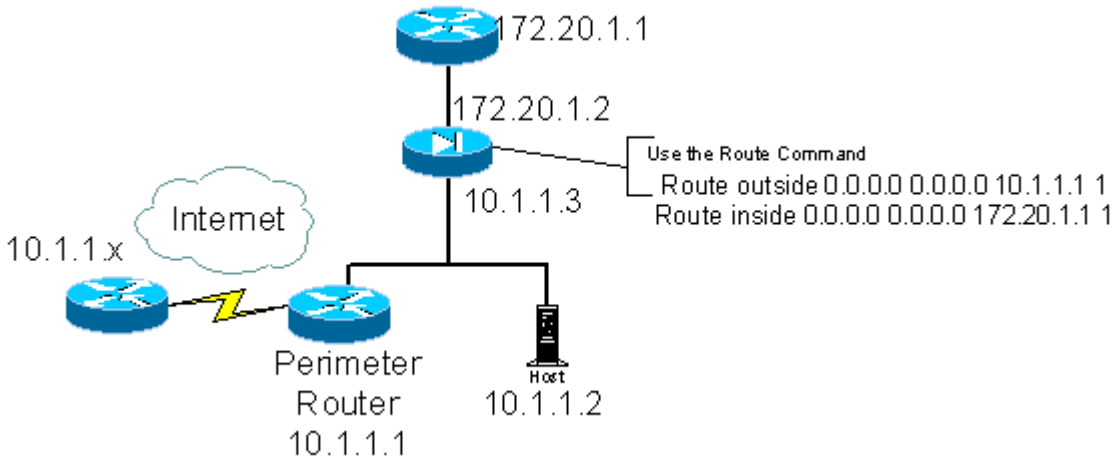
This is the basic gist of setting up the PIX and this should be enough to get you up, running, and functional.

Static Routes

Static routes can be configured with the **ROUTE** command. The route command allows you to add static or default routes for interfaces.

The syntax:

Route if_name ip_address netmask gateway_ip {metric}



The Metric is the number of hops to the gateway. You can use tracert, traceroute or trace to find this information.

Basic Configuration Command Set

Command	Basic Description
Enable	Get to privileged mode
Reload	Reboots / reloads config
Write erase	Clears current config in flash
Help or ?	To get help
Write terminal	To view current config
Passwd	(Yes, like Unix) Sets password for Telnet
Enable password	Sets privileged mode password
Configure Terminal	Starts configuration mode for the terminal
Hostname	Changes the PIX host name at command prompt
Nameif	Names interfaces / assigns security levels

Ip address	Sets an Ip address to a specific interface
Write memory	Writes current config to flash
{NO} debug icmp trace	Debugs icmp through the PIX
Conduit	Adds conduits through a PIX for incoming connections
Show arp	View the arp cache
Global	Create a pool of global addresses
Nat	Will associate a network with a pool of global Ip's
Clear xlate	Clears the translation slot information
Route	Used to enter a static default route

Click here For lengthy documentation from Cisco on how to configure the PIX

Configuring Access through the PIX Firewall

Recommended reading from Cisco:

Establishing Connectivity Through Cisco PIX Firewalls

Inbound and outbound access:

You should look at you security needs when designing the implementation of the PIX. You of course are going to have to allow some data through otherwise you have a denial of service on yourself. Ask yourself basic questions to get a feel for what you will need. Most of this will revolve around Internet access.

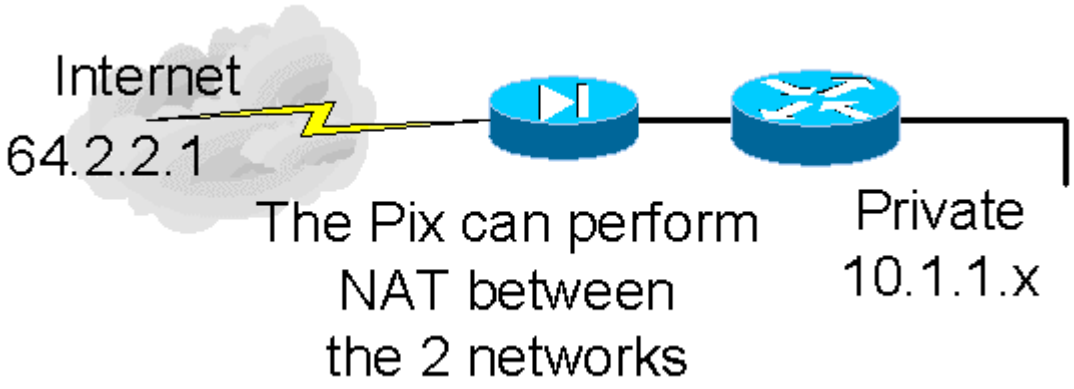
PIX NAT

What is NAT?

- The Network Address Translation (NAT) feature works by substituting, or translating, host addresses on an internal interface with a "global address" associated with an outside interface
- This protects internal host addresses from being exposed on other network interfaces
- To understand whether you want to use NAT, you have to decide if you want to expose your internal addresses on other network interfaces connected to the PIX Firewall.

- If you choose to protect internal host addresses using NAT, you must identify the pool of addresses you want to use for translation

This feature will enable you, the designer, to allow networks to connect using pre-existing addressing schemes. This is used many times when companies connect to other companies with the same private internal addressing schemes. Either that or it can translate private addressing to a public address for use on the Internet.



Example:

Global (outside) 1 64.2.2.x – 64.2.2.x

Nat (Inside) 1 10.1.1.0 255.255.225.0

This can become considerably more intricate as your designs get bigger and more involved. Make sure you have the fundamentals down for doing basic NAT commands.

You can also use the command: **Nat 0**

This will allow you to control what internal addresses are visible on the outside.

PIX PAT

This is for port address translation and can be configured so that the address pool maps TCP port numbers to a single IP address. PAT can also be used with NAT.

Static command

The static command is used to statically map a local IP to a global IP. The syntax is:

Static *{(internal_if_name, external_if_name)} global_ip local_ip {netmask network_mask} {max_cons {em_limit}} {norandomseq}*

internal_if_name

- Internal interface name

external_if_name

- External interface name

global_ip

- Global IP for the outside interface (this can't be a PAT IP)

local_ip

- Local IP for the inside network

netmask

- Use this word before specifying the actual netmask

network_mask

- The network mask

max_cons

- Maximum connections permitted across all interfaces

em_limit

- Embryonic connection limit

norandomseq

- This is an option (do not randomize packet sequence order)

Conduit command

The conduit command is used to permit or deny connections from outside the PIX firewall to access services from hosts inside the network. The Syntax is:

Conduit permit | deny protocol global_ip global_mask {operator port {port}} foreign_ip foreign_mask {operator port {port}}

Permit

- Permit access if conditions are met

deny

- Deny access if conditions are met

protocol

- Specifies transport protocol

global_ip

- An ip address defined by a global or static command

global_mask

- Network mask of global ip

operator

- Lets you specify a port or port range (e.g., any gt)

port

- Services you permit to be used while using global ip

foreign_ip

- External ip address

foreign_mask

- Network mask of external ip

Note: Remember that the conduit commands are processed in the order they are entered in the config

Fixup protocol

Allows you to view, change, enable, and disable application level protocol analysis through a PIX firewall. By default PIX is set to handle:

- H.323
- FTP
- SMTP
- HTTP
- RSH
- SQLNET

Command Set

No nat (inside)	Removes nat from inside interface of PIX
Nat (inside)	Configures nat on inside interface of PIX
Show nat	Displays nat info
Show xlate	Displays contents of the translation slots
Service	Resets inbound connections
Logging trap debug	Sends syslog messages to syslog server
Fixup protocol	Change, disable, list an application protocol feature
No debug all	Stops all debugging activity

Outbound access

To control outbound access you can use the **outbound** command.

You can use the PIX to construct access lists that will prevent outgoing traffic from traveling from a specific port to a specific IP, or to a specific service. The outbound command will create an access list, and the **apply** command applies that access list to an interface.

The PIX allows all outgoing connections unless you explicitly deny them. You should deny all outbound connections and selectively permit what you want.

To use the outbound command, use the following syntax:

Outbound *list_id except | permit | deny ip_address {netmask {java | port}* protocol

list_id

- *ID number for the access list*

except

- *Crete an exception to a previous outbound command*

permit

- *Allows the access list to access the specific IP and port*

deny

- *Deny the access list to access the specific IP and port*

ip_address

- *The IP for this access list entry*

netmask

- *The IP's network mask (note that 0.0.0.0 indicates ALL and can be abbreviated as 0)*

java | port

- *Java indicates port 80 which enables java applets to come through by default*
- *Port indicates a port or range of ports*

protocol

- Limit access to a protocol (TCP / UDP)

The apply command determines whether the permit or deny statements in the outbound command will apply to an outgoing interface. This is the syntax:

Apply *{(if_name)} list_id outgoing_src | outgoing_dest*

if_name

- *The internal network interface originating the connection*

list_id

- *The tag number for the access list*

outgoing_src

- *Used to deny | permit an internal IP the ability to start outbound connections*

outgoing_dest

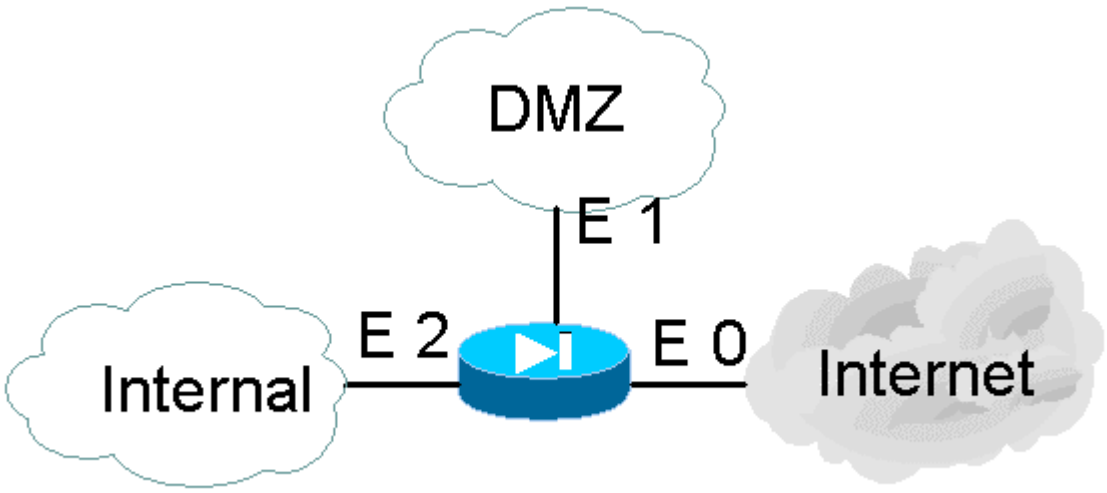
- Used to deny | permit access to an external IP

Configuring Multiple Interfaces

The PIX supports multiple perimeter interfaces to protect you network. It can do this by having three Ethernet interfaces. The first interface resides on the untrusted network (external network / Internet).

The next interface can reside on your DMZ where you have your bastion hosts or publicly assessable servers such as WEB, FTP, DNS and mail relay.

Your last interface can sit on your trusted Internal network. This method is a great way to enforce your security policy.



This will produce a three-legged firewall. You can also use other interfaces like token ring; you are not tied down to just Ethernet.

Use the following guidelines when planning a three legged PIX firewall design:

- Inside and outside interfaces can't be given different security levels or be renamed
- Packets can't flow between interfaces that have the same security level
- Set default routes and only use a single route to the outside interface
- Use NAT to allow users start outbound connections on their interfaces
- After setting up a config where you modify the global statement, save the config and use the clear xlate to update the Ip's in the translation table
- If you want to permit access to servers on networks that are protected, use the conduit (or static) command sets

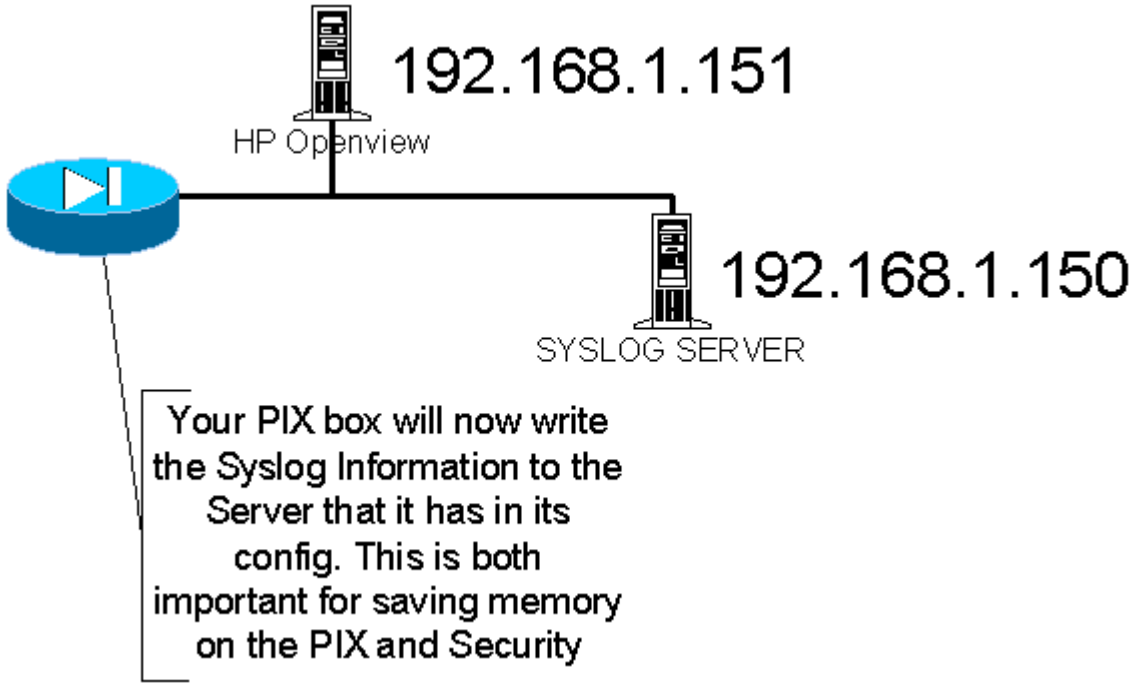
Links from Cisco on how to do the config for multiple interface configurations

- Two-Interface PIX Firewall
  This is a reference on how to set up a two interface PIX
- Three-Interface PIX Firewall
  This is a reference on how to set up a three interface PIX
- Four or More Interfaces in the PIX Firewall
  This is a reference on how to set up a four+ interface PIX
- Basic Two-Interface Configuration without NAT
  Basic Two-Interface Configuration with NAT
  Two Interface Multiple Server Configuration
  Three Interfaces without NAT
  Three Interfaces with NAT
  Four Interfaces with NAT
- Higher Security Level to Lower Security Level Access
  Lower Security Level to Higher Security Level Access
- Six Interfaces with NAT
- Higher Security Level to Lower Security Level Access
  Lower Security Level to Higher Security Level Access

Configuring Syslog

The PIX will generate syslog messages from system events. It will send these messages for document security, resources, system and accounting issues. You can enable logging simply by pointing the PIX to the IP of the syslog server.

Typical Syslog Solution



You want to use the logging command set to configure logging. Here is an example:

Logging on

Logging buffered

Logging console

Logging trap warnings

Logging host 192.168.1.150 (look at the diagram above)

The syntax is as follows:

On	Begins to send syslog messages to all output locations
Buffered	Sends the messages to the internal buffer
Console	Displays the messages on the PIX console
Facility	Specifies the syslog facility (default is 20)
Host	Specifies the server that will receive the syslog messages
Monitor	Displays syslog messages within telnet sessions

Trap	Used with SNMP and trapping
In_if_name	Defines interface where the syslog server is
Local_ip	Syslog servers IP address
Level	Specifies the syslog message level as a number or a string
Facility	Hosts the messages based on the facility number

To stop:

Use **no logging on**

To view:

Use **show logging**

Always set up a syslog server if you can. Now you can store and audit incoming syslog messages and not have to worry about overflowing your log on the PIX.

Links from Cisco on how to do the config for syslog configurations:

- Enable Syslog

- Viewing Messages from the Console
  Viewing Messages from a Telnet Console Session
  Sending Messages to a Syslog Server
  Changing PFSS Parameters
  Recovering from Disk-Full
  More on the logging Command

- Syslog Facility and Level

- Configuring a UNIX System for Syslog
- Setting Up PIX Syslog

Cisco Secure PIX Firewall failover

It is recommended to view this Documentation from Cisco:

How Failover Works on the Cisco Secure PIX Firewall

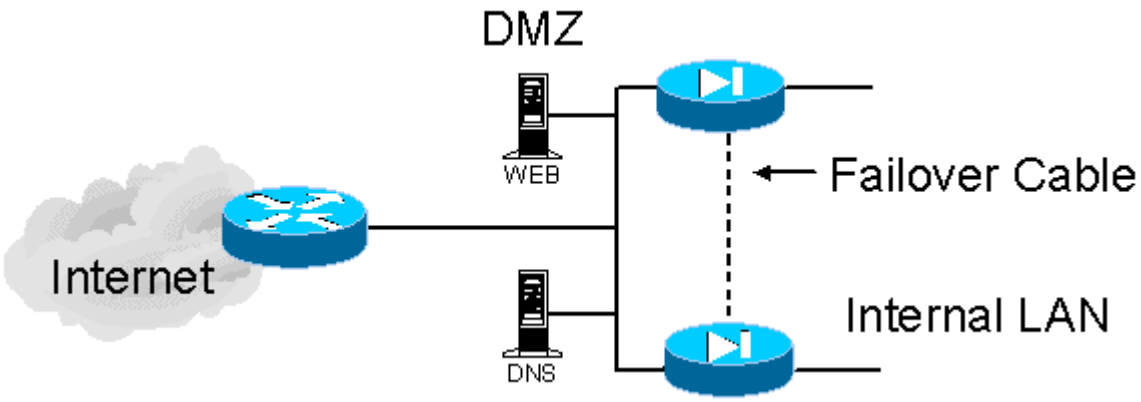
Advanced Configurations For PIX Failover

What is Failover?

You can use the PIX failover capability to have a hot standby solution for your PIX firewall design. In this scenario, you need to have two identical PIX boxes. One takes the role of primary and the other takes the role of secondary. If the primary dies, the secondary PIX will transparently pick up the workload. You must remember that the PIX boxes MUST BE IDENTICAL. You can't mix a PIX 515 in a failover solution with a PIX 520. A failover cable is used to connect the two firewalls and will provide the failover control signal.

In more detail, the standby unit uses the failover IP address and the MAC addresses of the Secondary unit. If a failover occurs, the units swap the IP address and MAC addresses they are using to replace each other on the network. The IP to MAC address relationships remain exactly the same, so no ARP tables in the network need to time out or be changed.

This would be a typical PIX failover solution



You can see that you have all the major benefits of a hot spare solution:

- Minimizes a single point of failure
- Maximizes your network reliability
- It is transparent (users behind the firewall do not know the difference)
- Still conforms to having a DMZ and you can apply security on the gateway router as well

To configure a Failover solution you can use the following commands and syntax:

Failover *{active}*

The active command makes the failover feature "active" or activated. You can use this command to force control back to a primary in the case that the secondary has to take over. You can also add **no failover active** on the secondary unit to initiate the same response.

Command Set

Failover active	Turns on failover for the PIX box
No failover active	Turns of Failover for a PIX box
Show failover	Shows status of the connection and determines which unit is active
Write standby	Forces an update on the active unit

Additional items to remember:

- Remember that Ethernet failover detection should occur within 30 seconds and Token Ring takes a longer time to occur
- The cable itself determines who is primary and who is secondary. Look for the markings on the cable
- Always make config changes to the active unit! Changes made to the standby unit are not saved to the active unit
- Remember that this solution is entirely for failover not load balancing
- PIX boxes must be identical and that includes: model, memory, network interface cards, IOS versions. This means identical!

More information from Cisco:

- Configuring Failover
- Configuration Replication
- Failover Configuration Commands
- Stateless TCP Failover

Command solution for Stateful failover:

failover on
failover ip address *if_name ip_address*
failover link *if_name*

Content Filtering

URL filtering and Java Blocking

If you want to provide maximum protection to your network and users, you must add additional configuration pieces into your PIX box. In most situations, you will need to permit access to port 80 for your users to access the Internet. This is a major problem because java applets can be downloaded because of access to http.

Java applets are known to be potentially dangerous and should not be allowed through. They can contain hidden code that could prove to be dangerous to your internal network if allowed through.

You can resolve this by using filtering:

To enable Java filtering you can use the **outbound** command with a keyword of *Java*

Here is the syntax:

Outbound *10 deny 192.168.1.1 255.255.255.0 java apply 10 outgoing_src*

To filter URLs you can use the following command string:

Url-server *host 192.168.1.1 filter url http 0 0 0 0*

Command Set

ActiveX	Used to block outbound ActiveX applets
Url	Filters URL's from the data going through the PIX
Http	Filters Http URL data
Except	This creates an exception to another filter condition

PIX Password Recovery

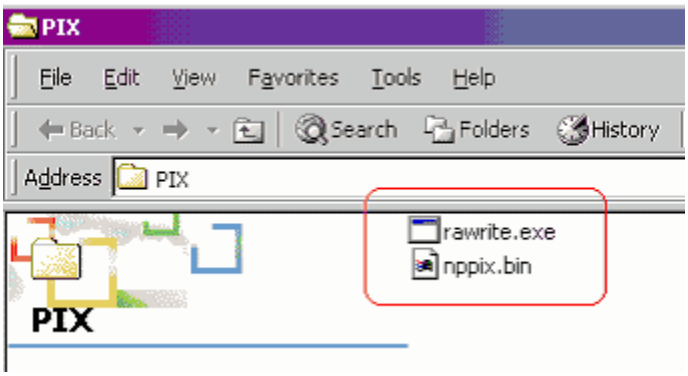
Please review Cisco Documentation:

PIX Password Recovery

Password recovery on a PIX box can be a little tricky. You would not follow the same procedures you would on a router with registers. For the PIX you need to follow different steps:

- Here is the step by step from Cisco
- First, you will need a CCO ID. This is given to partners and allows access to get images from Cisco. Without the login, you will not be able to do the following tasks

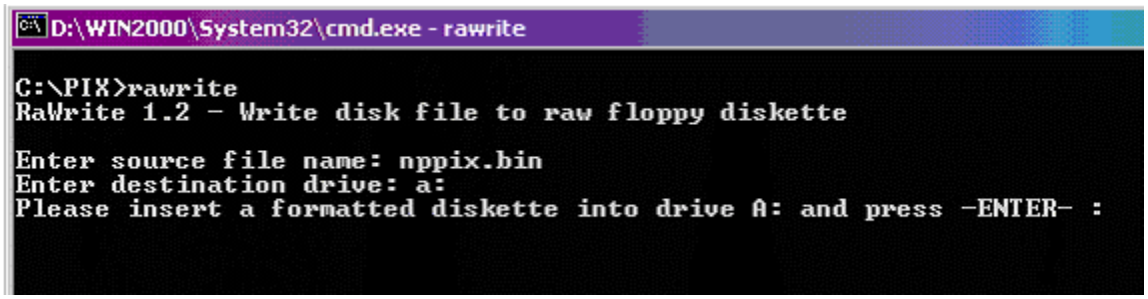
- Download the two images you need: rawrite.exe (mandatory)
- Now download one of the following files, depending on the PIX software version you are currently running, and place them both is the same directory:



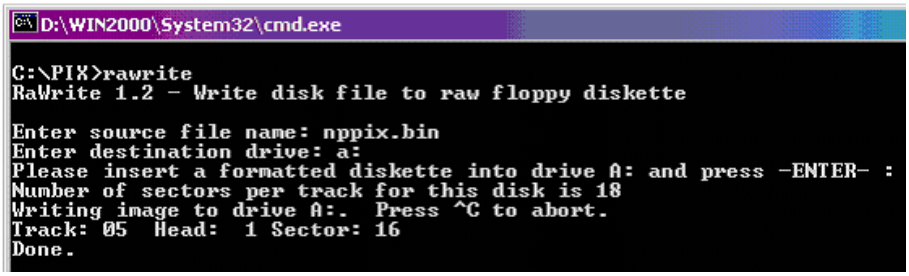
Below are versions you need depending on what version of the PIX you have:

  - nppix.bin (4.3 and earlier releases)
  - np44.bin (4.4 release)
  - np50.bin (5.0 release)
  - np51.bin (5.1 release)
  - np52.bin (5.2 release)
  - np53.bin (5.3 release)

- Now that you have both files in the same directly, execute **RAWRITE**



- This will start the program and start the process of setting up a floppy
- Next enter the file name that you need (I selected nppix.bin)
- Enter the source drive for the floppy
- Insert a formatted floppy and press enter



- Now you have a floppy with the password recovery tool

Note: Make sure you know how to do password recovery on the PIX – and know that the 515 is different.

For password recovery documentation for all Cisco's product go to this URL to find password recovery for all Cisco products: Advanced Password Recovery.

AAA Configuration on the Cisco Secure PIX Firewall

What is AAA?

- Authentication is who you are
- Authorization is what you can do
- Authentication **is** valid without authorization
- Authorization **is not** valid without authentication
- Accounting is what you did (logging)

To set up AAA on a PIX you need to first decide what level of access you are trying to set up. Here is a listing from Cisco:

Authentication Only
- Network Diagram
- Server Setup - Authentication Only
- PIX Initial Configuration - Authentication Only
- Configurable RADIUS Ports (5.3 only)
- PIX Authentication Debug Examples

To Set Up Authentication Only

The syntax is:

aaa-server *group_tag protocol authorization_protocol*

- The aaa-server command will allow you to specify a AAA server group
- You can have separate groups for Tacacs+ or Radius
- You can have up to 16 tag groups and each group can have up to 16 AAA servers (For a total of 256 AAA servers)

The syntax is:

aaa-server *group_tag (if_name) host server_ip key Timeout seconds*

- You can identify the AAA server group
- Next you can specify the interface out to the server
- The next line specifies the host server (Radius / Tacacs+ server) IP address
- The key is the alphanumeric key that is going to be used for encryption
- Timeout will be the max idle time before it switched to another server

Note: If the PIX finds the first server in the list to fail, it will go to the next server in the TAG group.

Authentication Plus Authorization

- Server Setup - Authentication Plus Authorization
- PIX Configuration - Adding Authorization
- PIX Authentication and Authorization Debug Examples
- New Access-list Feature

To Set Up Authentication and Authorization

To set up both Authentication and Authorization you will need to understand that if using this set up, Authentication will verify that you are who you say you are and Authorization will determine what services you can use. Now that that is understood, you can configure the PIX to perform this functionality:

The syntax is:

aaa authentication *authen_service except inbound | outbound if_name local_ip local_mask foreign_ip foreign_mask group_tag*

- This enable access to AAA
- It will authenticate both inbound and outbound traffic
- It will work with both Tacacs+ and Radius servers

The syntax is:

aaa authorization *author_service except inbound | outbound if_name local_ip Local_mask foreign_ip foreign_mask group_tag*

- This will enable authorization
- It will do both inbound and outbound traffic
- TACACS+ ONLY

Setting up Accounting:

The syntax is:

aaa accounting *acctg_service except inbound | outbound if_name local_ip Local_mask foreign_ip foreign_mask group_tag*

- Used to configure accounting
- Based on values such as ftp, http, telnet or protocol / port
- A port of 0 (zero) means all ports

Adding Accounting

- PIX Configuration - Adding Accounting
- Accounting Examples

Command Set

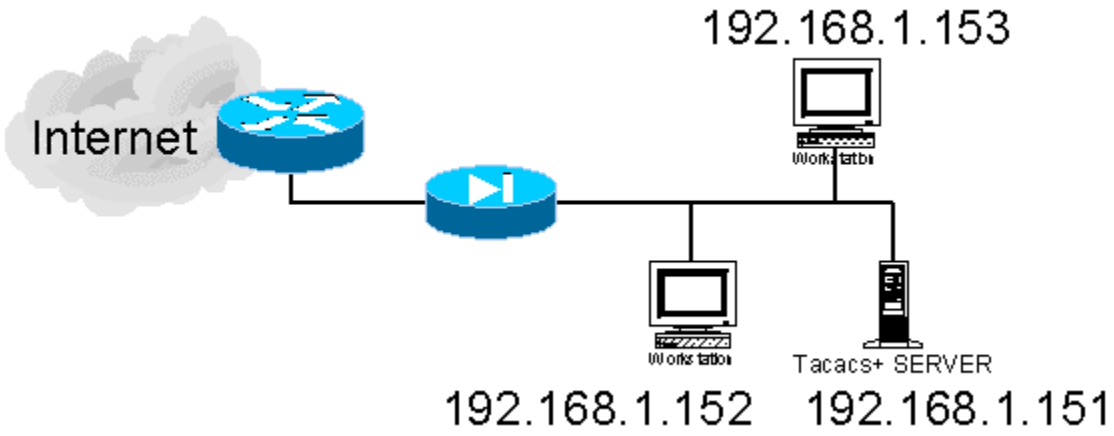
Accounting | *acctg_service*	Enable or disable (NO) accounting
Authentication | *authen_service*	Enable or disable (NO) authentication
Authorization | *author_service*	Enable or disable (NO) authorization
Inbound | Outbound	Specify traffic inbound or outbound

aaa-server	Specify an AAA server
If_name	The interface name where you require AAA
Group_tag	The group tag set with aaa-server command

AAA Tips

- Remember that if you lock yourself out, there is a backdoor and you can get to it through the console port with the Username and Password (Enable Password) string
- Please realize that as new code comes out, the AAA configurations alter slightly. Always check the latest documentation for whatever version of code you are using

AAA Diagram



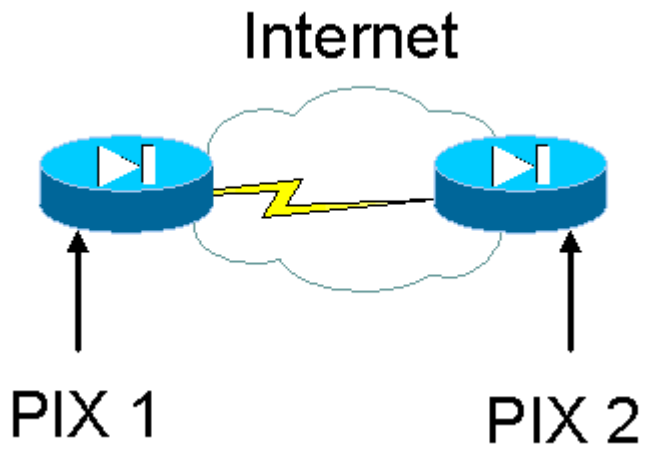
VPN Basics

What is a VPN?

Cisco's Primer for VPN's

A VPN (Or Virtual Private Network) is created to use the Internet (A public, unsecured media) to establish your WAN connections. It does this by creating a tunnel, encrypted and secure. Once the tunnel is created, you can set up a connection that is now secure.

Here is a set up of a simple VPN with two PIX appliances:



In this model, we can see that with the right configuration, you can set up a secure and encrypted tunnel over the Internet to create a Virtual Private Network.

To enable a PIX to have VPN functionality you need a specific piece of hardware:

- You can use the **VPN Accelerator Card** (VAC), which provides high-performance, tunneling and encryption services suitable for site-to-site and remote access applications
- This hardware-based VPN accelerator is optimized to handle the repetitive but mathematical functions required for IPsec
- Offloading encryption functions to the card not only improves IPsec encryption processing, but also maintains high-end firewall performance

Final Tips

Please use the Cramsession Links section. The 100+ links will guide you in the direction of all the commands used on the PIX and to white papers on how to set up all types of configurations. Almost all the information you need to prepare for this test is found on the Cisco site. If you can get your hands on the Documentation that comes in the PIX box, then that is a great study aid as well.

It is not entirely necessary to have hands on skills to pass this exam but you will be tested on the commands set for the PIX. You can use the Cramsession Links section to find a complete listing of all the commands and how to use them in simple to advanced configurations.

Good luck!

Special thanks to

Robert J. Shimonski for contributing this Cramsession. Please visit his site at http://www.rsnetworks.net/